JUNIPER NETWORKS

JunosE™ Software for E Series™ Broadband Services Routers

L2TP LNS

Release
14.3.x

Published: 2013-07-15

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

JunosE™ Software for E Series™ Broadband Services Routers L2TP LNS
Release 14.3.x

Revision History
July 2013—FRS JunosE 14.3.x

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

E Series and JunosE Documentation and Release Notes

For a list of related JunosE documentation, see http://www.juniper.net/techpubs/software/index.html.

If the information in the latest release notes differs from the information in the documentation, follow the *JunosE Release Notes.*

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Audience

This guide is intended for experienced system and network specialists working with Juniper Networks E Series Broadband Services Routers in an Internet access environment.

E Series and JunosE Text and Syntax Conventions

Table 1 on page xiv defines notice icons used in this documentation.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xiv defines text and syntax conventions that we use throughout the E Series and JunosE documentation.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents commands and keywords in text.	• Issue the **clock source** command. • Specify the keyword **exp-msg**.
Bold text like this	Represents text that the user must type.	**host1(config)#traffic class low-loss1**

`Fixed-width text like this`	Represents information as displayed on your terminal's screen.	**host1#show ip ospf 2**
		`Routing Process OSPF 2 with Router ID 5.5.0.250`
		`Router is an Area Border Router (ABR)`

Italic text like this	• Emphasizes words. • Identifies variables. • Identifies chapter, appendix, and book names.	• There are two levels of access: *user* and *privileged*. • *clusterId, ipAddress.* • *Appendix A, System Specifications*
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Syntax Conventions in the Command Reference Guide		
Plain text like this	Represents keywords.	terminal length
Italic text like this	Represents variables.	*mask*, *accessListName*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
| (pipe symbol)	Represents a choice to select one keyword or variable to the left or to the right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic | line
[ ] (brackets)	Represent optional keywords or variables.	[internal | external]
[ ]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 | level2 | l1]*
{ } (braces)	Represent required keywords or variables.	{ permit | deny } { in | out } { *clusterId* | *ipAddress* }

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the Technical Documentation page on the Juniper Networks Web site at http://www.juniper.net/.

To download complete sets of technical documentation to create your own documentation CD-ROMs or DVD-ROMs, see the Portable Libraries page at

http://www.juniper.net/techpubs/resources/index.html

Copies of the Management Information Bases (MIBs) for a particular software release are available for download in the software image bundle from the Juniper Networks Web site athttp://www.juniper.net/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

L2TP Functionalities

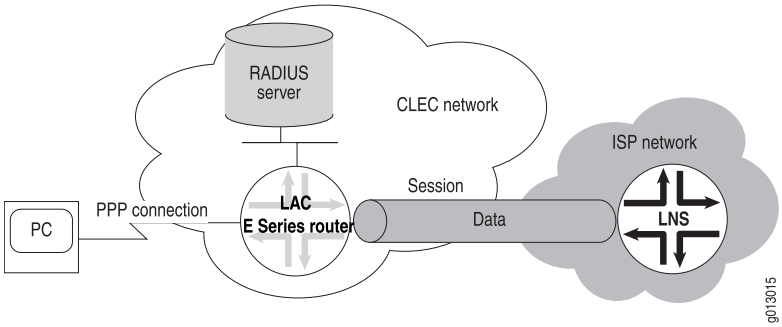
L2TP Overview

L2TP encapsulates layer 2 packets, such as PPP, for transmission across a network. An L2TP access concentrator (LAC), configured on an access device, such as an E Series router, receives packets from a remote client and forwards them to an L2TP network server (LNS), on a remote network.

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

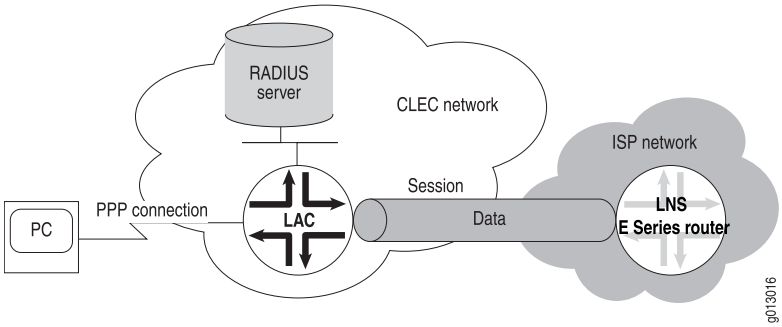
The E Series router creates tunnels dynamically by using authentication, authorization, and accounting (AAA) authentication parameters and transmits L2TP packets to the LNS via IP/User Datagram Protocol (UDP). Traffic travels in an L2TP *session*. A tunnel is an aggregation of one or more sessions. Figure 1 on page 3 and Figure 2 on page 4 show the E Series router in typical LAC and LNS arrangements.

Figure 1: Using the E Series Router as an LAC



.

Figure 2: Using the E Series Router as an LNS



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

Related Documentation

- Implementing L2TP on page 7
- L2TP Platform Considerations on page 12
- L2TP References on page 13

L2TP Terminology

Table 3 on page 4 describes the basic terms for L2TP.

Table 3: L2TP Terms

Term	Description
Attribute value pair (AVP)	Combination of a unique attribute—represented by an integer—and a value containing the actual value identified by the attribute.
LAC	L2TP access concentrator (LAC)—a node that acts as one side of an L2TP tunnel endpoint and is a peer to the LNS. An LAC sits between an LNS and a remote system and forwards packets to and from each.
Call	A connection (or attempted connection) between a remote system and an LAC.
LNS	L2TP network server (LNS)—a node that acts as one side of an L2TP tunnel endpoint and is a peer to the LAC. An LNS is the logical termination point of a PPP connection that is being tunneled from the remote system by the LAC.
Peer	In the L2TP context, refers to either the LAC or LNS. An LAC's peer is an LNS, and vice versa.
Proxy authentication	Authentication data from the PPP client that is sent from the LNS as part of a proxy LCP. Data might include attributes such as authentication type, authentication name, and authentication challenge.

Table 3: L2TP Terms *(continued)*

Term	Description
Proxy LCP	LCP (Link Control Protocol) negotiation that is performed by the LAC on behalf of the LNS. Proxy sent by the LAC to the LNS containing attributes such as the last configuration attributes sent and received from the client.
Remote system	An end-system or router attached to a remote access network, which is either the initiator or recipient of a call.
Session	A logical connection created between the LAC and the LNS when an end-to-end PPP connection is established between a remote system and the LNS. **NOTE:** There is a one-to-one relationship between established L2TP sessions and their associated PPP connections.
Tunnel	A connection between an LAC-LNS pair consisting of a control connection and 0 or more L2TP sessions.

Related Documentation

- L2TP Overview on page 3

Packet Fragmentation

The E Series router supports the reassembly of IP-fragmented L2TP packets. (For more information, see the *IP Reassembly for Tunnels* chapter in *JunosE IP Services Configuration Guide*.) However, it is preferable to prevent fragmentation within L2TP tunnels because of the effects of fragmentation and reassembly on performance.

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

To overcome the inadequacy of normal determination of the MRU under such circumstances, you can configure the PPP MRU size by using the **ppp mru** command in Profile Configuration mode, Interface Configuration mode, or Subinterface Configuration mode. Use Profile Configuration mode for dynamic PPP interfaces, and Interface Configuration mode or Subinterface Configuration mode for static PPP interfaces.

When you specify the size, you need to take into account the MRU for all possible links between the LAC and the LNS. You must also take into account the L2TP encapsulation that is added to all packets entering the tunnel.

For example, if the link between the LAC and LNS with the lowest MRU were an Ethernet link, the following calculation applies:

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

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

Related Documentation

- L2TP Overview on page 3
- Implementing L2TP on page 7

CHAPTER 2

L2TP Deployment

Implementing L2TP

The implementation of L2TP for the E Series router uses four levels:

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

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

Sequence of Events on the LAC

The E Series router creates destinations, tunnels, and sessions dynamically, as follows:

1. The client initiates a PPP connection with the router.
2. The router and the client exchange Link Control Protocol (LCP) packets. For details about negotiating PPP connections, see the *Configuring Point-to-Point Protocol* chapter in *JunosE Link Layer Configuration Guide*.
3. By using either a local database related to the domain name or RADIUS authentication, the router determines either to terminate or to tunnel the PPP connection.
4. If the router discovers that it should tunnel the session, it does the following:
   a. Sets up a new destination or selects an existing destination.
   b. Sets up a new tunnel or selects an existing tunnel.
   c. Opens a new session.
5. The router forwards the results of the LCP negotiations and authentication to the LNS.

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

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

Sequence of Events on the LNS

The E Series router sets up an LNS as follows:

1. An LAC initiates a tunnel with the router.
2. The router verifies that a tunnel with this LAC is valid—destination configured, hostname and tunnel password correct.
3. The router completes the tunnel setup with the LAC.
4. The LAC sets up a session with the router.
5. The router creates a dynamic PPP interface on top of the session.
6. If they are enabled and present, the router takes the proxy LCP and the proxy authentication data and passes them to PPP.
7. The E Series PPP processes the proxy LCP, if it is present, and, if acceptable, places LCP on the router in opened state without renegotiation of LCP.

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

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

Related Documentation

- L2TP Overview on page 3
- L2TP Platform Considerations on page 12
- L2TP Module Requirements on page 11
- L2TP References on page 13

Overriding LNS Out-of-Resource Result Codes 4 and 5

When the number of L2TP sessions reaches the configured maximum value, the LNS sends an out-of-resource result code (4 or 5) in a CDN (Call-Disconnect-Notify) message

to the LAC. This signals the LAC to fail over to another LNS that has the resources for more sessions.

Some third-party LAC implementations fail over only when they receive result code 2 sent in the CDN from the LNS. You can override result codes 4 and 5 with result code 2 on the LNS to enable such routers to fail over to another LNS. These codes have the following meanings:

- 2—Call disconnected for the reason indicated in error code
- 4—Call failed due to lack of appropriate facilities being available (temporary condition)
- 5—Call failed due to lack of appropriate facilities being available (permanent condition)

The following sections describe how to override the result codes and how to display the current code values.

- Overriding the Result Codes on page 9
- Displaying the Current Override Setting on page 9

Overriding the Result Codes

You can override the out-of-resource result codes 4 and 5 by issuing the **session-out-of-resource-result-code-override** command on the LNS.

- To override result codes 4 and 5:

```
host1:boston(config-l2tp-dest-profile-host)#session-out-of-resource-result-code-override
```

Displaying the Current Override Setting

You can view the current override setting for the LNS result codes in the L2TP destination profile.

- To display the current override setting:

```
ERX(config)#show l2tp destination profile boston
L2TP destination profile boston
Configuration
  Destination address
    Transport ipUdp
    Virtual router default
    Peer address 10.10.76.12
Statistics
  Destination profile current session count is 0
Host profile attributes
  Remote host is LAC
    Configuration
      Tunnel password is TunnelPass
      Local host name is LNS
      Local ip address is 46.1.1.2
      Disconnect-cause avp is enabled
      Tunnels are single-shot
      Override out-of-resource-result-code is enabled
    Statistics
      Current session count is 0
1 L2TP host profile found
```

Related Documentation

- session-out-of-resource-result-code-override on page 118
- show l2tp destination profile on page 174

CHAPTER 3

L2TP Platform and Module Requirements

L2TP Module Requirements

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

ERX7xx Models, ERX14xx Models, and the ERX310 Router

To use an LNS on ERX7xx models, ERX14xx models, and the ERX310 router, at least one Service line module (SM) or a module that supports the use of shared tunnel-server ports must be installed in the ERX router. For information about installing modules in the ERX router, see the *ERX Hardware Guide*.

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

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

When you configure the GE-2 line module or the GE-HDE line module with a shared tunnel-server port, the available bandwidth for tunnel services is limited to 0.5 Gbps per module. When you configure the ES2 4G line module with a shared tunnel-server port, the available bandwidth for tunnel services is limited to 0.8 Gbps per module.

For information about configuring tunnel services on dedicated and shared tunnel-server ports, see the *Managing Tunnel-Service and IPsec-Service Interfaces* chapter in *JunosE Physical Layer Configuration Guide*.

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

E120 Router and E320 Router

To use an LNS on an E120 router or an E320 router, you must install an ES2 4G line module (LM) or an ES2 10G ADV LM with an ES2-S1 Service I/O adapter (IOA). With the ES2 4G LM, it is also possible to use an LNS with an IOA that supports the use of shared tunnel-server ports. For information about installing modules in these routers, see the *E120 and E320 Hardware Guide*.

The combination of an ES2 4G LM or an ES2 10G ADV LM with an ES2-S1 Service IOA provides a dedicated tunnel-server port that is always configured on the IOA. Unlike SMs, the ES2 4G LM and the ES2 require the ES2-S1 Service IOA to condition it to receive and transmit data to other line modules. The ES2-S1 Service IOA also does not have ingress or egress ports. The ES2 10G ADV LM with the ES2-S1 Service IOA supports L2TP LNS functionality, which supports IPv4 as well as IPv6 encapsulated within PPP and L2TP over IPv4.

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

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

Related Documentation

- L2TP Overview on page 3
- Implementing L2TP on page 7
- L2TP Platform Considerations on page 12
- L2TP References on page 13

L2TP Platform Considerations

For information about modules that support LNS and LAC on the ERX7xx models, ERX14xx models, and the ERX310 Broadband Services Router:

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

For information about modules that support LNS and LAC on the E120 and E320 Broadband Services Routers:

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

Related Documentation

- L2TP Overview on page 3
- L2TP References on page 13

L2TP References

For more information about L2TP, see the following resources:

- RFC 2661—Layer Two Tunneling Protocol " L2TP" (August 1999)
- RFC 3145—L2TP Disconnect Cause Information (July 2001)
- Fail Over extensions for L2TP " failover" —draft-ietf-l2tpext-failover-06.txt (April 2006 expiration)
- RFC 4951—Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover" (August 2007)

For information about L2TP high availability support, see the *Managing High Availability* chapter in *JunosE System Basics Configuration Guide*.

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

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

For information about how to secure Layer 2 Tunneling Protocol (L2TP) tunnels with IP Security (IPsec) on your E Series router, see the *Securing L2TP and IP Tunnels with IPsec* chapter in *JunosE IP Services Configuration Guide*.

Related Documentation

- L2TP Overview on page 3
- L2TP Platform Considerations on page 12

CHAPTER 4

L2TP Sessions and Tunnels

Sessions and Tunnels Supported

The E120 and E320 routers support 60,000 L2TP sessions, the ERX1440 router supports 32,000 L2TP sessions, and all other E Series routers support a maximum of 16,000 L2TP sessions. The following guidelines apply:

- On all E Series routers

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

- On the E120 router, E320 router, and the ERX1440 router

  You can create a systemwide maximum of 60,000 sessions per E120 or E320 router or 32,000 sessions per ERX1440 router. The maximum session limit is spread in any combination across a maximum of 8000 tunnels. For a router that is operating as an LAC for some tunnels and as an LNS for others, the 8000 tunnels and the router's applicable maximum sessions limits apply to the combined total of LAC and LNS tunnels and sessions.

- On all E Series routers except the ERX1440 router, E120 router, and the E320 router

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

NOTE: In previous releases, the JunosE Software required that you use the **license l2tp-session** command to configure a license to enable support for the maximum allowable L2TP sessions on ERX1440 routers, E120 routers, and E320 routers. The **license l2tp-session** command still appears in the CLI, but it has no effect on the actual enforced limit. The reported license limit is 60,000. The **show license l2tp-session** command also still appears in the CLI.

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

Related Documentation

- L2TP Overview on page 3
- Implementing L2TP on page 7
- L2TP Module Requirements on page 11

Stateful Line Module Switchover Platform Considerations

Stateful line module switchover is supported on all E120 and E320 routers that contain ES2 4G line modules installed with the ES2-ES1 Service IOA. See the *E120 and E320 Module Guide* for modules supported on the E120 and E320 Broadband Services Routers.

Table 4 on page 16 lists the line module, SRP module, and IOA slot combinations that support stateful switchover of line modules and stateful switchover for LNS sessions, when the router operates as an LNS device on one side of an L2TP tunnel.

Table 4: Module Configurations Supported for Stateful Switchover of LNS Sessions

Router Model	SRP and SFM Model	Number of L2TP tunnels and sessions	Number of Active and Standby ES2-ES1 Service IOAs	Downlink and Uplink LMs	Support for Stateful Switchover of LNS Sessions
E320	SRP-100	16,000 tunnels and 16,000 sessions	2 Service IOAs (1 active and 1 standby)	ES2 4G LM and GE-4 IOA	Supported
E320	SRP-100	16,000 tunnels and 32,000 sessions	4 Service IOAs (2 active and 2 standby)	ES2 4G LM and GE-4 IOA	Supported
E320	SRP-320	32,000 tunnels and 32,000 sessions	4 Service IOAs (2 active and 2 standby)	ES2 4G LM and GE-4 IOA	Supported
E120	SRP-320	16,000 tunnels and 16,000 sessions	2 Service IOAs (1 active and 1 standby)	ES2 10G LM and GE-8 IOA	Not supported
E120	SRP-320	32,000 tunnels and 32,000 sessions	4 Service IOAs (2 active and 2 standby)	ES2 10G LM and GE-8 IOA	Not supported

Table 4: Module Configurations Supported for Stateful Switchover of LNS Sessions *(continued)*

Router Model	SRP and SFM Model	Number of L2TP tunnels and sessions	Number of Active and Standby ES2-ES1 Service IOAs	Downlink and Uplink LMs	Support for Stateful Switchover of LNS Sessions
E120	SRP-320	16,000 tunnels and 16,000 sessions	2 Service IOAs (1 active and 1 standby)	ES2 4G LM and GE-8 IOA	Supported
E120	SRP-320	32,000 tunnels and 32,000 sessions	4 Service IOAs (2 active and 2 standby)	ES2 4G LM and GE-8 IOA	Supported

Related Documentation

- *Stateful Line Module Switchover Overview*
- *System Operations When Stateful Line Module Switchover Is Enabled*
- *Replacement of Line Modules When Stateful Line Module Switchover Is Enabled*
- Application Support for Stateful Line Module Switchover on page 17

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 Documentation

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

Application Support for Stateful Line Module Switchover

Applications are either supported or unsupported by stateful line module switchover.

- Supported—You can configure supported applications without having any adverse impact to stateful line module switchover. When a switchover occurs, supported applications can react to switchovers in one of two different ways:
  - Gracefully recover using mirrored static and dynamic information (for example, IP, PPP, and PPPoE)
  - Recover using static configuration only; that is, no runtime state is restored after a switchover. Dynamic configuration and state information are lost. (For example, CLI sessions are restarted, telnet sessions are dropped, multicast routes must be rebuilt, and so on.)
- Unsupported—We recommend that you not configure unsupported applications on a line module running in high availability mode. Although configured unsupported applications suspend high availability or prevent high availability from becoming active, they do not cause any problems with the function of the router.

The sections that follow describe the working behavior of applications that support stateful line module switchover.

NOTE: **Only the applications discussed in the sections that follow are compatible with stateful line module switchover.**

Policy Management

Because the policy application in the line module does not contain the complete state of all the policy definitions in mirrored containers, the SRP module is used to download the policy definitions and attachments to the newly active line module when a stateful switchover occurs. The policy application sends multiple policy attachment requests from the SRP module to the line module in a single notify operation and in a bulk manner, instead of one policy attachment request in each notify event. This method of transferring policy attachment requests in bulk reduces the time to download all the attachments to the newly active line module.

QoS

QoS configuration is maintained in each line module and these settings are mirrored to the standby line module. During a stateful line module switchover, the QoS agent in the line module restores the configuration in the newly active line module. The QoS agent clients (such as IP and Ethernet) bind and register to the QoS agent before they replay the interfaces for creating QoS attachments. The QoS agents ensure that the queues are reestablished appropriately for the interfaces.

Connection Manager and Queue Manager

The queue manager resides on the SRP and the queue manager agents are present on all the line modules. When the primary line module resets, the spare module takes over the usage of the redundancy database. The queue manager identifies a connection based on the queue ID, the connection manager uses the stream ID to recognize a connection, the forwarding controller uses the stream ID, similar to the connection manager, to

determine a connection. For example, when slot 2 communicates with slot 1, the queue manager identifies this connection as QID1. Similarly, when slot 3 communicates with slot 2, this link is labeled as QID2.

The connection manager uses SID1 to denote the connection from any slot with slot 2 and SID2 to signify the link from any slot with slot 3. The slot 2 address is specified as 2a2, where '2' refers to the logical slot, 'a' indicates the active state of the slot, and '2' represents the physical slot. When slot 0 takes over slot 2, the slot that is taken over is identified as 2a0. On reception of the controller up event on the SRP module for the spare line module, the queue manager initiates a request to the connection manager to create a fresh connection for the address 2a0. The connection manager logically labels the stream ID that refers to slot 2 to be down and creates a new stream ID to communicate with slot 0. The forwarding controller database that possesses a mapping of the slot ID, stream ID, and traffic class is updated accordingly to replace any streams that earlier pointed to slot 2 to start referring to slot 0. The queue manager agent running on the line modules handle the forwarding controller updates.

PPP

The PPP application on the line module contains the basic protocol, timers, and state machines in a running state. All the dynamic session data collected from protocol negotiations is present in the mirrored storage containers on the line module. For stateful line module switchover, all the mirrored storage data is saved on the standby module, replicating the session on the standby module. After the switchover takes place, the application initialization process on the standby module reconstructs the mirrored data and brings up the sessions to the established state (operational status is up). Some of the sessions that are still in the process of being created (alternating between the up and down operational states) are not retained during the switchover. This behavior of not preserving sessions that are not established is similar to the characteristic followed during unified ISSU, where sessions that are not completely created retry after the newly configured primary line module is available.

The total time required for the standby module to become active is dependent on the size of the configuration parameters. On a normal basis, it takes about 2-3 minutes for the new primary module to become active, in which case, clients running small intervals of keepalives expire. This system of expiry of keepalives poses a limitation on the stateful switchover model. This limitation is similar to the restriction seen during the upgrade phase of the unified ISSU process in which traffic forwarding is interrupted for a brief period. To work around this restriction, echo requests for the sessions that terminate on the failed line module are redirected to a different hardware. For failures on tunnel server modules (ES2 4G LMs with Service IOA), the access module handles such problems.

L2TP

L2TP configuration and operation data are maintained in the line module and this information is mirrored to the standby module. After the switchover of the primary tunnel server module to the secondary module occurs, the L2TP application on the line module restores the configuration and operation data to the newly active primary module. This mechanism is similar to the warm start procedure during unified ISSU. The L2TP application on the SRP module handles the line module events related to the primary and secondary modules.

Forwarding Controller

When a stateful line module switchover occurs, the forwarding controller (FC) tables that refer to the failed line module are updated with stream IDs that map to the line module (ES2 4G LM with Service IOA) that has taken over the role of the primary module. FC tables use a combination of slot ID, stream ID, and key hash table. The modifications to the FC tables enables packets to be sent to the newly functioning primary module after the switchover is complete.

During the stateful line module switchover, PPP subscriber sessions on an LNS device in an L2TP tunnel might be terminated due to the lack of PPP keepalive responses from the LNS device. To prevent the termination of subscriber sessions, the access module in the LNS device handles the PPP echo requests from all active subscriber sessions (on behalf of the failed line module) and responds with valid PPP echo reply messages. After a successful switchover, the access module in the LNS stops responding to the PPP echo request messages.

When the access module in the LNS receives an event from the application, such as PPP, to denote a failure with the primary line module, the access module starts processing the PPP echo requests that are destined for the LNS. The access module in the LNS concludes the handling of PPP echo requests after it receives a notification that the switchover is complete.

The following configuration events also take place during a stateful switchover on tunnel server modules that are installed on E120 and E320 routers that operate as LNS devices in an L2TP tunnel:

- All possible next hop attributes, which signify the IP address of the node that is closer to the advertised prefix (such as MPLS and ATM sessions), at the LNS are supported.
- PPP keepalive messages are not considered for the session statistics calculated during stateful switchover.
- Only the PPP echo request messages received on the L2TP tunnels or sessions that terminate at the LNS are handled by the access module during switchover. The FC in the access module in the LNS device does not send or generate any PPP echo request messages on its own.
- Sequence number checking for data packets received on all L2TP tunnels in the router and L2TP over IPsec to configure secured transport connections are not supported during a stateful line module switchover.
- During the switchover, when the access module that handles the echo request messages on the LNS fails (stops responding or traffic stops flowing), the PPP subscriber sessions that wait for echo response messages from the LNS terminate owing to the absence of a response.
- If line module redundancy is enabled and a switchover is being performed on an access module in a LNS device, and if a stateful line module switchover also commences at the same time, echo replies are not sent from the access module in the LNS. The PPP

subscriber sessions that expect the echo response messages from the LNS during the switchover are terminated owing to the absence of an echo response.

- During a stateful line module switchover, if the secondary tunnel server module (ES2 4G LM with Service IOA and configured on a router that acts as the LNS) encounters a fault, the access module stops responding to PPP echo request messages after it receives the notification from the SRP module or the PPP application.

When you perform a stateful switchover on one pair of line modules enabled for high availability, L2TP sessions continue to be established on the other tunnel server modules. The Server Card manager (SCM) application selects the circuits from other tunnel server modules to reroute the L2TP sessions until the stateful switchover from the primary module to the secondary module is completed. The L2TP application notifies the SCM after the switchover is completed and the SCM continues to balance the sessions across all the available tunnel server modules.

Mirroring Subsystem

The mirroring application is used to synchronize the configuration information available on the line modules. The mirroring state machine resides on both the primary and secondary line modules. The mirroring functionality uses interchassis communication (ICC) sessions to coordinate between line modules. Mirroring is supported for the volatile memory present on the line modules. After an initial bulk synchronization of storage data from the primary line module to the secondary line module occurs, any subsequent data is mirrored as and when transactions are posted. When a stateful switchover occurs, applications recover to the steady state by restoring the configuration data from the mirrored containers.

State machine-dependent applications, such as PPP, L2TP, and QoS applications, contain a dummy forwarding controller database that is populated on the access line module (receives traffic from low-speed circuits and routes them to uplink modules). This dummy database enables responses to be sent from the access line module to the keepalives that it receives until the switchover completes. This method of sending responses to hello packets ensures minimal data outage during the switchover of line modules. After the stateful switchover, the stateful applications start their regular processing by reestablishing their containers and perform a synchronization with the SRP module for dynamic data.

Unified ISSU

A unified ISSU operation proceeds properly if the configured secondary line module had taken over as the newly active primary line module. When you enter the **issu start** command to begin the upgrade phase of the unified ISSU process, the secondary line module is disabled. The disabled line module during unified ISSU is cold booted after the unified ISSU operation is complete. Only the primary line module participates in the unified ISSU operation.

ICCP

Interchassis Communication Protocol (ICCP) is used to establish communication sessions between line modules that are configured for stateful switchover (configured in the high availability pair). Controller events are generated for existing sessions on the line modules

with a notification about the session establishment and session teardown. The applications that are running on the SRP module with ICC sessions formed between the SRP and line modules are notified with the controller events after a stateful line module switchover occurs.

The line module high availability manager resides on the SRP module to enable the stateful switchover from a failed primary module to the secondary module in a high availability pair of devices. The high availability manager interacts with its peer agent on the line modules using ICC session and control bus. After the modules in a high availability pair become operational in primary and secondary modes, the high availability manager notifies interchassis controller (ICC) to enable ICC communication between the line modules.

Related Documentation

- *Stateful Line Module Switchover Modes*
- *Stateful Line Module Switchover States*
- *Activating High Availability*
- *Deactivating High Availability*

CHAPTER 5

Termination of PPP and L2TP Subscriber Sessions

VSAs for Dynamic IP Interfaces Overview

Table 5 on page 23 describes the VSAs that apply to dynamic IP interfaces and are supported on a per-user basis from RADIUS. For details, see *JunosE Link Layer Configuration Guide*.

Table 5: VSAs That Apply to Dynamic IP Interfaces

VSA	Description	Type	Length	Subtype	Subtype Length	Value
Ingress-Policy-Name	Specifies the name of the input (ingress) policy	26	len	10	sublen	string: *input-policy-name*
Egress-Policy-Name	Specifies the name of the output (egress) policy	26	len	11	sublen	string: *output-policy-name*
Ingress-Statistics	Indicates whether statistics are collected on input	26	12	12	6	integer: 0 – disable, 1 – enable
Egress-Statistics	Indicates whether statistics are collected on output	26	12	13	6	integer: 0 – disable, 1 – enable

Table 5: VSAs That Apply to Dynamic IP Interfaces *(continued)*

VSA	Description	Type	Length	Subtype	Subtype Length	Value
QoS-Profile-Name	Specifies the name of the QoS profile to attach to the interface	26	len	26	sublen	string: *qos-profile-name*

To use the VSAs shown in Table 5 on page 23:

- Specify the policy, or one or more QoS VSAs in the desired RADIUS user entries.
- Create the ingress or egress policy, or the QoS profile. Policies minimally consist of one or more policy commands and may include classifier control lists and rate limit profiles. See the *JunosE Policy Management Configuration Guide* for more information about policies and policy routing. See the *JunosE Quality of Service Configuration Guide* for information about creating QoS profiles.

When a dynamic interface is created according to a profile, the router checks with RADIUS to determine whether an input or output policy or a QoS profile must be applied to the interface. The VSA, if present, provides the name, enabling policy or QoS profile lookup. If found, the policy or QoS profile is applied to the dynamic interface.

The router also determines whether the creation profile specifies any policies to be applied to the interface. Policies specified by the RADIUS VSA supersede any specified by the profile, as described in the following example:

The RADIUS user entry includes an Ingress-Policy-Name VSA that specifies the policy input5. The profile specifies two policies, input7 and output1. In this case, the RADIUS-specified input policy (input5) and the profile-specified output policy (output1) are applied to the dynamic interface.

For information about assigning policies via profiles, see the *JunosE Policy Management Configuration Guide*. Only attributes assigned by RADIUS appear in RADIUS Acct-Start messages. RADIUS attributes specified by a profile for dynamic interfaces do not appear in RADIUS Acct-Start messages because the profile is not active when the Acct-Start message is generated. These attributes appear in RADIUS Acct-Stop messages for a profile that is active when the session is terminated.

The following section explains traffic shaping for PPP over ATM interfaces:

- Traffic Shaping for PPP over ATM Interfaces on page 24

Traffic Shaping for PPP over ATM Interfaces

The router supports the configuration of traffic shaping parameters for PPP over ATM (PPPoA) via domain-based profiles and RADIUS. In connection with this feature, Table 6 on page 25 describes VSAs that apply to dynamic IP interfaces and are supported on a per-user basis from RADIUS.

Table 6: Traffic-Shaping VSAs That Apply to Dynamic IP Interfaces

VSA	Description	Type	Length	Subtype	Subtype Length	Value
Service-Category	Specifies the type of service	26	12	14	6	integer: 1 – UBR 2 – UBR PCR 3 – NRT VBR 4 – CBR 5 – RT VBR
PCR	Specifies the value for the peak cell rate (PCR)	26	12	15	6	integer
SCR	Specifies the value for the sustained cell rate (SCR)	26	12	16	6	integer
MBS	Specifies the maximum burst size (MBS)	26	12	17	6	integer

To configure traffic-shaping parameters for PPPoA via domain maps, use the **atm** command in Domain Map Configuration mode.

Related Documentation

- *Creating an IP Interface*

Mapping Application Terminate Reasons and RADIUS Terminate Codes Overview

The JunosE Software uses a default configuration that maps terminate reasons to RADIUS Acct-Terminate-Cause attributes. You can optionally create customized mappings between a terminate reason and a RADIUS Acct-Terminate-Cause attribute—these mappings enable you to provide different information about the cause of a termination.

When a subscriber's L2TP or PPP session is terminated, the router logs a message for the internal terminate reason and logs another message for the RADIUS Acct-Terminate-Cause attribute (RADIUS attribute 49). RADIUS attribute 49 is also included in RADIUS Acct-Off and Acct-Stop messages. You can use the logged information to help monitor and troubleshoot terminated sessions.

Use the **show terminate-code** command to display information about the mappings between application terminate reasons and RADIUS Acct-Terminate-Cause attributes.

Table 7 on page 26 lists the IETF RADIUS Acct-Terminate-Cause codes that you can use to map application terminate reasons. In addition, you can also configure and use proprietary codes for values beyond 22.

Table 7: Supported RADIUS Acct-Terminate-Cause Codes

Code	Name	Description
1	User Request	User initiated the disconnect (log out)
2	Lost Carrier	DCD was dropped on the port
3	Lost Service	Service can no longer be provided; for example, the user's connection to a host was interrupted
4	Idle Timeout	Idle timer expired
5	Session Timeout	Subscriber reached the maximum continuous time allowed for the service or session
6	Admin Reset	System administrator reset the port or session
7	Admin Reboot	System administrator terminated the session on the NAS; for example, prior to rebooting the NAS
8	Port Error	NAS detected an error on the port that required ending the session
9	NAS Error	NAS detected an error (other than on the port) that required ending the session
10	NAS Request	NAS ended the session for a non-error reason
11	NAS Reboot	NAS ended the session due to a non-administrative reboot
12	Port Unneeded	NAS ended the session because the resource usage fell below the low threshold; for example, the bandwidth-on-demand algorithm determined that the port was no longer needed
13	Port Preempted	NAS ended the session to allocate the port to a higher-priority use
14	Port Suspended	NAS ended the session to suspend a virtual session
15	Service Unavailable	NAS was unable to provide the requested service
16	Callback	NAS is terminating the current session in order to perform callback for a new session
17	User Error	An error in the user input caused the session to be terminated
18	Host Request	The login host terminated the session normally
19	Supplicant Restart	Supplicant state machine was reinitialized
20	Reauthentication Failure	A previously authenticated supplicant failed to reauthenticate successfully following expiration of the reauthentication timer or explicit reauthentication request by management action

Table 7: Supported RADIUS Acct-Terminate-Cause Codes *(continued)*

Code	Name	Description
21	Port Reinitialized	The port's MAC has been reinitialized
22	Port Administratively Disabled	The port has been administratively disabled

Related Documentation

- *Configuring Custom Mappings for PPP Terminate Reasons*

CHAPTER 6

PPP Accounting Statistics

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 the *PPP Accounting Statistics Overview* section in *JunosE Link Layer Configuration Guide* .

Related Documentation

- Application Support for Stateful Line Module Switchover on page 17
- *Collecting Accounting Statistics*
- *RADIUS IETF Attributes Supported for Subscriber AAA Accounting Messages*

CHAPTER 7

How L2TP Dial-Out Works

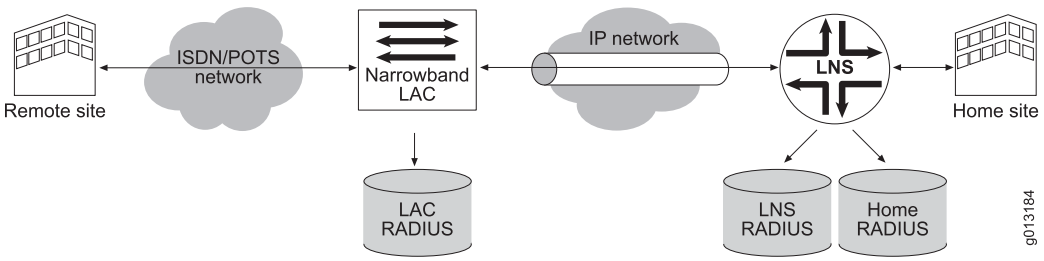
L2TP Dial-Out Overview

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

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

Figure 3 on page 31 shows the dial-out model in which the LNS initiates L2TP sessions and provides enough information to the narrowband LAC so that it can complete the dial-out from the home site to the remote site.

Figure 3: Network Model for Dial-Out



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

Related Documentation

- L2TP Overview on page 3
- *L2TP Dial-Out Terms*
- L2TP Dial-Out Network Model on page 32
- L2TP Dial-Out Operational States on page 34
- L2TP Dial-Out Process on page 33
- L2TP Dial-Out Outgoing Call Setup Details on page 37

L2TP Dial-Out Platform Considerations

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

For information about the modules supported on E Series routers:

- See the *ERX Module Guide* for modules supported on ERX7xx models, ERX14xx models, and the ERX310 Broadband Services Router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 and E320 Broadband Services Routers.

Related Documentation

- L2TP Dial-Out Overview on page 31
- L2TP Dial-Out Network Model on page 32

L2TP Dial-Out References

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

Related Documentation

- L2TP Dial-Out Overview on page 31
- L2TP Dial-Out Network Model on page 32

L2TP Dial-Out Network Model

In the figure in "L2TP Dial-Out Overview" on page 31, the home site connects to the Internet over a permanent leased line to the Internet service provider's (ISP's) E Series LNS. The ISP uses an IP network to connect the LNS to the narrowband access point of the network where the narrowband LAC exists. The narrowband LAC connects to a narrowband network (ISDN) that the remote site is also connected to.

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

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

Related Documentation

- L2TP Dial-Out Overview on page 31
- *L2TP Dial-Out Terms*
- L2TP Dial-Out Operational States on page 34
- L2TP Dial-Out Process on page 33
- L2TP Dial-Out Outgoing Call Setup Details on page 37

L2TP Dial-Out Process

The following is the dial-out process used in the network model illustrated in "L2TP Dial-Out Overview" on page 31:

1. The router receives a trigger packet.
2. The router builds a RADIUS Access-Request message and sends it to the RADIUS server that is associated with the virtual router on which the dial-out route is defined—typically, the RADIUS home server.
3. The RADIUS server's response to the Access-Request is similar to the response used for LAC incoming calls. Notable differences are that the IP addresses of the peer are interpreted as LAC addresses instead of LNS addresses. In addition, narrowband details, such as calling numbers, are returned.
4. The LNS makes the outgoing call using a load-balancing or round-robin mechanism identical to the one that the E Series LAC uses for incoming calls. The LAC may also employ the LAC RADIUS in tunnel authentication.
5. Once the LNS successfully completes a control connection and session with the LAC, the LAC performs the actual narrowband dial-out operation to the remote site using the information passed by the LNS during session setup.
6. A PPP session is started on the remote customer premises equipment (CPE), and mutual PPP authentication is performed at the remote CPE and the LNS as follows:
   a. The LNS uses the LNS RADIUS server to validate the remote CPE's PPP session, while the CPE can use its own RADIUS server to validate the LNS's PPP session.
   b. The LNS uses the username and password that is returned in the first Access-Accept message.
7. Once authentication is successful, an IP interface is built on top of the PPP interface at the LNS. Internet Protocol Control Protocol (IPCP) is negotiated, and the framed route that RADIUS returns as a result of the PPP authentication supersedes the dial-out route.

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

Related Documentation

- L2TP Dial-Out Overview on page 31
- *L2TP Dial-Out Terms*
- L2TP Dial-Out Network Model on page 32
- L2TP Dial-Out Operational States on page 34
- L2TP Dial-Out Outgoing Call Setup Details on page 37

L2TP Dial-Out Operational States

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

Chassis

Table 8 on page 34 describes the operational states of the chassis.

Table 8: Chassis Operational States

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

Virtual Router

Table 9 on page 34 describes the operational states of the virtual router.

Table 9: Virtual Router Operational States

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

Targets

Table 10 on page 35 describes the operational states of the targets.

Table 10: Target Operational States

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

Sessions

Table 11 on page 35 describes operational states of the sessions.

Table 11: Session Operational States

State	Description
authenticating	New sessions start in the authenticating state. In this state, the dial-out state machine has received a valid trigger and is waiting for authentication, authorization, and accounting (AAA) to complete the initial authentication. On getting a grant from AAA, the session transitions to the connecting state. Alternatively, on getting a deny from AAA, the session transitions to the inhibited state.
connecting	Sessions enter the connecting state when authentication is complete. In this state, the dial-out state machine has initiated an outgoing L2TP call. On entering this state, the session-connecting timer is set to the chassis-wide trigger timer value. The session stays in this state until either the outgoing call is successful or the connecting timer expires. Any new trigger packets received for this session when it is in the connecting state are discarded.
inService	A session enters the inService state from the connecting state on successful completion of the dial-out call request. The session stays in this state until the outgoing call is closed.

Table 11: Session Operational States *(continued)*

State	Description
inhibited	A session enters the inhibited state from the connecting state when the connecting timer expires (that is, the outgoing call was unsuccessful). This state prevents the router from thrashing on an outgoing call that cannot be completed. When in this state, the router discards all trigger packets received for the session. The inhibited timer controls the amount of time spent in this state. The setting of the inhibited timer varies depending on whether the session is entering the inhibited state for the first time or is reentering the state. • If it is the first time, the inhibited timer is initialized to the chassis-wide trigger value. • If it is reentering the state, the inhibited timer is initialized to 2 times the previous value of the inhibited timer, up to a maximum of 8 times the chassis-wide trigger value. For example, if the chassis-wide trigger value is 30 seconds, the setting of the inhibited timer within the session (on subsequent immediate reentries; see postInhibited state) is 30, 60, 120, 240. Since 240 is 8 x 30, the inhibited timer for this session is never set larger than 240 seconds.
postInhibited	A session enters the postInhibited state after completion of an inhibited state. The inhibited timer is reused to control the amount of time the session stays in postInhibited state. In this state the timer repeatedly times out and reduces the inhibited timer by a factor of 2 on each iteration. Once the inhibited timer reaches zero, the session transitions to dormant. The receipt of a trigger in this state results in a transition to the authenticating state.
dormant	A session enters the dormant state after completion of a postInhibited state. The dormant timer is initialized to the chassis-wide dormant timer value, minus the time the session spent in the postInhibited state. Receipt of a new trigger packet transitions the session to the authenticating state. If the dormant timer expires, the session is deleted. The dormant state exists to allow analysis of a dial-out session before it is deleted.
pending	A session enters the pending state when a valid trigger is received but there already are the maximum number of connecting sessions in the router. The router discards all subsequent trigger packets until other sessions transition out of the connecting state. When this happens, pending sessions can transition to the dormant state.
failed	A session enters the failed state when the router detects a configuration error that prevents the successful operation of the session. Specifically, one of the final steps in a dial-out request is mutual PPP authentication at the LNS. A side-effect of authentication is the installation of an access route for the outgoing call. If the access route does not correspond to the trigger packet (that is, the trigger packet cannot be routed successfully by the new access route), the router detects this discrepancy as a configuration error because trigger packets that arrive are not forwarded into the outgoing call; rather, they are buffered or discarded. The only way to exit the failed state is with the **l2tp dial-out session reset** command.

Related Documentation

- L2TP Dial-Out Overview on page 31
- *L2TP Dial-Out Terms*
- L2TP Dial-Out Network Model on page 32
- L2TP Dial-Out Process on page 33
- L2TP Dial-Out Outgoing Call Setup Details on page 37

L2TP Dial-Out Outgoing Call Setup Details

This section details the process described in "L2TP Dial-Out Process" on page 33.

Access-Request Message

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

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

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

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

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

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

Access-Accept Message

The router expects RADIUS attributes that define a tunnel to be returned with the additions in Table 12 on page 37. If tunnel attributes are excluded from the Access-Accept message or the returned Service-Type attribute is not set to outbound, the dial-out session is denied.

Table 12: Additions to RADIUS Attributes in Access-Accept Messages

Attribute Number	Attribute Name	Content
6	Service-Type	Outbound
67	Tunnel-Server-Endpoint	IP address of LAC
Juniper VSA 26-35	Tunnel-Dialout-Number	L2TP dial-out number

Table 12: Additions to RADIUS Attributes in Access-Accept Messages *(continued)*

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

Outgoing Call

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

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

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

Mutual Authentication

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

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

Route Installation

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

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

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

Related Documentation

- L2TP Dial-Out Overview on page 31
- *L2TP Dial-Out Terms*
- L2TP Dial-Out Network Model on page 32
- L2TP Dial-Out Operational States on page 34
- L2TP Dial-Out Process on page 33

PART 2

Configuration

CHAPTER 8

Configuration Tasks for LNS

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 Documentation

- virtual-router on page 121
- ip router-id on page 92

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 **virtual-router** 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 46.

   ```
   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 47.

   ```
   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 the LNS override out-of-resource result codes 4 and 5 with code 2 for interoperation with third-party implementations that do not support codes 4 and 5.

   ```
   host1:boston(config-l2tp-dest-profile-host)#session-out-of-resource-result-code-override
   ```

10. (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 the *Using DNIS* section in *Mapping a User Domain to a Virtual Router Overview*.

Related Documentation

- Creating an L2TP Destination Profile on page 46
- Creating an L2TP Host Profile on page 47
- Configuring the Maximum Number of LNS Sessions on page 47
- Configuring the RADIUS Connect-Info Attribute on the LNS on page 51
- Overriding LNS Out-of-Resource Result Codes 4 and 5 on page 8
- Selecting Service Modules for LNS Sessions Using MLPPP on page 55
- **bundled-group-id on page 85**
- **bundled-group-id-overrides-mlppp-ed on page 86**
- **default-upper-type mlppp on page 87**

- disable proxy lcp on page 88
- enable proxy authenticate on page 90
- l2tp destination profile on page 93
- local host on page 101
- local ip address on page 102
- max-sessions on page 104
- radius connect-info-format on page 105
- remote host on page 116
- session-out-of-resource-result-code-override on page 118
- tunnel password on page 119

Creating an L2TP Destination Profile

You can 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 **l2tp destination profile** 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:

- Issue the **l2tp destination profile** command in Global Configuration mode.

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

Use the **no** version to delete the L2TP destination 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 are dropped.

Related Documentation

- *L2TP/IPsec Tunnels Overview*
- *Configuring an L2TP Destination Profile to Enable IPsec Support for L2TP Tunnels*
- *Configuring Single-Shot L2TP/IPsec Tunnels*

- Creating an L2TP Host Profile on page 47
- l2tp destination profile on page 93

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 Documentation

- Creating an L2TP Destination Profile on page 46
- l2tp destination profile on page 93

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 Documentation

- max-sessions on page 104

Configuring Groups for LNS Sessions

You can define and configure session limit groups under the L2TP destination profile. Under each destination profile, you can define a maximum of 4096 session limit groups.

The maximum session limit is applied for each of the session limit groups in L2TP Destination Profile Sessions Limit Group Configuration mode.

NOTE: The **max-sessions** command is also supported in L2TP Destination Profile Configuration mode and L2TP Destination Profile Host Configuration mode.

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 session count is less than the configured limit, the LNS then performs the same check on the L2TP destination sessions limit profile. If no limit is set, or if the current session limit is less than the configured limit, the LNS then performs the same check on the L2TP destination host profile limit. If no limit is set, or if the current session count is also less than the L2TP destination host profile limit, then the new session can be established. If a session request exceeds any of the maximum sessions settings, the LNS rejects the session.

To set the maximum sessions allowed for a group for the specified destination, use the **max-sessions** command in L2TP Destination Profile Sessions Limit Group Configuration mode. You can configure this as follows:

1. Define an L2TP destination profile.

```
host1(config)#l2tp destination profile abc virtual-router default ip address 10.10.10.1
```

2. Define a session limit group in L2TP Destination Profile Configuration mode.

   host1(config-l2tp-dest-profile)#sessions-limit-group g1

3. Define the maximum number of sessions allowed in the group.

   host1(config-l2tp-dest-profile-sessions-limit-group)#max-sessions 8000

4. To view the output, use the **show l2tp destination profile** command.

   host1#show l2tp destination profile abc

To set the maximum sessions allowed for a group for the specified host, use the **max-sessions** command in L2TP Destination Profile Sessions Limit Group Configuration mode. You can configure this as follows:

1. Configure a remote host name.

   host1(config-l2tp-dest-profile)#remote host xyz

2. Assign a sessions limit group name for the remote host.

   host1(config-l2tp-dest-profile-host)#sessions-limit-group g1

   NOTE: **Ensure that the group name is already defined under the destination profile.**

3. To view the output, use the **show l2tp destination profile** command.

   host1#show l2tp destination profile abc

Related Documentation

- Configuring the Maximum Number of LNS Sessions on page 47
- max-sessions on page 104
- sessions-limit-group on page 117

CHAPTER 9

Configuration Tasks for TX Speed and RX Window Sizes

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 Documentation

- radius connect-info-format on page 105

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* . 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 *Subscriber*

AAA Access Messages Overview. For more information about the L2tp-Recv-Window-Size attribute, see *RADIUS IETF Attributes*.

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
   ```

CHAPTER 10

Bundled LNS Sessions

Selecting Service Modules for LNS Sessions Using MLPPP

You can install multiple 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 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 ERX1440 Broadband Services Router has 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 service modules installed in the router have available space.

For more information about endpoint discriminators, see the *Configuring Multilink PPP* chapter in *JunosE Link Layer Configuration Guide*.

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 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 Documentation

- bundled-group-id on page 85
- bundled-group-id-overrides-mlppp-ed on page 86

CHAPTER 11

Configuring L2TP Tunnels on LNS

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 Documentation

- l2tp tunnel-switching on page 97

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 Documentation

- l2tp tunnel idle-timeout on page 99

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 Documentation

- l2tp tunnel test on page 100

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 59.

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 page 57.
- 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 61.
   - 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 62.
   - 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 63.
   - 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 62.

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 57.

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 .*

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* .

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 *Subscriber AAA Access Messages Overview*. For more information about the Tunnel-Switch-Profile attribute, see *RADIUS IETF Attributes*.

Related Documentation

- Enabling Tunnel Switching on the Router on page 60
- Configuring L2TP Tunnel Switch Profiles on page 60
- Applying L2TP Tunnel Switch Profiles by Using AAA Domain Maps on page 61
- Applying L2TP Tunnel Switch Profiles by Using AAA Tunnel Groups on page 62
- Applying Default L2TP Tunnel Switch Profiles on page 62
- Applying L2TP Tunnel Switch Profiles by Using RADIUS on page 63
- **aaa tunnel switch-profile on page 82**
- **avp on page 84**
- **l2tp switch-profile on page 96**
- **l2tp tunnel-switching on page 97**

CHAPTER 12

Configuration Task for L2TP Disconnect-Cause Code

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.

1. Generating the Disconnect Cause AVP Globally on page 65
2. Generating the Disconnect Cause AVP with a Host Profile on page 66
3. Enabling RADIUS Accounting for Disconnect Cause on page 66
4. Displaying Disconnect Cause Statistics on page 66

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

CHAPTER 13

Peer Resynchronization Methods for Failover

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.

NOTE: If an LNS device at one end of an L2TP tunnel encounters a failure and is not configured with the L2TP peer resynchronization method to enable the LNS device to resynchronize with the non-failed endpoint peer (the LAC device at the other end of the tunnel), the tunnel is brought down immediately after the configured value for the number of retransmission attempts is exceeded. The tunnel between the LAC device and the failed LNS device that is recovering is not preserved for the default recovery time period, which is 15 minutes. Instead, the tunnel is terminated immediately and the LAC device sends the Failover Capability attribute-value pair (AVP) in the Stop-Control-Connection-Notification (StopCCN) packet to the original address with a failover recovery time field set to zero.

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

1. Configuring Peer Resynchronization for L2TP Host Profiles and AAA Domain Map Tunnels on page 68
2. Configuring the Global L2TP Peer Resynchronization Method on page 69
3. Using RADIUS to Configure Peer Resynchronization on page 70

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 13 on page 71 describes the L2TP-Resynch-Method RADIUS attribute. For more information about RADIUS Access-Accept messages, see *Subscriber AAA Access Messages Overview*. For more information about the L2TP-Resynch-Method attribute, see *RADIUS IETF Attributes*.

Table 13: 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

CHAPTER 14

Transmit Connect Speed Method for L2TP Sessions

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 77.
- 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 78.
- 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 79.
- 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 79.

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 the *Connection Admission Control* section in *JunosE Link Layer Configuration Guide* .

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*.

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 74 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 14 on page 76 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 14: 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 15 on page 76 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 15: 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.

Table 15: Transmit Connect Speeds for L2TP over Ethernet Example *(continued)*

Calculation Method	Transmit Connect Speed Reported in AVP 24	Reason
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 *AAA 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 .*

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*.

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 the *Configuring Virtual Routers* chapter in *JunosE System Basics Configuration Guide*.

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 78:
     - **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 16 on page 80 describes the Tunnel-Tx-Speed-Method RADIUS attribute. For more information about RADIUS Access-Accept messages, see *Subscriber AAA Access Messages Overview*. For a description of the RADIUS attributes supported by JunosE Software, see *RADIUS IETF Attributes*.

Table 16: 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 Documentation

- Transmit Connect Speed Calculation Methods on page 74
- Using AAA Domain Maps to Configure the Transmit Connect Speed Calculation Method on page 77
- Using AAA Tunnel Groups to Configure the Transmit Connect Speed Calculation Method on page 78
- Using AAA Default Tunnel Parameters to Configure the Transmit Connect Speed Calculation Method on page 79
- Using RADIUS to Configure the Transmit Connect Speed Calculation Method on page 80
- **aaa tunnel tx-connect-speed-method on page 83**
- **tx-connect-speed-method on page 120**

CHAPTER 15

Configuration Commands

aaa tunnel switch-profile

Syntax aaa tunnel switch-profile *profileName*

no aaa tunnel switch-profile

Release Information Command introduced in JunosE Release 7.2.0.

Description Applies a default L2TP tunnel switch profile to a virtual router. The default tunnel switch profile defines the L2TP tunnel switching behavior for the interfaces to which this profile is assigned. 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 **no** version removes the default tunnel switch profile assignment from the virtual router.

Options

- *profileName*—Name of the default tunnel switch profile; a string of up to 64 alphanumeric characters

Mode Global Configuration

aaa tunnel tx-connect-speed-method

Syntax aaa tunnel tx-connect-speed-method { static-layer2 | dynamic-layer2 | qos | actual }

no aaa tunnel tx-connect-speed-method

Release Information Command introduced in JunosE Release 8.0.0.

Description Configures the method used to calculate the transmit connect speed of the subscriber's access interface for establishing a tunneled L2TP session associated with a virtual router. This speed is reported in L2TP Transmit (TX) Speed AVP 24. 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. The **no** version removes configuration of the transmit connect speed calculation method from the tunneled L2TP sessions associated with the virtual router.

Options

- static-layer2—Calculates the transmit connect speed of the subscriber's access interface based on statically configured settings for the underlying layer 2 interface
- dynamic-layer2—Calculates the transmit connect speed of the subscriber's access interface based on dynamically configured settings for the underlying layer 2 interface
- qos—Calculates the transmit connect speed of the subscriber's access interface based on settings determined by QoS
- actual—Calculates the transmit connect speed of the subscriber's access interface as the lesser of the **dynamic-layer2** value or the **qos** value

Mode Global Configuration

avp

Syntax avp *avpType action*

no avp *avpType*

Release Information Command introduced in JunosE Release 7.2.0.

Description Configures the L2TP tunnel switching behavior for a specified L2TP AVP type. The **no** version restores the default L2TP tunnel switching behavior for AVPs of the specified type.

Options

- *avpType*—One of the following L2TP AVPs
  - bearer-type—L2TP Bearer Type AVP 18; by default, the router regenerates this AVP at the outbound LAC session, based on the local policy that is 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 that is in effect
  - cisco-nas-port—Cisco NAS Port Info AVP 100; by default, the router drops this AVP
- *action*—One of the following actions that characterize the tunnel switching behavior; currently, only the **relay** action is supported
  - relay—Causes the router to preserve the value of an incoming AVP of the specified type when packets are switched between an inbound LNS session and an outbound LAC session

Mode L2TP Tunnel Switch Profile Configuration

bundled-group-id

Syntax [no] bundled-group-id *bundledGroupID*

Release Information Command introduced before JunosE Release 7.1.0.

Description Assigns a bundled group identifier when no endpoint discriminator is available for bundled sessions using an L2TP destination host profile. When multiple tunnel-service modules are installed in a router that is deployed as an LNS and the tunnel sessions carry MLPPP, the router can use the bundled group identifier when selecting a tunnel-service module for bundled sessions. The **no** version restores the default value, no assigned bundled group identifier.

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

Options

- *bundledGroupID*—Identifier for a bundled group in the range 0–4294967295

Mode L2TP Destination Profile Host Configuration

bundled-group-id-overrides-mlppp-ed

Syntax [no] bundled-group-id-overrides-mlppp-ed

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies that the router uses the bundled group identifier you assigned using the **bundled-group-id** command when selecting a tunnel-service module instead of any endpoint discriminator. The **no** version removes the override.

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

Mode L2TP Destination Profile Host Configuration

default-upper-type mlppp

Syntax default-upper-type mlppp

no default-upper-type

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies that L2TP creates an MLPPP interface for the current LNS session when full LCP proxy data is not available. The **no** version deletes the MLPPP specification.

Mode L2TP Destination Profile Host Configuration

disable proxy lcp

Syntax [no] disable proxy lcp

Release Information Command introduced before JunosE Release 7.1.0.

Description Disables the proxy LCP parameter for the remote host. The **no** version enables the proxy LCP parameter for the remote host.

Mode L2TP Destination Profile Host Configuration

disconnect-cause

Syntax [no] disconnect-cause

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables an E Series LNS to generate, for the L2TP session to which the L2TP host profile applies, a PPP Disconnect Cause Code attribute value pair (AVP) and include it in all L2TP Call-Disconnect-Notify (CDN) messages that it sends to an LAC. This action provides a mechanism for the LAC to obtain information about the cause of a session disconnection. The **no** version disables generation of the PPP Disconnect Cause Code AVP, which is the default setting.

Mode L2TP Destination Profile Host Configuration

enable proxy authenticate

Syntax [no] enable proxy authenticate

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures proxy authenticate for a remote host. The **no** version removes proxy authenticate configuration from the remote host.

Mode L2TP Destination Profile Host Configuration

failover-resync

Syntax failover-resync { failover-protocol | failover-protocol-fallback-to-silent-failover | silent-failover | disable | not-configured }

no failover-resync

Release Information Command introduced in JunosE Release 7.3.0.

Description Configures the L2TP peer resynchronization method that an L2TP failed endpoint uses to resynchronize with its peer non-failed endpoint. This command configures peer resynchronization for a host profile or a domain map tunnel, and overrides a global peer resynchronization method that is specified in Global Configuration mode. The **no** version restores the default setting, not-configured.

Options

- failover-protocol—Specifies the L2TP failover protocol method
- failover-protocol-fallback-to-silent-failover—Specifies the L2TP failover protocol method; however, if the peer does not support this method, the silent failover method is used
- silent-failover—Specifies the silent failover method
- disable—Disables peer resynchronization
- not-configured—Specifies that peer resynchronization is not configured for L2TP host profiles and AAA domain map tunnels. L2TP uses the global failover method; the default setting

Mode Domain Map Tunnel Configuration, L2TP Destination Profile Host Configuration

ip router-id

Syntax [no] ip router-id [*vrfName*] *ipAddress*

Release Information Command introduced before JunosE Release 7.1.0.

Description Establishes the IP address of a router. The **no** version removes the IP address assignment.

Options
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
- *ipAddress*—IP address of the router

Mode Global Configuration

Related Documentation
- *Configuring the Loopback Interface and Router ID for BGP for VPWS*
- *Configuring the Loopback Interface and Router ID for VPLS*

l2tp destination profile

Syntax l2tp destination profile { *profileName* [[virtual-router *vrName*] ip address *ipAddress*] | [virtual-router *vrName*] ip address *ipAddress* }

no l2tp destination profile { *profileName* | [virtual-router *vrName*] ip address *ipAddress* }

Release Information Command introduced before JunosE Release 7.1.0.

Description Creates or accesses a destination profile that defines the location of a LAC. The **no** version removes the L2TP destination profile.

Options

- *profileName*—Name of the L2TP destination profile
- *vrName*—Name of the virtual router to be used to reach the destination (that is, the LAC). If you do not specify a virtual router, the current virtual router context is used.
- *ipAddress*—IP address to be used to reach the destination

Mode Global Configuration

l2tp disconnect-cause

Syntax [no] l2tp disconnect-cause

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables an E Series LNS to generate, for all L2TP sessions, a PPP Disconnect Cause Code attribute value pair (AVP) and include it in all L2TP Call-Disconnect-Notify (CDN) messages that it sends to an LAC. This action provides a mechanism for the LAC to obtain information about the cause of a session disconnection. The **no** version disables generation of the PPP Disconnect Cause Code AVP, which is the default setting.

Mode Global Configuration

l2tp failover-resync

Syntax l2tp failover-resync { failover-protocol | failover-protocol-fallback-to-silent-failover | silent-failover | disable }

no l2tp failover-resync

Release Information Command introduced in JunosE Release 7.3.0.

Description Configures the global L2TP peer resynchronization method that an L2TP failed endpoint uses to resynchronize with its peer non-failed endpoint. This setting can be overridden by a peer resynchronization method that is configured by either an L2TP host profile or an AAA domain map tunnel configuration. The **no** version disables peer resynchronization. The **default** version restores the default peer resynchronization method, failover-protocol-fallback-to-silent-failover.

Options

- failover-protocol—Specifies the L2TP failover protocol method
- failover-protocol-fallback-to-silent-failover—Specifies the L2TP failover protocol method; however, if the peer does not support this method, the silent failover method is used; this is the default setting
- silent-failover—Specifies the silent failover method
- disable—Disables peer resynchronization

Mode Global Configuration

l2tp switch-profile

Syntax [no] l2tp switch-profile *profileName*

Release Information Command introduced in JunosE Release 7.2.0.

Description Creates and names an L2TP tunnel switch profile. This command accesses L2TP Tunnel Switch Profile Configuration mode, from which you can define the L2TP tunnel switching behavior for the interfaces to which this profile is assigned. The **no** version removes the named tunnel switch profile from the router.

Options
- *profileName*—Name of the tunnel switch profile; a string of up to 64 alphanumeric characters

Mode Global Configuration

l2tp tunnel-switching

Syntax [no] l2tp tunnel-switching

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables tunnel switching chassis-wide. The **no** version restores the default, disabling tunnel switching.

Mode Global Configuration

l2tp tunnel default-receive-window

Syntax l2tp tunnel default-receive-window *receiveWindowSize*

no l2tp tunnel default-receive-window

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures the default L2TP receive window size (RWS) for a tunnel on both the LAC and the LNS. The RWS is the number of packets that the peer can transmit without receiving an acknowledgment from the router. This command affects only those tunnels configured on the router after the command is issued; it has no effect on previously configured tunnels. The **no** version restores the default behavior, in which the router chooses the default RWS.

Options

- *receiveWindowSize*—Default receive window size, in packets; currently, the only supported value is 4

Mode Global Configuration

l2tp tunnel idle-timeout

Syntax l2tp tunnel idle-timeout [*timeOutValue*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures the tunnel idle-timeout value. Creates persistent tunnels by setting the value to 0. There is no **no** version.

Options
- *timeOutValue*—Number in the range 0–86400 seconds

Mode Global Configuration

l2tp tunnel test

Syntax l2tp tunnel test *authenticateName* [*tunnelName*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Allows you to force the establishment of a tunnel in order to verify the tunnel configuration and to verify connectivity. There is no **no** version.

Options
- *authenticateName*—Authenticate name used to look up tunnel test parameters
- *tunnelName*—Name of the tunnel to be tested

Mode Privileged Exec

local host

Syntax local host *hostname*

no local host

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures an L2TP local hostname to be used with a remote host. The **no** version removes the local hostname from use with a remote host.

Options
- *hostname*—L2TP local hostname; string of up to 64 characters (no spaces)

Mode L2TP Destination Profile Host Configuration

local ip address

Syntax From L2TP Destination Profile Host Configuration mode:

local ip address *ipAddress*

no local ip address

From IPsec Transport Profile Configuration mode:

[no] local ip address *transportIpAddress*

From IPsec Tunnel Profile Configuration mode:

local ip address *transportIpAddress* { pre-share *keyString*
| pre-share-masked *maskedKeyString* }

no local ip address

Release Information Command introduced before JunosE Release 7.1.0.
IPsec Tunnel Profile Configuration mode added in JunosE Release 7.3.0.

Description From L2TP Destination Profile Host Configuration mode, configures a local IP address for use with a remote host. The **no** version removes the local IP address from use with a remote host.

From IPsec Transport Profile Configuration mode, specifies the local endpoint of the IPsec transport connection. It also enters Local IPsec Transport Profile Configuration mode. The **no** version deletes the local IP address.

From IPsec Tunnel Profile Configuration mode, specifies the given local IP address as a server address. The router continues to monitor UDP port 500 for incoming user login requests (that is, IKE source address negotiations). When using global preshared keys, consider the following points:

- Global preshared keys enable a group of users to share a single authentication key. Using a shared key for a group of users simplifies the administrative job of setting up keys. However, changing or removing a preshared key for one user (for security reasons) affects other users with the same key.
- Specific keys for individual users take precedence over global keys assigned to the same user. In other words, if a user has both an assigned specific key and a global key that user must use the specific key or authentication fails.
- Avoid specifying the same local endpoint and virtual router in the same profile. Local endpoint and virtual router values override each other. The last value set in the profile is the value used.

The **no** version causes the router to stop monitoring UDP port 500 for user requests and removes any preshared key associations with the local IP address.

Options

- *ipAddress*—IP address used in packets sent to the LAC
- *transportIpAddress*—Local endpoint for the IPsec transport connection
- *keyString*—Key value in ASCII format
- *maskedKeyString*—Key value in ascii format

Mode IPsec Transport Profile Configuration, IPsec Tunnel Profile Configuration, L2TP Destination Profile Host Configuration

max-sessions

Syntax For RADIUS:

max-sessions *sessionLimit*

no max-sessions

For AAA domain map and tunnel group tunnels:

max-sessions *maxSessionsPerTunnel*

{ no | default } max-sessions

For L2TP:

max-sessions *maxSessionsPerProfile*

{ no | default } max-sessions

Release Information Command introduced before JunosE Release 7.1.0.

Description For RADIUS, specifies the number of outstanding requests to a server. The **no** version reverts to the default value.

For AAA domain map, and tunnel group tunnels , sets the maximum sessions per tunnel. The **no** version disables the feature. The **default** version sets the value to zero.

For L2TP, sets the maximum sessions allowed for destination and host profiles by the LNS. The **no** and **default** versions disable the feature.

Options

- *sessionLimit*—Maximum number of outstanding requests to a specific server in the range from 10 through to the maximum value; default value is 255

  For information about the number of concurrent RADIUS requests that the router supports for authentication and accounting servers, see *JunosE Release Notes*, *Appendix A*, *System Maximums*.

- *maxSessionsPerTunnel*—Maximum number of sessions that can be configured on a tunnel in the range 0–4294967295; default value is zero

- *maxSessionsPerProfile*—Maximum number of sessions that can be established at the LNS for a destination or host profile; in the range from 1 through to a maximum of the chassis-wide limit; default value is the chassis-wide limit

  For information about the maximum number of L2TP sessions supported per chassis, see *JunosE Release Notes*, *Appendix A*, *System Maximums*.

Mode Domain Map Tunnel Configuration, L2TP Destination Profile Configuration, L2TP Destination Profile Host Configuration, RADIUS Configuration, Tunnel Group Tunnel Configuration, L2TP Destination Profile Sessions Limit Configuration, L2TP Destination Profile Host Sessions Limit Configuration

radius connect-info-format

Syntax radius connect-info-format { l2tp-connect-speed | l2tp-connect-speed-rx-when-equal }

no radius connect-info-format

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the format and enables the generation of RADIUS attribute 77, Connect-Info, on the LNS. The format uses the received L2TP connect-speed AVPs that the LAC sends to the LNS. The **no** version restores the default, in which the LNS does not generate the Connect-Info attribute.

Options

- l2tp-connect-speed—Specifies that the Connect-Info attribute include only the RX speed when the RX speed is different from the TX speed and is greater than zero.
- l2tp-connect-speed-rx-when-equal—Specifies that the Connect-Info attribute always include the RX speed when the speed is greater than zero.

Mode Global Configuration

radius include

Syntax

radius include *attributeName*
{ access-request | acct-on | acct-off | acct-start | acct-stop } { enable | disable }

no radius include *attributeName*
{ access-request | acct-on | acct-off | acct-start | acct-stop }

Release Information

Command introduced before JunosE Release 7.1.0.
l2c-access-loop-parameters attribute added in JunosE Release 7.2.0.
l2cd attributes added in JunosE Release 9.0.0.
framed-interface-id and **framed-ipv6-prefix** attributes, and acct-stop support for **framed-ip-addr** attribute added in JunosE Release 9.0.0.
downstream-calculated-qos-rate and **upstream-calculated-qos-rate** attributes added in JunosE Release 9.1.0.
ipv6-accounting, **delegated-ipv6-prefix**, **framed-ipv6-pool**, **framed-ipv6-route**, **ipv6-local-interface**, **ipv6-nd-ra-prefix**, **ipv6-primary-dns**, **ipv6-secondary-dns**, and **ipv6-virtual-router** attributes added in JunosE Release 10.2.0.
icr-partition-id attribute added in JunosE Release 10.3.0.
framed-route attribute added in JunosE Release 11.3.0.
ipv6-egress-policy-name and **ipv6-ingress-policy-name** attributes added in JunosE Release 13.0.0.
dhcp-option82-circuitid and **dhcp-option82-remoteid** attributes added in JunosE Release 13.1.0.
qos-profile-name, ds-lite-tunnel-name, and **pcp-server-name** attributes added in JunosE Release 13.2.0.

Description

Configures the inclusion of RADIUS attributes in RADIUS messages. Not all attributes are available in all message types. The listed attributes are included by default except where noted. The **no** version restores the default.

Options

- *attributeName*—One of the following RADIUS attributes; not all attributes are available in all message types.

  Attributes available for Access-Request, Acct-Start, and Acct-Stop messages:

  - acct-multi-session-id—Includes RADIUS attribute 50, Acct-Multi-Session-Id
  - acct-tunnel-connection—Includes RADIUS attribute 68, Acct-Tunnel-Connection
  - ascend-num-in-multilink—Includes RADIUS attribute 188, Ascend-Num-In-Multilink
  - called-station-id—Includes RADIUS attribute 30, Called-Station-Id
  - calling-station-id—Includes RADIUS attribute 31, Calling-Station-Id
  - connect-info—Includes RADIUS attribute 77, Connect-Info
  - dhcp-options—Includes RADIUS attribute 26-55, DHCP-Options
  - dhcp-option82—Includes RADIUS attribute 26–159, DHCP-Option 82
  - dhcp-option82-circuitid—Includes RADIUS attribute 26–1, DHCP-Option 82

- dhcp-option82-remoteid—Includes RADIUS attribute 26–2, DHCP-Option 82
- dhcp-gi-address—Includes RADIUS attribute 26-57, DHCP-GI-Address
- dhcp-mac-address—Includes RADIUS attribute 26-56, DHCP-MAC Address
- downstream-calculated-qos-rate—Excluded by default; includes RADIUS attribute 26-141, Downstream-Calculated-Qos-Rate
- framed-interface-id—Excluded by default; includes RADIUS attribute 96, Framed-Interface-Id, if an IPv6 interface ID is assigned to the subscriber
- framed-ip-addr—Includes RADIUS attribute 8, Framed-IP-Address, if an IP address is assigned to the subscriber
- framed-ipv6-prefix—Excluded by default; includes RADIUS attribute 97, Framed-Ipv6-Prefix, if at least one IPv6 prefix is assigned to the subscriber
- icr-partition-id—Excluded by default; includes RADIUS attribute 26-150, ICR-Partition-Id, which is a user-configured value of up to 128 characters
- interface-description—Excluded by default; includes RADIUS attribute 26-63, Interface-Desc; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2c-downstream-data—Excluded by default; includes RADIUS attribute 26-92, L2C-Down-Stream-Data
- l2c-upstream-data—Excluded by default; includes RADIUS attribute 26-93, L2C-Up-Stream-Data
- l2cd-acc-loop-cir-id—Excluded by default; includes RADIUS attribute 26-110, Acc-Loop-Cir-Id; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-acc-aggr-cir-id-bib—Excluded by default; includes RADIUS attribute 26-111, Acc-Aggr-Cir-Id-Bin; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-acc-aggr-cir-id-asc—Excluded by default; includes RADIUS attribute 26-112, Acc-Aggr-Cir-Id-Asc; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-act-data-rate-up—Excluded by default; includes RADIUS attribute 26-113, Act-Data-Rate-Up; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-act-data-rate-dn—Excluded by default; includes RADIUS attribute 26-114, Act-Data-Rate-Dn; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-min-data-rate-up—Excluded by default; includes RADIUS attribute 26-115, Min-Data-Rate-Up; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-min-data-rate-dn—Excluded by default; includes RADIUS attribute 26-116, Min-Data-Rate-Dn; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages

- l2cd-att-data-rate-up—Excluded by default; includes RADIUS attribute 26-117, Att-Data-Rate-Up; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-att-data-rate-dn—Excluded by default; includes RADIUS attribute 26-118, Att-Data-Rate-Dn; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-max-data-rate-up—Excluded by default; includes RADIUS attribute 26-119, Max-Data-Rate-Up; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-max-data-rate-dn—Excluded by default; includes RADIUS attribute 26-120, Max-Data-Rate-Dn; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-min-lp-data-rate-up—Excluded by default; includes RADIUS attribute 26-121, Min-LP-Data-Rate-Up; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-min-lp-data-rate-dn—Excluded by default; includes RADIUS attribute 26-122, Min-LP-Data-Rate-Dn; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-max-interlv-delay-up—Excluded by default; includes RADIUS attribute 26-123, Max-Interlv-Delay-Up; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-act-interlv-delay-up—Excluded by default; includes RADIUS attribute 26-124, Act-Interlv-Delay-Up; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-max-interlv-delay-dn—Excluded by default; includes RADIUS attribute 26-125, Max-Interlv-Delay-Dn; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-act-interlv-delay-dn—Excluded by default; includes RADIUS attribute 26-126, Act-Interlv-Delay-Dn; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-dsl-line-state—Excluded by default; includes RADIUS attribute 26-127, DSL-Line-State; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- l2cd-dsl-type—Excluded by default; includes RADIUS attribute 26-128, DSL-Type; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- mlppp-bundle-name—Excluded by default; includes RADIUS attribute 26-62, MLPPP-Bundle-Name; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- nas-port—Includes RADIUS attribute 5, NAS-Port
- nas-port-id—Includes RADIUS attribute 87, NAS-Port-Id

NOTE: For subscribers connected over the link aggregation group (LAG) interface in DHCP standalone authenticate mode, RADIUS uses the LAG interface ID for the Nas-Port-Id attribute.

- nas-port-type—Includes RADIUS attribute 61, NAS-Port-Type

NOTE: For subscribers connected over the LAG interface in DHCP standalone authenticate mode, RADIUS calculates the value of the Nas-Port-Type attribute.

- pppoe-description—Includes RADIUS attribute 26-24, Pppoe-Description
- profile-service-description—Includes RADIUS attribute 26-53, Service-Description
- tunnel-client-auth-id—Includes RADIUS attribute 90, Tunnel-Client-Auth-Id
- tunnel-client-endpoint—Includes RADIUS attribute 66, Tunnel-Client-Endpoint
- tunnel-interface-id—Excluded by default; includes RADIUS attribute 26-44, Tunnel-Interface-ID
- tunnel-medium-type—Includes RADIUS attribute 65, Tunnel-Medium-Type
- tunnel-server-attributes—Excluded by default; includes all supported tunnel server attributes; that is, the attributes of the tunnel client when PPP is terminated at the LNS on the router
- tunnel-server-auth-id—Includes RADIUS attribute 91, Tunnel-Server-Auth-Id
- tunnel-server-endpoint—Includes RADIUS attribute 67, Tunnel-Server-Endpoint
- tunnel-type—Includes RADIUS attribute 64, Tunnel-Type
- upstream-calculated-qos-rate—Excluded by default; includes RADIUS attribute 26-142, Upstream-Calculated-Qos-Rate

Attributes available for Access-Request messages only:

- access-loop-parameters—Excluded by default; includes RADIUS attribute 26-81, L2c-Information

Attributes available for Acct-Start and Acct-Stop messages only:

- acct-link-count—Includes RADIUS attribute 51, Acct-Link-Count
- class—Includes RADIUS attribute 25, Class
- ds-lite-tunnel-name —Excluded by default; includes RADIUS attribute 144, DS-Lite-Tunnel-Name; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- egress-policy-name—Includes RADIUS attribute 26-11, Egress-Policy-Name
- framed-compression—Includes RADIUS attribute 13, Framed-Compression

- framed-ip-netmask—Includes RADIUS attribute 9, Framed-IP-Netmask
- framed-route—Excluded by default; includes RADIUS attribute 22, Framed-Route
- ingress-policy-name—Includes RADIUS attribute 26-10, Ingress-Policy-Name
- tunnel-assignment-id—Includes RADIUS attribute 82, Tunnel-Assignment-Id
- tunnel-preference—Includes RADIUS attribute 83, Tunnel-Preference
- ipv6-ingress-policy-name—Includes RADIUS attribute 26-106, Ipv6-Ingress-Policy-Name; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- ipv6-egress-policy-name—Includes RADIUS attribute 26-107, Ipv6-Egress-Policy-Name; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- pcp-server-name—Excluded by default; includes RADIUS attribute 26-165, PCP-Server-Name; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages
- qos-profile-name—Excluded by default; includes RADIUS attribute 26-26, QoS-Profile-Name; attribute automatically included in Interim-Acct messages when included in Acct-Stop messages

NOTE:

- The QoS profile names configured through the SRC software and CLI are not included in the RADIUS accounting messages. Only the profile name received from the RADIUS server in the Access-Accept messages is included in the RADIUS accounting messages.
- The QoS profile name configured locally is not sent in the authentication Access-Request messages.
- The QoS profile name returned by the RADIUS server is sent in the subsequent RADIUS accounting messages even after the QoS profile name configured through RADIUS is overridden with the QoS profile name configured through the CLI; this is a limitation.

Attributes available for Acct-Stop messages only:

- delegated-ipv6-prefix—Excluded by default; includes RADIUS attribute 123, Delegated-Ipv6-Prefix
  - The attribute value received from the RADIUS server in the Access-Accept message is used in the accounting messages
  - When prefix delegation occurs, an immediate-update (if enabled) message, which contains the delegated prefix information, is sent to the RADIUS server
  - When the prefix to be delegated to clients is obtained from the IPv6 local address server and not the RADIUS server and the **aaa dhcpv6-delegated-prefix delegated-ipv6-prefix** command is configured, the delegated prefix is sent to the

RADIUS server in this attribute in the immediate accounting, Acct-Stop, or Interim-Acct messages

- When the prefix to be delegated to clients is allocated from the IPv6 local address server and the **aaa dhcpv6-delegated-prefix delegated-ipv6-prefix** command is not configured, the delegated prefix is sent to the RADIUS server in the Framed-Ipv6-Prefix attribute in the immediate accounting, Acct-Stop, or Interim-Acct messages
- For static interfaces, although the prefix configured using the CLI command is used for DHCPv6 Prefix Delegation instead of the value returned by the RADIUS server, the immediate accounting, Acct-Stop, or Interim-Acct messages contain the prefix returned from the RADIUS server
- If this attribute is not returned from the RADIUS server, the immediate accounting, Acct-Stop, or Interim-Acct messages do not report this attribute

- framed-ipv6-pool—Excluded by default; includes RADIUS attribute 100, Framed-IPv6-Pool; the attribute value received from the RADIUS server in the Access-Accept message is used in the accounting messages; if this attribute is configured in the AAA domain map using the CLI and is not returned from RADIUS server, the Acct-Start, Acct-Stop, or Interim-Acct messages report the value configured in the domain map
- framed-ipv6-route—Excluded by default; includes RADIUS attribute 99, Framed-IPv6-Route; the attribute value received from the RADIUS server in the Access-Accept message is used in the accounting messages; when this attribute is not returned from the RADIUS server in the Access-Accept message, the immediate accounting, Acct-Stop, or Interim-Acct messages do not report this attribute
- input-gigapkts—Includes RADIUS attribute 26-35, Acct-Input-Gigapackets
- input-gigawords—Includes RADIUS attribute 52, Acct-Input-Gigawords
- ipv6-accounting—Excluded by default; automatically included in Interim-Acct messages when included in Acct-Stop messages; includes the following RADIUS attributes:
  - IPv6-Acct-Input-Octets [26-151]
  - IPv6-Acct-Output-Octets [26-152]
  - IPv6-Acct-Input-Packets [26-153]
  - IPv6-Acct-Output-Packets [26-154]
  - IPv6-Acct-Input-Gigawords [26-155]
  - IPv6-Acct-Output-Gigawords [26-156]
- ipv6-local-interface—Excluded by default; includes RADIUS attribute 26-46, Ipv6-Local-Interface; the attribute value received from the RADIUS server in the Access-Accept message is used in the accounting messages; if IPv6 local interface is configured in the AAA domain map and is not returned from the RADIUS server, the Acct-Start, Acct-Stop, or Interim-Acct messages report the value configured in the domain map

- ipv6-nd-ra-prefix—Excluded by default; includes RADIUS attribute 26-129, Ipv6-NdRa-Prefix; the attribute value received from the RADIUS server in the Access-Accept message is included in the accounting messages; for dynamic interfaces, if the Ipv6-NdRa-Prefix attribute is configured in the profile and is not returned from RADIUS server, this attribute is not included in the Acct-Start, Acct-Stop, and Interim-Acct messages

NOTE: When you attempt to configure the Ipv6-NdRa-Prefix attribute using the dynamic configuration manager (DCM) profile, the prefix is not successfully configured and the subscriber does not come up. In this scenario, the RADIUS server rejects the authentication request from the subscriber and records an error message stating that address allocation failed. However, if you attempt to configure the Ipv6-NdRa-Prefix attribute using the RADIUS profile, the prefix is correctly configured and the subscriber comes up successfully. This behavior is expected when the DCM profile is used to configure the Ipv6-NdRa-Prefix attribute.

This scenario occurs when router advertisements are enabled in the DCM profile and the RADIUS server returns only the Framed-Interface-Id attribute. Because the AAA server requires one of the following attributes to authenticate IPv6 subscribers, and none of these attributes are returned from the RADIUS server, the logging in of subscribers fails:

- Ipv6-NdRa-Prefix (VSA 26-129)
- Framed-IPv6-Prefix (RADIUS IETF attribute 97)
- Framed-IPv6-Route (RADIUS IETF attribute 99)
- Framed-IPv6-Pool (RADIUS IETF attribute 100)
- Delegated-IPv6-Prefix (RADIUS IETF attribute 123)

- ipv6-primary-dns—Excluded by default; includes RADIUS attribute 26-47, Ipv6-Primary-DNS; the attribute value received from the RADIUS server in the Access-Accept message is used in the accounting messages; if the IPv6 primary DNS server is configured in the AAA domain map and is not returned from the RADIUS server, the Acct-Start, Acct-Stop, or Interim-Acct messages report the value configured in the AAA domain map
- ipv6-secondary-dns—Excluded by default; includes RADIUS attribute 26-48, Ipv6-Secondary-DNS; the attribute value received from the RADIUS server in the Access-Accept message is used in the accounting messages; if the IPv6 secondary DNS server is configured in the AAA domain map and is not returned from the RADIUS server, the Acct-Start, Acct-Stop, or Interim-Acct messages report the value configured in the AAA domain map
- ipv6-virtual-router—Excluded by default; includes RADIUS attribute 26-45, Ipv6-Virtual-Router

- The attribute value received from the RADIUS server in the Access-Accept message is used in the accounting messages
- If the IPv6 virtual router is configured in the AAA domain map and is not returned from the RADIUS server, the Acct-Start, Acct-Stop, or Interim-Acct messages report the value configured in the domain map
- If IPv6 virtual router is not configured in the AAA domain map and is not returned from the RADIUS server, it is not included in the Acct-Start message because the value is not yet known
- If the IPv6 virtual router context is configured from the profile, it is reported in the immediate-update message for DHCPv6 prefix delegation
- If you configure the default virtual router as the authentication virtual router for the domain map using the **ipv6-router-name** command in Domain Map Configuration Mode and the IPv6-Virtual-Router RADIUS VSA attribute [26-45] is returned from the RADIUS server in the Access-Accept message, the IPv6 virtual router context returned from the RADIUS server overrides the IPv6 virtual router context configured in the AAA domain map. If you configure a nondefault virtual router as the authentication virtual router for the AAA domain map and the IPv6-Virtual-Router RADIUS VSA attribute [26-45] is returned from the RADIUS server in the Access-Accept message, the IPv6 virtual router context in the AAA domain map takes precedence over the IPv6 virtual router context returned from the RADIUS server.

- l2tp-ppp-disconnect-cause—Includes RADIUS attribute 26-51, Disconnect-Cause
- output-gigapkts—Includes RADIUS attribute 26-36, Acct-Output-Gigapackets
- output-gigawords—Includes RADIUS attribute 53, Acct-Output-Gigawords

Attributes available for Access-Request, Acct-Start, Acct-Stop, Acct-On, and Acct-Off messages:

- nas-identifier—Includes RADIUS attribute 32, NAS-Identifier

Attributes available for Access-Request, Acct-On, and Acct-Off messages:

- acct-session-id—Includes RADIUS attribute 44, Acct-Session-Id; can be optionally included in the change-of-authorization (COA) message from the RADIUS server or in the user login request if the packet mirroring operation is required; the Acct-Session-Id VSA is used:
  - In the RADIUS-initiated COA message to start the mirroring session when the user is already logged in
  - As a trigger in user-initiated mirroring to identify the user whose traffic is to be mirrored

Attributes available for Acct-Start, Acct-Stop, Acct-On, and Acct-Off messages:

- event-timestamp—Includes RADIUS attribute 55, Event-Timestamp

Attributes available for Acct-On and Acct-Off messages only:

- acct-authentic—Includes RADIUS attribute 45, Acct-Authentic

- acct-delay-time—Includes RADIUS attribute 41, Acct-Delay-Time

Attributes available for Acct-Off messages only:

- acct-terminate-cause—Includes RADIUS attribute 49, Acct-Terminate-Cause

- access-request—Specifies RADIUS Access-Request messages
- acct-on—Specifies RADIUS Acct-On messages
- acct-off—Specifies RADIUS Acct-Off messages
- acct-start—Specifies RADIUS Acct-Start messages
- acct-stop—Specifies RADIUS Acct-Stop messages
- enable—Enables attribute inclusion
- disable—Disables attribute inclusion; the attribute is excluded

Mode Global Configuration

receive-window

Syntax receive-window *receiveWindowSize*

no receive-window

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures the L2TP receive window size (RWS) for a tunnel on the LAC (in Domain Map Tunnel Configuration and Tunnel Group Tunnel Configuration modes) or on the LNS (in L2TP Destination Profile Host Configuration mode). The RWS is the number of packets that the peer can transmit without receiving an acknowledgment from the router. The **no** version reverts to the systemwide RWS setting configured with the l2tp tunnel default-receive-window command.

Options

- *receiveWindowSize*—Tunnel receive window size, in packets; currently, the only supported value is 4

Mode Domain Map Tunnel Configuration, L2TP Destination Profile Host Configuration, Tunnel Group Tunnel Configuration

remote host

Syntax [no] remote host { *hostname* | default }

Release Information Command introduced before JunosE Release 7.1.0.

Description Defines an L2TP host profile. Accesses the L2TP Destination Profile Host Configuration mode. The **no** version removes an L2TP host profile.

Options
- *hostname*—Name the LAC must supply in the hostname AVP of the receive SCCRQ; can be up to 64 characters in length (no spaces)
- default—Allows the LAC to use any hostname in the hostname AVP

Mode L2TP Destination Profile Configuration

sessions-limit-group

Syntax [no] sessions-limit-group *groupName*

Release Information Command introduced before JunosE Release 12.2.0.

Description Defines a session limit group. The **no** version removes the session limit group.

NOTE: Under each destination profile, you can define a maximum of 4096 session limit groups.

Options
- *groupName*—Name of the group

Mode L2TP Destination Profile Configuration, L2TP Destination Profile Host Configuration

Related Documentation
- Configuring Groups for LNS Sessions on page 48

session-out-of-resource-result-code-override

Syntax [no] session-out-of-resource-result-code-override

Release Information Command introduced in JunosE Release 9.2.0.

Description Overrides out-of-resource result codes 4 [Call failed due to lack of appropriate facilities being available (temporary condition)] and 5 [Call failed due to lack of appropriate facilities being available (permanent condition)] with code 2 (Call disconnected for the reason indicated in error code) on a router configured as an LNS. The **no** version halts the overriding of codes 4 and 5.

Mode L2TP Destination Profile Host Configuration

tunnel password

Syntax tunnel password *tunnelPassword*

no tunnel password

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures a password for the L2TP tunnel. The **no** version removes the password.

Options
- *tunnelPassword*—Password used for challenge response to the tunnel peer; in the domain map, it is used only by the LAC

Mode L2TP Destination Profile Host Configuration

tx-connect-speed-method

Syntax tx-connect-speed-method { static-layer2 | dynamic-layer2 | qos | actual }

no tx-connect-speed-method

Release Information Command introduced in JunosE Release 8.0.0.

Description Configures for an AAA domain map (when used from Domain Map Tunnel Configuration mode) or for an AAA tunnel group (when used from Tunnel Group Tunnel Configuration mode) the method used to calculate the transmit connect speed of the subscriber's access interface for establishing a tunneled L2TP session. This speed is reported in L2TP Transmit (TX) Speed AVP 24. The **no** version removes configuration of the transmit connect speed calculation method from the AAA domain map or AAA tunnel group.

Options

- static-layer2—Calculates the transmit connect speed of the subscriber's access interface based on statically configured settings for the underlying layer 2 interface
- dynamic-layer2—Calculates the transmit connect speed of the subscriber's access interface based on dynamically configured settings for the underlying layer 2 interface
- qos—Calculates the transmit connect speed of the subscriber's access interface based on settings determined by QoS
- actual—Calculates the transmit connect speed of the subscriber's access interface as the lesser of the **dynamic-layer2** value or the **qos** value

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel Configuration

virtual-router

Syntax virtual-router *vrName* | :*vrfName* | *vrName*:*vrfName*

no virtual-router *vrName* [wait-for-completion [*waitSeconds*]]

Release Information Command introduced before JunosE Release 7.1.0.

Description Creates a virtual router or accesses the context of a previously created virtual router or a VRF. The **no** version deletes the virtual router, and the router defaults to the default virtual router. Issuing a **no** version that specifies an existing VRF only displays the error message: " Cannot delete a VRF with this command." You must use the **no ip vrf** command to remove a VRF.

NOTE: In Domain Map Configuration mode, the **virtual-router** command has been replaced by the *router-name* command and may be removed completely from Domain Map Configuration mode in a future release.

Options

- *vrName*—Name of the virtual router; a string of 1–32 alphanumeric characters
- :*vrfName*—Name of a VRF in the current VR context; a string of 1–32 alphanumeric characters
- *vrName*:*vrfName*—Name of a VRF in the context of a VR other than the current VR
- wait-for-completion—Specifies (in the absence of *waitSeconds*) that the CLI waits for completion of the **no** version operation before it returns a prompt, regardless of how long that takes
- *waitSeconds*—Number of seconds, in the range 1–64000, that the CLI waits before it returns a prompt, regardless of whether the **no** version operation has been completed

Mode Global Configuration, Privileged Exec

PART 3

Administration

CHAPTER 16

Verifying Domain Maps and L2TP Tunnels with AAA

Monitoring the Mapping for User Domains and Virtual Routers with AAA

Purpose Display the mapping between user domains and virtual routers.

Action To display the mapping between user domains and virtual routers:

```
host1#show aaa domain-map
```

```
Domain: lac-tunnel; router-name: lac; ipv6-router-name: default
Tunnel                 Tunnel   Tunnel   Tunnel    Tunnel
 Tag     Tunnel Peer   Source    Type    Medium   Password    Tunnel Id
------   -----------   ------   ------   ------   --------   -----------
5        192.168.1.1   <null>   l2tp     ipv4     welcome    lac-tunnel

                       Tunnel                Tunnel
Tunnel     Tunnel      Server     Tunnel       Max
 Tag     Client Name    Name    Preference   Sessions     Tunnel RWS
------   -----------   ------   ----------   --------   --------------
5        lac           boston   5            0          4

                                                 Tunnel
         Tunnel     Tunnel      Tunnel        Tx
Tunnel   Virtual   Failover     Switch      Speed
 Tag     Router     Resync     Profile      Method
------   -------   --------   ---------    ------
5        <null>    <null>      denver      qos
```

Meaning Table 17 on page 125 lists the **show aaa domain-map** command output fields.

Table 17: show aaa domain-map Output Fields

Field Name	Field Description
Domain	Name of the domain
router-name	Virtual router to which user domain name is mapped

Table 17: show aaa domain-map Output Fields *(continued)*

Field Name	Field Description
router-mask	IPv4 mask of the local interface
tunnel-group	Name of the tunnel group assigned to the domain map
ipv6-router-name	IPv6 virtual router to which user domain name is mapped
local-interface	Interface information to use on the local (E Series) side of the subscriber's interface
ipv6-local-interface	IPv6 interface information to use on the local (E Series) side of the subscriber's interface
poolname	Local address pool from which the router allocates addresses for this domain
IP hint	IP hint is enabled
strip-domain	Strip domain is enabled
override-username	Single username used for all users from a domain in place of the values received from the remote client
override-password	Single password used for all users from a domain in place of the values received from the remote client
Tunnel Tag	Tag that identifies the tunnel
Tunnel Peer	Destination address of the tunnel
Tunnel Source	Source address of the tunnel
Tunnel Type	L2TP
Tunnel Medium	Type of medium for the tunnel; only IPv4 is supported
Tunnel Password	Password for the tunnel
Tunnel Id	ID of the tunnel
Tunnel Client Name	Host name that the LAC sends to the LNS when communicating to the LNS about the tunnel
Tunnel Server Name	Host name expected from the peer (the LNS) when during tunnel startup
Tunnel Preference	Preference level for the tunnel

Table 17: show aaa domain-map Output Fields *(continued)*

Field Name	Field Description
Tunnel Max Sessions	Maximum number of sessions allowed on a tunnel
Tunnel RWS	L2TP receive window size (RWS) for a tunnel on the LAC; displays either the configured value or the default behavior, which is indicated by system chooses
Tunnel Virtual Router	Name of the virtual router to map to the user domain name
Tunnel Failover Resync	L2TP peer resynchronization method
Field descriptions	The actual fields displayed depend on your configuration
Tunnel Switch Profile	Name of the L2TP tunnel switch profile
Tunnel Tx Speed Method	Method that the router uses to calculate the transmit connect speed of the subscriber's access interface: static layer2, dynamic layer2, qos, actual, not set

Related Documentation

- show aaa domain-map on page 168

Monitoring Configuration of Tunnel Parameters with AAA

Purpose Display configuration of tunnel parameters used for tunnel definitions.

Action To display the configuration of tunnel parameters used for tunnel definitions:

```
host1#show aaa tunnel-parameters
Tunnel password is 3&92k%b#q4
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 (stacked)
 Tunnel calling number format fallback is fixed
```

Meaning Table 18 on page 127 lists the **show aaa tunnel-parameters** command output fields.

Table 18: show aaa tunnel-parameters Output Fields

Field Name	Field Description
Tunnel password	Default tunnel password

Table 18: show aaa tunnel-parameters Output Fields *(continued)*

Field Name	Field Description
Tunnel client-name	Hostname that the LAC sends to the LNS when communicating about the tunnel
Tunnel nas-port-method	Default NAS port type
Tunnel switch profile is	Name of the default L2TP tunnel switch profile
Tunnel tx-connect-speed-method is	Method that the router uses to calculate the transmit connect speed of the subscriber's access interface: static layer2, dynamic layer2, qos, actual, not set
Tunnel nas-port ignore	Whether the router uses the tunnel peer's NAS-Port [5] attribute; enabled or disabled
Tunnel nas-port-type ignore	Whether the router uses the tunnel peer's NAS-Port-Type [61] attribute; enabled or disabled
Tunnel assignmentId format	Value of the tunnel assignment ID that is passed to PPP/L2TP
Tunnel calling number format	Format configured for L2TP Calling Number AVP 22 generated by the LAC
Tunnel calling number format fallback	Fallback format configured for L2TP Calling Number AVP 22 generated by the LAC

Related Documentation

- show aaa tunnel-parameters on page 170

Monitoring Configured Tunnel Groups with AAA

Purpose Display the currently configured tunnel groups.

Action To display information about currently configured tunnel groups:

```
host1#show aaa tunnel-group

Tunnel Group: boston
Tunnel                  Tunnel   Tunnel   Tunnel    Tunnel
 Tag     Tunnel Peer    Source    Type    Medium   Password    Tunnel Id
------   -----------   ------   ------   ------   --------   -----------
3        192.168.1.1   <null>   l2tp     ipv4     msn        <null>

                       Tunnel                Tunnel
Tunnel     Tunnel      Server     Tunnel      Max
 Tag     Client Name    Name    Preference   Sessions     Tunnel RWS
------   -----------   ------   ----------   --------   --------------
3        msn.del.com   <null>   2000         0          4

                                           Tunnel
         Tunnel     Tunnel      Tunnel       Tx
Tunnel   Virtual   Failover     Switch     Speed
```

```
 Tag     Router     Resync     Profile     Method
------   -------   --------   ---------    ------
3        <null>    <null>      sanjose     qos
```

Meaning Table 19 on page 129 lists the **show aaa tunnel-group** command output fields.

Table 19: show aaa tunnel-group Output Fields

Field Name	Field Description
Domain	Name of the domain
router-name	Virtual router to which user domain name is mapped
router-mask	IPv4 mask of the local interface
tunnel-group	Name of the tunnel group assigned to the domain map
ipv6-router-name	IPv6 virtual router to which user domain name is mapped
local-interface	Interface information to use on the local (E Series) side of the subscriber's interface
ipv6-local-interface	IPv6 interface information to use on the local (E Series) side of the subscriber's interface
poolname	Local address pool from which the router allocates addresses for this domain
IP hint	IP hint is enabled
strip-domain	Strip domain is enabled
override-username	Single username used for all users from a domain in place of the values received from the remote client
override-password	Single password used for all users from a domain in place of the values received from the remote client
Tunnel Tag	Tag that identifies the tunnel
Tunnel Peer	Destination address of the tunnel
Tunnel Source	Source address of the tunnel
Tunnel Type	L2TP
Tunnel Medium	Type of medium for the tunnel; only IPv4 is supported
Tunnel Password	Password for the tunnel

Table 19: show aaa tunnel-group Output Fields *(continued)*

Field Name	Field Description
Tunnel Id	ID of the tunnel
Tunnel Client Name	Host name that the LAC sends to the LNS when communicating to the LNS about the tunnel
Tunnel Server Name	Host name expected from the peer (the LNS) when during tunnel startup
Tunnel Preference	Preference level for the tunnel
Tunnel Max Sessions	Maximum number of sessions allowed on a tunnel
Tunnel RWS	L2TP receive window size (RWS) for a tunnel on the LAC; displays either the configured value or the default behavior, which is indicated by system chooses
Tunnel Virtual Router	Name of the virtual router to map to the user domain name
Tunnel Failover Resync	L2TP peer resynchronization method
Field descriptions	The actual fields displayed depend on your configuration
Tunnel Switch Profile	Name of the L2TP tunnel switch profile
Tunnel Tx Speed Method	Method that the router uses to calculate the transmit connect speed of the subscriber's access interface: static layer2, dynamic layer2, qos, actual, not set

Related Documentation

- The information displayed is almost identical to the tunnel information displayed using the **show aaa domain-map** command. See Monitoring the Mapping for User Domains and Virtual Routers with AAA on page 125.
- show aaa tunnel-group on page 169

CHAPTER 17

Verifying the L2TP Tunnel Aggregated Settings

Monitoring Global Configuration Status on E Series Routers

Purpose Display the global configuration and status for L2TP on E Series routers, including switched sessions.

Action To display the global configuration and status for L2TP on E Series routers, including switched sessions:

```
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
  Reject remote transmit address change is enabled for ip address
  Ignore remote transmit address change is disabled
  Disconnect-cause avp generation is enabled
  Default receive window size is system chooses
  Rx speed avp when equal is enabled
  Destination lockout timeout is 300 seconds
  Destination lockout test is disabled
  Failover resync is silent-failover
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
```

Meaning Table 20 on page 132 lists the **show l2tp** command output fields.

Table 20: show l2tp Output Fields

Field Name	Field Description
Configuration	Configuration and status for L2TP on E Series routers, including switched sessions
L2TP administrative state	Status of L2TP on the router; enabled or disabled
Dynamic interface destruct timeout	Number of seconds that the router maintains dynamic destinations, tunnels, and sessions after they have terminated
Data packet checksums	Status of checking data integrity via UDP; enabled or disabled
Receive data sequencing	Whether the router processes or ignores sequence numbers in incoming data packets
Tunnel switching	Enabled or disabled
Retransmission retries for established tunnels	Number of retries configured for established tunnels
Retransmission retries for not-established tunnels	Number of retries configured for tunnels not established
Tunnel idle timeout	Length of the tunnel idle timeout, in seconds
Failover within a preference level	Enabled or disabled
Weighted load balancing	Enabled or disabled
Tunnel authentication challenge	Enabled or disabled
Calling number avp	Whether the E Series LAC sends Calling-Station-Id and Called-Station-Id AVPs in ICRQ packets, enabled or disabled
Reject remote transmit address change	Enabled or disabled for IP address, UDP port, or both
Ignore remote transmit address change	Enabled or disabled for IP address, UDP port, or both
Disconnect-cause avp generation	Enabled or disabled
Default receive window size	Default L2TP RWS for a tunnel on both the LAC and the LNS; displays either the configured value or the default behavior, indicated by system chooses
Rx speed avp when equal	Enabled or disabled

Table 20: show l2tp Output Fields *(continued)*

Field Name	Field Description
Destination lockout timeout	Number of seconds that L2TP destinations remain in the lockout state after they become unavailable
Destination lockout test	Status of the L2TP destination lockout test, enabled or disabled
Failover resync	Global L2TP peer resynchronization configuration
Sub-interfaces	Sub-interface information about L2TP
total	Number of destinations, tunnels, and sessions that the router created
active	Number of operational destinations, tunnels, and sessions
failed	Number of requests that did not reach an operational state
auth-errors	Number of requests that failed because the tunnel password was invalid

Related Documentation

- show l2tp on page 171

CHAPTER 18

Monitoring L2TP Destination Settings

Monitoring Detailed Configuration Information for Specified Destinations

Purpose Display detailed configuration information about specified destinations.

Action To display detailed configuration information about specified destinations:

To display information about a specific destination:

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

To display information about all destinations:

```
host1#show l2tp destination detail 1
L2TP destination 1 is Up with 5 active tunnels and 64 active sessions
Configuration
  Administrative state is enabled
  SNMP traps are enabled
Destination address
  Transport ipUdp
  Virtual router default
  Local address 192.168.1.230, peer address 172.31.1.98
Destination status
  Effective administrative state is enabled
Sub-interfaces total active failed auth-errors
  Tunnels      5     5      0      0
  Sessions     64    64     0      n/a
Statistics    packets      octets       discards   errors
  Control rx  69           3251          2          0
  Control tx  195          23939         0          0
  Data rx     68383456     68383456      0          0
  Data tx     68383456     68383456       0         0
```

Meaning Table 21 on page 136 lists the **show l2tp destination** command output fields.

Table 21: show l2tp destination Output Fields

Field Name	Field Description
Configuration	Configured status of the destination
Administrative state	Administrative status of the destination: • enabled—No restrictions on creation and operation of sessions and tunnels for this destination • disabled—Router disabled existing sessions and tunnels and will not create new sessions or tunnels for this destination • drain—Router will not create new sessions or tunnels for this destination
SNMP traps	Whether or not the router sends traps to SNMP for operational state changes
Destination address	Address information for the specified destination
Transport	Method used to transfer traffic
Virtual	Name of the virtual router on which the tunnel is configured
Local and peer addresses	Addresses of the local and remote interfaces
Destination status	Effective administrative state—The more restrictive of the router and destination administrative states. This setting, rather than the administrative state of the destination, determines whether the router can create new sessions or tunnels and whether the sessions or tunnels are disabled for this destination.
Sub-interfaces	Sub-interface information about the L2TP destination
total	Number of sessions or tunnels that the router created for this destination
active	Number of operational sessions or tunnels for this destination
failed	Number of requests that did not reach an operational state for this destination
auth-errors	Number of requests that failed because the tunnel password was invalid for this destination
Statistics	Information about the traffic sent and received

Related Documentation

- show l2tp destination on page 172

Monitoring Configured and Operational Status of all Destinations

Purpose Display summary of the configured and operational status of all L2TP destinations.

Action To display a summary of the configured and operational status of all L2TP destinations.:

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

Meaning Table 22 on page 137 lists the **show l2tp destination summary** command output fields.

Table 22: show l2tp destination summary Output Fields

Field Name	Field Description
Administrative status	Administrative status of the L2TP destination: • enabled—No restrictions on creation and operation of sessions and tunnels for this destination • drain—Router will not create new sessions or tunnels for this destination • disabled—Router disabled existing sessions and tunnels and will not create new sessions or tunnels for this destination
Operational status	Operational status of the L2TP destination: • up—Destination is available for tunnels • down—Destination is not available for tunnels • lower-down—Underlying transport is unavailable; for example, you removed the virtual router • not-present—Hardware supporting the destination is unavailable; for example, you removed a required line module

Related Documentation
- show l2tp destination on page 172

Monitoring Locked Out Destinations

Purpose Display information about the L2TP destinations that are currently locked out.

Action To display information about the L2TP destinations that are currently locked out:

```
host1#show l2tp destination lockout
L2TP destination 36 is waiting for lockout timeout (45 seconds remaining)
L2TP destination 54 is waiting for lockout test start
L2TP destination 76 is waiting for lockout test complete
3 L2TP lockout destinations found
```

Meaning Table 23 on page 138 lists the **show l2tp destination lockout** command output fields.

Table 23: show l2tp destination lockout Output Fields

Field Name	Field Description
L2TP destination waiting	Name of destination and its lockout status. The status indicates whether the destination is waiting for the lockout timeout to expire (and how much time is left), or waiting for the lockout test to start or finish
L2TP lockout destinations found	Number of destinations that are currently in lockout state

Related Documentation

- show l2tp destination lockout on page 173

Monitoring Configured L2TP Destination Profiles or Host Profiles

Purpose

Display either a list of configured Layer 2 Tunneling Protocol (L2TP) destination profiles or the host profiles defined in a particular profile.

If a nondefault L2TP receive window size (RWS) is configured for a particular host profile, the command displays the RWS setting as an attribute of that host profile.

Action

To display either a list of configured L2TP destination profiles or the host profiles defined in a particular profile:

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

If a nondefault L2TP RWS is configured for a particular host profile, to display the RWS setting as an attribute of that host profile:

```
host1#show l2tp destination profile westford
L2TP destination profile westford
Configuration
  Destination address
    Transport ipUdp
    Virtual router lns
    Peer address 192.168.1.99
  Destination profile maximum sessions is 5000
Current session count in group-A is 14, max-sessions configured is 3400
Current session count in group-B is 2, max-sessions configured is 4600
Statistics
  Destination profile current session count is 30
Host profile attributes
  Remote host is remhost22.xyz.com
    Configuration
      Tunnel password is 23erf5
      Interface profile is ebcints
      Bundled group id is 1
      Bundled group id override is enabled
      Maximum sessions is 400
      Failover resync is failover-protocol
      Sessions-limit-group is group-A
    Statistics
      Current session count is 14
```

```
  Remote host is asciitext
    Configuration
      Bundled group id is 0
      Tunnel password is 222
      Interface profile is ascints
      Default upper binding type mlppp
      Maximum sessions is 250
      Failover resync is failover-protocol
      Sessions-limit-group is group-B
  Statistics
      Current session count is 2
  Remote host is mexico
    Configuration
      Local ip address is 10.10.2.2
      Proxy lcp is disabled
      Proxy authenticate is enabled
      mlppp upper binding type
      Disconnect-cause avp is enabled
      Receive window size is 4
      Maximum sessions is 500
      Failover resync is failover-protocol
    Statistics
      Current session count is 14
  Remote host is LAC
    Configuration
      Tunnel password is TunnelPass
      Local host name is LNS
      Local ip address is 46.1.1.2
      Disconnect-cause avp is enabled
      Tunnels are single-shot
      Override out-of-resource-result-code is enabled
    Statistics
      Current session count is 0
5 L2TP host profiles found
```

Meaning Table 24 on page 139 lists the **show l2tp destination profile** command output fields.

Table 24: show l2tp destination profile Output Fields

Field Name	Field Description
Transport	Method used to transfer traffic
Virtual router	Name of the virtual router
Peer address	IP address of the L2TP access concentrator (LAC)
Destination profile maximum sessions	Maximum number of sessions allowed for the destination profile
Current session count in group-A	Number of current sessions in group-A
Current session count in group-B	Number of current sessions in group-B
Destination profile current session count	Number of current sessions for the destination profile

Table 24: show l2tp destination profile Output Fields *(continued)*

Field Name	Field Description
Host profile attributes	Host profile attributes of the L2TP destination
Remote host	Name of the remote host
Local host name	Name of the local host
Local ip address	IP address of the local host
Bundled group id	Identifier for bundled sessions
Bundled group id override	Status of the bundled group ID override: enabled or disabled
Tunnel password	Password for the tunnel
Interface profile	Name of the host profile
Default upper binding type	The default upper binding type: mlpp
Proxy lcp	Status of the proxy LCP for the remote host
mlppp upper binding type	Default upper binding type
Proxy authenticate	The status of the proxy authentication: enabled or disabled
Disconnect-cause avp	Status of the disconnect-cause attribute-value pair (AVP): enabled or disabled
Tunnels are single-shot	Indicates that single-shot tunnels are configured for this host profile
Receive window size	Number of packets that the peer can transmit without receiving an acknowledgment from the router
Maximum sessions	Maximum number of sessions allowed for the host profile
Failover resync	L2TP peer resynchronization method for the host profile
Override out-of-resource-result-code	State of the out-of-resource-result-code override: enabled or disabled
Current session count	Number of current sessions for the host profile
Sessions-limit-group	Name of the sessions limit group

Related Documentation

- *Configuring an L2TP Destination Profile to Enable IPsec Support for L2TP Tunnels*
- *Configuring Single-Shot L2TP/IPsec Tunnels*
- show l2tp destination profile on page 174

CHAPTER 19

Viewing the Disconnect Cause-Codes for PPP Sessions

Monitoring Statistics on the Cause of a Session Disconnection

Purpose Display statistics for all information the LAC receives from an LNS about the cause of an L2TP session disconnection.

Action To display statistics for all information the LAC receives from an LNS about the cause of an L2TP session disconnection.

```
host1# show l2tp received-disconnect-cause-summary
Disconnect Cause (Code)                          Global     Peer       Local
------------------------------------------------ ---------- ---------- ----------
no info (0)                                      0          0          0
admin disconnect (1)                             0          0          0
renegotiation disabled (2)                       0          0          0
normal disconnect (3)                            0          0          0
compulsory encryption refused (4)                0          0          0
lcp failed to converge (5)                       0          0          0
lcp peer silent (6)                              0          0          0
lcp magic number error (7)                       0          0          0
lcp keepalive failure (8)                        0          0          0
lcp mlppp endpoint discriminator mismatch (9)    0          0          0
lcp mlppp peer mrru not valid (10)               0          0          0
lcp mlppp peer ssn invalid (11)                  0          0          0
lcp callback refused (12)                        0          0          0
authenticate timed out (13)                      0          0          0
authenticate mlppp name mismatch (14)            0          0          0
authenticate protocol refused (15)               0          0          0
authenticate failure (16)                        0          0          0
ncp no negotiation completed (17)                0          0          0
ncp no ncps available (18)                       0          0          0
ncp addresses failed to converge (19)            0          0          0
ncp negotiation inhibited (20)                   0          0          0
```

Meaning Table 25 on page 144 lists the **show l2tp received-disconnect-cause-summary** command details.

Table 25: show l2tp received-disconnect-cause-summary Output Fields

Field Name	Field Description
show l2tp received-disconnect-cause-summary	Display statistics for all information the LAC receives from an LNS about the cause of an L2TP session disconnection.

Related Documentation

- show l2tp received-disconnect-cause-summary on page 175

CHAPTER 20

Viewing the Configured L2TP Session Details

Monitoring Detailed Configuration Information about Specified Sessions

Purpose Display detailed configuration information about specified sessions.

Action To display detailed configuration information about specified sessions:

To display L2TP session:

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

To display L2TP session details:

```
host1#show l2tp session detail
L2TP session 1/1/1 is Up
Configuration
  Administrative state is enabled
  SNMP traps are enabled
Session status
  Effective administrative state is enabled
  State is established
  Local session id is 25959, peer session id is 2
Statistics packets octets discards errors
  Data rx  7       237    1        0
  Data tx  6       160    0        0

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

Meaning Table 26 on page 146 lists the **show l2tp session** command output fields.

Table 26: show l2tp session Output Fields

Field Name	Field Description
Configuration	Configured status of the session
Administrative state	Administrative status of the destination: • enabled—No restrictions on the operation of this session • disabled—Router terminated this session
SNMP traps	Whether or not the router sends traps to Simple Network Management Protocol (SNMP) for operational state changes
Session status	Session status of the destination
Effective administrative state	Most restrictive of the following administrative states: router, destination, tunnel, and session. This setting, rather than the administrative state of the session, determines whether the router can maintain this session or not.
State	Status of the session: idle, connecting, established, or disconnecting
Local and peer session id	Names the router uses to identify the session locally and remotely
Statistics	Information about the traffic for this session
Session operational configuration	Information received from the peer when the session was created

Related Documentation

- show l2tp session on page 180

Monitoring Configured and Operational Summary Status

Purpose Display a summary of the configured and operational status of all L2TP sessions.

Action To display a summary of the configured and operational status of all L2TP sessions:

```
host1#show  l2tp session summary
Administrative status  enabled   disabled
                       64        0
Operational status     up        down   lower-down   not-present
                       64        0      0            0
```

Meaning Table 27 on page 147 lists the **show l2tp session summary** command output fields.

Table 27: show l2tp session summary Output Fields

Field Name	Field Description
Administrative status:	Administrative status of the session: • enabled—No restrictions on the creation of sessions • disabled—Router disabled these sessions
Operational status:	Operational status of the session: • up—Session is available • down—Session is unavailable • lower-down—Session is unavailable because the tunnel supporting it is inaccessible • not-present—Session is unavailable because the hardware (such as a line module) supporting it is inaccessible

Related Documentation

- show l2tp session on page 180 summary

CHAPTER 21

Viewing L2TP Switch-Profiles

Monitoring Configured Switch Profiles on Router

Purpose Display information about the L2TP switch profiles configured on the router.

Action To display only the names of the L2TP tunnel switch profiles configured on the router:

```
host1#show l2tp switch-profile
L2TP tunnel switch profile concord
L2TP tunnel switch profile myProfile
2 L2TP tunnel switch profiles found
```

To display information about the settings in a particular L2TP tunnel switch profile:

```
host1#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
```

Meaning Table 28 on page 149 lists the **show l2tp switch-profile** command output fields.

Table 28: show l2tp switch-profile Output Fields

Field Name	Field Description
L2TP tunnel switch profile	Name of the L2TP tunnel switch profile
AVP *actionType* action is	Indicates the tunnel switching behavior or action type (for example, relay) configured for the specified L2TP AVP type

Related Documentation

- show l2tp switch-profile on page 181

CHAPTER 22

Monitoring L2TP Tunnel Settings

Monitoring Detailed Configuration Information about Specified Tunnels

Purpose Display detailed configuration information about specified tunnels.

Action To display detailed configuration information about specified tunnel by IP address:

NOTE: For L2TP tunnels configured with output IPv4 or IPv6 policy lists, the output of the **show ip interface tunnel** *l2tp:tunnel-name* and the **show ipv6 interface tunnel** *l2tp:tunnel-name* commands display only the forwarded packets and bytes fields, and the dropped packets and bytes fields in the rate-limit-profile section for policies with hierarchical parent groups under the IP policy output or IPv6 policy output headings, respectively, when scheduler profile–based computation of service session accounting is enabled. In such a case, the committed, conformed, exceeded, saturated, and unconditional packets and bytes fields are not displayed in the rate-limit-profile section in the output of these commands for policies with hierarchical parent groups.

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

To display detailed configuration information about specified tunnel:

```
host1#show l2tp tunnel detail 1/xyz
L2TP tunnel 1/xyz is Up with 13 active sessions
Configuration
  Administrative state is enabled
  SNMP traps are enabled
Tunnel address
  Transport ipUdp
```

```
  Virtual router default
  Local address 192.168.1.230, peer address 172.31.1.98
  Local UDP port 1701, peer UDP port: 1701
Tunnel status
  Effective administrative state is enabled
  State is established
  Local tunnel id is 14529, peer tunnel id is 34
  Host profile is none
  Tunnel is Up for: 12 days, 8 hours, 24 minutes, 23 seconds
Sub-interfaces    total   active   failed
  Sessions        13      13       0
Statistics    packets      octets       discards   errors
  Control rx  14           683          0          0
  Control tx  41           4666         0          0
  Data rx     67900944     67900944     0          0
  Data tx     67900944     67900944     0          0
Control channel statistics
  Receive window size = 4
  Receive ZLB = 17
  Receive out-of-sequence = 0
  Receive out-of-window = 0
  Transmit window size = 4
  Transmit ZLB = 12
  Transmit queue depth = 0
  Retransmissions = 8
Tunnel operational configuration
  Peer host name is 'Juniper-POS'
  Peer vendor name is 'XYZ, Inc.'
  Peer protocol version is 1.1
  Peer firmware revision is 0x1120
  Peer bearer capabilities are digital and analog
  Peer framing capabilities are sync and async
```

Meaning Table 29 on page 152 lists the **show l2tp tunnel** command output fields.

Table 29: show l2tp tunnel Output Fields

Field Name	Field Description
Configuration	Configured status of the tunnel enabled.
Administrative state	Administrative status of the enabled tunnel: • enabled—No restrictions on creation and operation of sessions for this tunnel • disabled—Router disabled existing sessions and will not create new sessions on this tunnel • drain—Router will not create new sessions on this tunnel
SNMP traps	Whether or not the router sends traps to SNMP for operational state changes.
Tunnel address	Tunnel address information.
Transport	Method used to transfer traffic.

Table 29: show l2tp tunnel Output Fields *(continued)*

Field Name	Field Description
Virtual router	Name of the virtual router on which the tunnel is configured.
Local and peer addresses	IP addresses of the local and remote ends of the tunnel. If the router is set up to ignore address and port changes in SCCRP packets, both the transmit and receive addresses are listed for the peer.
Local and peer UDP ports	UDP ports for the local and remote ends of the tunnel. If the router is set up to accept address and port changes in SCCRP packets, both the transmit and receive UDP ports are listed for the peer.
Tunnel status	Tunnel status information.
Effective administrative state	Most restrictive of the following administrative states: E Series router, destination, and tunnel. This setting, rather than the administrative state of the tunnel, determines whether the router can create new sessions on a tunnel or whether the sessions on a tunnel are disabled or not.
State	Status of the enabled tunnel: • idle • connecting • established • disconnecting
Local and peer tunnel id	Names the router used to identify the tunnel locally and remotely.
Host profile	Name of the L2TP host profile, if it is configured. Otherwise, the label “none” is displayed to specify that a host profile is not enabled.
Tunnel is Up for	Duration for which the tunnel is operationally up, which is denoted in terms of days, hours, minutes, and seconds.
Sub-interfaces:	Sub-interface information for the enabled tunnel: • total—Number of sessions that the router has created on this tunnel • active—Number of operational sessions on the tunnel • failed—Number of requests that did not reach an operational state
Statistics	Information about the traffic sent and received.

Table 29: show l2tp tunnel Output Fields *(continued)*

Field Name	Field Description
Control channel statistics	Tunnel control channel information.
Receive window size	Number of packets that the peer can transmit without receiving an acknowledgment from the router.
Receive ZLB	Number of acknowledgments that the router has received from the peer.
Receive out-of-sequence	Number of received control packets that were out of order.
Receive out-of-window	Number of packets that arrived at the router outside the receiving window.
Transmit window size	Number of packets that the router can transmit before receiving an acknowledgment from the peer.
Transmit ZLB	Number of acknowledgments that the router has sent to the peer.
Transmit queue depth	Number of packets that the router is waiting to send to the peer, plus the number of packets for which the peer has not yet acknowledged receipt.
Tunnel operation configuration	Information received from the peer when the tunnel was created.

Related Documentation

- show l2tp tunnel on page 182

Monitoring Configured and Operational Status of All Tunnels

Purpose Display a summary of the configured and operational status of all L2TP tunnels.

Action To display a summary of the configured and operational status of all L2TP tunnels:

```
host1#show l2tp tunnel summary

Administrative status   enabled   drain   disabled
                        5         0       0
Operational status      up        down    lower-down   not-present
             5          0         0       0            0
```

Meaning Table 30 on page 155 lists the **show l2tp tunnel summary** command output fields.

Table 30: show l2tp tunnel summary Output Fields

Field Name	Field Description
Administrative status	Administrative status of all tunnels: • enabled—No restrictions on the creation and operation of sessions for this tunnel • drain—Router will not create new sessions for this tunnel • disabled—Router disabled existing sessions and will not create new sessions for this tunnel
Operational status	Operational status of all tunnels: • up—Tunnel is available • down—Tunnel is unavailable • lower-down—Tunnel is unavailable because the destination supporting it is inaccessible • not-present—Tunnel is unavailable because the hardware (such as a line module) supporting the tunnel is inaccessible

Related Documentation

- show l2tp tunnel on page 182 summary

CHAPTER 23

Monitoring L2TP Dial-Out Settings

Monitoring Chassis-wide Configuration for L2TP Dial-out

Purpose To display the chassis-wide configuration, operational state, and statistics for L2TP dial-out.

This command displays aspects of the dial-out state machine and details about the dial-out routes themselves. This section presents sample output. The actual output on your router may differ significantly.

Action To display chassis-wide configuration, operational state, and statistics for L2TP dial-out:

```
host1#show l2tp dial-out
Operational status: inService
Connecting timer value: 30 seconds
Dormant timer value: 300 seconds
```

To display detailed chassis-wide configuration information:

```
host1#show l2tp dial-out detail
    Dial-out Chassis Configuration and Operational Status
      Chassis operational status :   inService
      Dormant timeout            :   30 seconds
      Connecting timeout         :   30 seconds

Dial-out Chassis Statistics
  Current sessions:                              0
  Maximum sessions:                              0
  Current sessions in the process of connecting:   0
  Maximum sessions connecting at one time:         0
  Current sessions pending:                      0
  Maximum sessions pending:                      0
  Current targets inhibited:                     0
  Maximum targets inhibited:                     0
  Authentication grant for nonexistent session:    0
  Authentication deny for nonexistent session:     0

Dial-out Virtual router statistics
  Virtual routers active:                     0
```

```
  Virtual routers created:                        0
  Virtual routers removed:                        0
  Virtual routers in init-pending state:          0
  Virtual routers in init-failed state:           0
  Virtual routers in down state:                  0
  Virtual routers in in-service state:            0
  IP Discarded trigger frames:                    0
  Trigger frames received for unknown route:      0
  Sessions in dormant state:                      0
  Sessions in pending state:                      0
  Sessions in authenticating state:               0
  Sessions in connecting state:                   0
  Sessions in in-service state:                   0
  Sessions in inhibited state:                    0
  Sessions in post-inhibited state:               0
  Sessions in failed state:                       0

Dial-out target statistics
  Targets active:                                 0
  Targets created:                                0
  Targets removed:                                0
  Targets in down state:                          0
  Targets in inhibited state:                     0
  Targets in in-service state:                    0
  Triggers discarded:                             0
Dial-out session statistics
  Sessions active:                                0
  Sessions created:                               0
  Sessions removed:                               0
  Sessions reset:                                 0
  Triggers received:                              0
  Triggers enqueued:                              0
  Triggers discarded:                             0
  Triggers forwarded:                             0
  Triggers max enqueued:                          0
  Authentication requests:                        0
  No resources for authentication:                0
  Authentication grants:                          0
  Authentication Denies:                          0
  Dial-outs requested:                            0
  Dial-outs rejected:                             0
  Dial-outs established:                          0
  Dial-outs timed out:                            0
  Dial-outs torn down:                            0
```

To display summary information for chassis-wide configuration:

```
host1#show l2tp dial-out summary
      Virtual routers in init pending state :             0
      Virtual routers in init failed state  :             0
      Virtual routers in down state         :             0
      Virtual routers in inService state    :             0
      Targets in down state                 :             0
      Targets in inhibited state            :             0
      Targets in inService state            :             0
      Sessions in dormant state             :             0
      Sessions in pending state             :             0
      Sessions in authenticating state      :             0
      Sessions in connecting state          :             0
      Sessions in inService state           :             0
      Sessions in inhibited state           :             0
```

```
Sessions in postInhibited state       :              0
Sessions in failed state              :              0
```

To display information about the operational or administrative state:

```
host1#show l2tp dial-out state inService
```

Meaning Table 31 on page 159 lists the **show l2tp dial-out** command output fields.

Table 31: show l2tp dial-out Output Fields

Field Name	Field Description
Operational status	Current operational status of the chassis
Connecting timer value	Configuration of the connecting timeout
Dormant timer value	Configuration of the dormant timeout
Dial-out Chassis Statistics	Statistics at the chassis level
Current sessions	Total number of session currently active on the chassis
Maximum sessions	Highest value of current sessions recorded on the chassis since the last router restart
Current sessions in the process of connecting	Sessions currently in the connecting state
Maximum sessions connecting at one time	Highest number of sessions recorded on the chassis at the same time since the last router restart
Current sessions pending	Sessions in the pending state
Maximum sessions pending	Highest number of sessions recorded in the pending state since the last router restart
Current targets inhibited	Targets currently in the inhibited state
Maximum targets inhibited	Highest value of targets recorded in the inhibited state since the last router restart
Authentication grant for nonexistent session	Number of authentication requests granted to nonexistent sessions
Authentication deny for nonexistent session	Number of authentication requests denied to nonexistent sessions
Dial-out Virtual router statistics	Statistics at the virtual router level
Virtual routers active	VRs in use by the state machine
Virtual routers created	VRs that have been used by the state machine

Table 31: show l2tp dial-out Output Fields *(continued)*

Field Name	Field Description
Virtual routers removed	VRs no longer used by the state machine
Virtual routers in init-pending state	VRs in the initializationPending state
Virtual routers in init-failed state	VRs in the initializationFailed state
Virtual routers in down state	VRs in the down state
Virtual routers in in-service state	VRs in the inService state
IP Discarded trigger frames	Trigger frames that IP discarded
Trigger frames received for unknown route	Trigger frames received for an unknown route
Sessions in dormant state	Sessions on the VR that are in the dormant state
Sessions in pending state	Sessions on the VR that are in the pending state
Sessions in authenticating state	Sessions on the VR that are in the authenticating state
Sessions in connecting state	Sessions on the VR that are in the connecting state
Sessions in in-service state	Sessions on the VR that are in the inService state
Sessions in inhibited state	Sessions on the VR that are in the inhibited state
Sessions in post-inhibited state	Sessions on the VR that are in the postInhibited state
Sessions in failed state	Sessions on the VR that are in the failed state
Dial-out target statistics	Statistics at the route target level
Targets active	Current active targets
Targets created	All targets created
Targets removed	Targets deleted
Targets in down state	Targets in the down state
Targets in inhibited state	Targets in the inhibited state
Targets in in-service state	Targets in the inService state
Triggers discarded	Trigger packets discarded

Table 31: show l2tp dial-out Output Fields *(continued)*

Field Name	Field Description
Dial-out session statistics	Statistics at the session level
Sessions active	Currently active sessions
Sessions created	All sessions created
Sessions removed	Sessions deleted
Sessions reset	Sessions reset using the **l2tp dial-out session reset** command
Triggers received	Triggers received for dial-out sessions
Triggers enqueued	Triggers that have been put into the queue
Triggers discarded	Trigger packets discarded
Triggers forwarded	Trigger packets forwarded
Triggers max enqueued	Maximum number of triggers that have been enqueued simultaneously since the last router reset
Authentication requests	Authentication requests received
No resources for authentication	Authentication requests not processed because of insufficient resources
Authentication grants	Authentication requests granted
Authentication Denies	Authentication requests denied
Dial-outs requested	Outgoing calls requested for sessions
Dial-outs rejected	Outgoing call requests that were rejected
Dial-outs established	Successful outgoing calls before the connecting timer expired
Dial-outs timed out	Number of times the connecting timer expired
Dial-outs torn down	Successful outgoing calls that were terminated

Related Documentation

- L2TP Dial-Out Operational States on page 34
- show l2tp dial-out on page 176
- show l2tp dial-out virtual-router on page 179

Monitoring Dial-out Targets within the Current VR Context

Purpose Display configured dial-out targets within the current virtual router context.

This command displays aspects of the dial-out state machine and details about the dial-out routes themselves. This section presents sample output. The actual output on your router may differ significantly.

Action To display general information for all targets within the virtual router:

```
host1:dialout#show l2tp dial-out target
Target          Status      Active Sessions
------          ------      ---------------
10.10.1.1/16    up          14
10.1.1.0/24     up          10
```

To display detailed information about a particular target, specify the target IP address and mask:

```
host1:dialout#show l2tp dial-out target 10.1.1.0/24
Target 10.1.1.0/24
Operational status: up
Active sessions: 10
Total triggers: 127
Failed sessions: 2
Connected sessions: 8
```

To display aggregate counts for targets in each of the possible operational and administrative states:

```
host1:dialout#show l2tp dial-out target summary
```

To display detailed configuration, state, and statistics:

```
host1:dialout#show l2tp dial-out target detail
```

To display information about the operational or administrative state:

```
host1:dialout#show l2tp dial-out target state inService
```

To displays dial-out information across all virtual routers:

```
host1:dialout#show l2tp dial-out target allVirtualRouters
```

NOTE: The level of a user's permission determines the use of the **allVirtualRouters** option. For example, if you have permission to view only the current virtual router, then that is all that is displayed when you enter a command.

Meaning Table 32 on page 163 lists the **show l2tp dial-out target** command output fields.

Table 32: show l2tp dial-out target Output Fields

Field Name	Field Description
Target	Address of the target
Status	Status of the connection to the target
Active Sessions	Currently active session to the target
Total triggers	Trigger packets received for the target
Failed sessions	Sessions that are currently in the failed state
Connected sessions	Sessions that are currently in the connected state

Related Documentation

- L2TP Dial-Out Operational States on page 34
- show l2tp dial-out target on page 178

Monitoring Operational Status within the Current VR Context

Purpose Display dial-out state machine operational status and statistics within the current VR context.

This command displays aspects of the dial-out state machine and details about the dial-out routes themselves. This section presents sample output. The actual output on your router may differ significantly.

Action To display dial-out state machine operational status and statistics within the current VR context:

```
host1#show l2tp dial-out virtual-router
Dial-out Virtual Router Configuration and Operational Status
Virtual router host1:
Virtual router operational status: inService
Maximum trigger buffers per session: 0
```

To display aggregate counts for dial-out state machines in each of the possible operational and administrative states:

```
host1:dialout#show l2tp dial-out virtual-router summary
```

To display detailed configuration, state, and statistics:

```
host1:dialout#show l2tp dial-out virtual-router detail
```

To display information about the operational or administrative state:

```
host1:dialout#show l2tp dial-out virtual-router state down
```

To displays dial-out information across all virtual routers:

```
host1:dialout#show l2tp dial-out virtual-router allVirtualRouters
```

NOTE: The level of a user's permission determines the use of the **allVirtualRouters** option. For example, if you have permission to view only the current virtual router, then that is all that is displayed when you enter a command.

Meaning Table 33 on page 164 lists the **show l2tp dial-out virtual-router** command output fields.

Table 33: show l2tp dial-out virtual-router Output Fields

Field Name	Field Description
Virtual router	Name of VR
Virtual router operational status	Operational status of the VR
Maximum trigger buffers per session	Maximum number of trigger packets held in buffer while the dial-out session is being established

Related Documentation

- L2TP Dial-Out Operational States on page 34
- show l2tp dial-out virtual-router on page 179

Monitoring Status of Dial-out Sessions

Purpose Display the status of dial-out sessions.

This command displays aspects of the dial-out state machine and details about the dial-out routes themselves. This section presents sample output. The actual output on your router may differ significantly.

Action To display all sessions within the current virtual router context:

```
host1#show l2tp dial-out session
Session          Status
---------        ---------
10.10.1.1        connected
10.10.2.1         dormant
```

To display detailed information about a particular session, specify the trigger IP address for the session:

```
host1#show l2tp dial-out session 10.1.1.1
Session 10.1.1.1
Operational status: dormant
```

To display aggregate counts for dial-out sessions in each of the possible operational and administrative states:

```
host1#show l2tp dial-out session summary
```

To display detailed configuration, state, and statistics:

```
host1#show l2tp dial-out session detail
```

To display information about the operational or administrative state:

```
host1#show l2tp dial-out session state connecting
```

To display dial-out information across all virtual routers

```
host1#show l2tp dial-out session allVirtualRouters
```

NOTE: The level of a user's permission determines the use of the **allVirtualRouters** option. For example, if you have permission to view only the current virtual router, then that is all that is displayed when you enter a command.

Meaning Table 34 on page 165 lists the **show l2tp dial-out session** command output fields.

Table 34: show l2tp dial-out session Output Fields

Field Name	Field Description
Session	IP address of the session
Status	Current status of the session
Operational status	Current operational status of session

Related Documentation

- L2TP Dial-Out Operational States on page 34
- **show l2tp dial-out session on page 177**

CHAPTER 24

Monitoring Commands

show aaa domain-map

Syntax show aaa domain-map [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the mapping between user domains and virtual routers. The display includes a tunnel group if one is assigned to the domain map.

Options
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show aaa tunnel-group

Syntax show aaa tunnel-group [*tunnelGroupName*] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays currently configured tunnel groups.

Options
- *tunnelGroupName*—Name of the tunnel group
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show aaa tunnel-parameters

Syntax show aaa tunnel-parameters [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays default tunnel parameters that are configured for tunnel definitions.

Options
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp

Syntax show l2tp [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about the L2TP configuration on the router.

Options
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp destination

Syntax show l2tp destination [detail] [*destinationName* |
[virtual-router *vrName*] ip *ipAddress*] [*filter*]

show l2tp destination summary [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about selected L2TP destinations.

Options

- detail—Provides complete information about the specified destinations, including destination profiles
- *destinationName*—Name the router assigns to the peer at the other end of the tunnel
- *vrName*—Name of the virtual router on which the destination exists
- *ipAddress*—IP address of the peer at the other end of the tunnel
- summary—Displays a summary of destination profile configuration
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp destination lockout

Syntax show l2tp destination lockout [*filter*]

Release Information Command introduced in JunosE Release 7.2.0.

Description Displays information about the L2TP destinations that are currently unavailable because they are in the lockout state.

Options
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp destination profile

Syntax show l2tp destination profile [*profileName*] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays destination profile configuration.

Options
- *profileName*—Name of a profile
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp received-disconnect-cause-summary

Syntax show l2tp received-disconnect-cause-summary [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays aggregate summary statistics for all information received by an LAC from an LNS about the cause of an L2TP session disconnection. The LAC receives this information from the LNS by means of a PPP Disconnect Cause Code attribute value pair (AVP) included in an L2TP Call-Disconnect-Notify (CDN) message.

Options
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp dial-out

Syntax show l2tp dial-out [[detail] [state *operState*] | summary] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the chassis-wide configuration, operational state, and statistics for L2TP dial-out.

Options

- detail—Displays configuration, states, and statistics
- *operState*—One of the following operational states:
  - inService
  - initIncomplete
  - restricted
- summary—Displays aggregate counts for virtual routers, targets, and sessions in each of the possible operational and administrative states
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp dial-out session

Syntax show l2tp dial-out session [*triggerIpAddress* | allVirtualRouters] [detail] [state *operState*] [*filter*]

To display summary information:

show l2tp dial-out session summary [allVirtualRouters] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the status of L2TP dial-out sessions.

Options

- *triggerIpAddress*—Trigger IP address for the session that you want to display
- allVirtualRouters—Displays dial-out information for all virtual routers
- detail—Displays configuration, state, and statistics
- *operState*—One of the following operational states:
  - authenticating
  - connecting
  - dormant
  - failed
  - inService
  - inhibited
  - pending
  - postInhibited
- *filter*—See *Filtering show Commands*
- summary—Displays aggregate counts for dial-out sessions in each of the possible operational and administrative states

Mode Privileged Exec

show l2tp dial-out target

Syntax show l2tp dial-out target [*targetIpAddress targetIpAddressMask* | allVirtualRouters] [detail] [state *operState*] [*filter*]

To display summary information:

show l2tp dial-out target summary [allVirtualRouters] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays configured dial-out targets within the current virtual router context.

Options

- *targetIpAddress*—Trigger IP address for the target that you want to display
- *targetIpAddressMask*—Mask for the trigger IP address
- allVirtualRouters—Displays dial-out information for all virtual routers
- detail—Displays configuration, state, and statistics
- *operState*—One of the following operational states:
  - down
  - inService
  - inhibited
- *filter*—See *Filtering show Commands*
- summary—Displays aggregate counts for targets in each of the possible operational and administrative states

Mode Privileged Exec

show l2tp dial-out virtual-router

Syntax show l2tp dial-out virtual-router [allVirtualRouters] [detail] [state *operState*] [*filter*]

To display summary information:

show l2tp dial-out virtual-router summary [allVirtualRouters] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays dial-out state machine operational status and statistics within the current virtual router context.

Options

- allVirtualRouters—Displays dial-out information across all virtual routers
- detail—Displays configuration, state, and statistics
- *operState*—One of the following operational states:
  - down
  - inService
  - initFailed
  - initPending
- *filter*—See *Filtering show Commands*
- summary—Displays aggregate counts for dial-out state machines in each of the possible operational and administrative states

Mode Privileged Exec

show l2tp session

Syntax show l2tp session [detail] [state { *adminState* | *ifOperStatus* }]
[*l2tpName* | [virtual-router *vrName*] ip *ipAddress* [*l2tpNameNoDest*]] [*filter*]

To display summary information:

show l2tp session summary [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays detailed information about selected L2TP sessions or summary information for all L2TP sessions.

Options

- detail—Provides complete information about the specified sessions
- state—Restricts display to sessions in a specific state
- *adminState*—Effective administrative state
- *ifOperStatus*—Operational state
- *l2tpName*—Session name
- *vrName*—Name of the virtual router on which the session exists
- *ipAddress*—IP address
- *l2tpNameNoDest*—Name of the session
- *filter*—See *Filtering show Commands*
- summary—Displays the configured and operational status of all L2TP sessions

Mode Privileged Exec

show l2tp switch-profile

Syntax show l2tp switch-profile [*profileName*] [*filter*]

Release Information Command introduced in JunosE Release 7.2.0.

Description Displays the names of all L2TP tunnel switch profiles currently configured on the router, or displays detailed information about a particular L2TP tunnel switch profile.

Options
- *profileName*—Name of the tunnel switch profile; a string of up to 64 alphanumeric characters
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp tunnel

Syntax show l2tp tunnel [detail] [state { *adminState* | *ifOperStatus* | failover-resync *failoverResyncMode* }] [*l2tpName* | [virtual-router *vrName*] ip *ipAddress* [*l2tpNameNoDest*]] [*filter*]

To display summary information:

show l2tp tunnel summary [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.
failover-resync keyword and *failoverResyncMode* variable added in JunosE Release 9.0.0.

Description Displays detailed information about the configured and operational status of selected L2TP tunnels or summary information for all L2TP tunnels.

Options

- detail—Provides complete information about the specified sessions, including the L2TP host profile name
- *adminState*—Displays information about tunnels only with the specified effective administrative state
  - enabled—Effective administrative state is disabled
  - disabled—Effective administrative state is enabled
  - drain—Effective administrative state is drain
- *ifOperStatus*—Displays information about tunnels only with the specified operational state
  - up—Operational state is up
  - down—Operational state is down
  - lower-down— Operational state is lower down
  - not-present—Operational state is not-present
- *failoverResyncMode*—Displays information about tunnels that use the specified failover resynchronization mode:
  - disable—Peer failover resynchronization is disabled
  - failover-protocol—Uses the L2TP failover protocol method
  - failover-protocol-fallback-to-silent-failover—Uses the L2TP failover protocol method; however, if the peer does not support this method, the silent failover method is used
  - not-configured—Uses the global failover method because peer failover resynchronization is not configured for L2TP host profiles and AAA domain map tunnels
  - silent-failover—Uses the L2TP silent failover method
- *l2tpName*—Tunnel name

- *vrName*—Name of the virtual router on which the tunnel exists
- *ipAddress*—IP address
- *l2tpNameNoDest*—Tunnel name
- *filter*—See *Filtering show Commands*
- summary—Displays the configured and operational status of all L2TP tunnels

Mode Privileged Exec

PART 4

Index

Index

M

N

O

P

Q

R

S

T

U

V