



JunosE™ Software for E Series™ Broadband Services Routers

L2TP Operations

Release

13.3.x



Published: 2012-09-24

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

Copyright © 2012, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

JunosE™ Software for E Series™ Broadband Services Routers L2TP Operations
Release 13.3.x
Copyright © 2012, Juniper Networks, Inc.
All rights reserved.

Revision History
October 2012—FRS JunosE 13.3.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

	About the Documentation	xi
	E Series and JunosE Documentation and Release Notes	xi
	Audience	xi
	E Series and JunosE Text and Syntax Conventions	xi
	Obtaining Documentation	xiii
	Documentation Feedback	xiii
	Requesting Technical Support	xiii
	Self-Help Online Tools and Resources	xiv
	Opening a Case with JTAC	xiv
Part 1	Overview	
Chapter 1	L2TP Functionalities	3
	L2TP Overview	3
	L2TP Terminology	4
	Packet Fragmentation	5
Chapter 2	L2TP Deployment	7
	Implementing L2TP	7
	Sequence of Events on the LAC	7
	Sequence of Events on the LNS	8
Chapter 3	L2TP Platform and Module Requirements	9
	L2TP Module Requirements	9
	ERX7xx Models, ERX14xx Models, and the ERX310 Router	9
	E120 Router and E320 Router	10
	L2TP Platform Considerations	10
	L2TP References	10
Chapter 4	L2TP Sessions and Tunnels	13
	Sessions and Tunnels Supported	13
Chapter 5	Termination of PPP and L2TP Subscriber Sessions	15
	VSAs for Dynamic IP Interfaces Overview	15
	Traffic Shaping for PPP over ATM Interfaces	16
	Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes	17
Chapter 6	How L2TP Dial-Out Works	21
	L2TP Dial-Out Overview	21
	L2TP Dial-Out Platform Considerations	22
	L2TP Dial-Out References	22
	L2TP Dial-Out Network Model	22

	L2TP Dial-Out Process	23
	L2TP Dial-Out Operational States	24
	Chassis	24
	Virtual Router	24
	Targets	24
	Sessions	25
	L2TP Dial-Out Outgoing Call Setup Details	27
	Access-Request Message	27
	Access-Accept Message	27
	Outgoing Call	28
	Mutual Authentication	28
	Route Installation	29
Part 2	Configuration	
Chapter 7	Configuring L2TP Dial-Out	33
	Configuring L2TP Dial-Out	33
	Creating an L2TP Dial-Out Session	33
	Specifying the Maximum Timeout Period for Establishing an L2TP Dial-Out Session	34
	Specifying the Duration for an L2TP Dial-Out Session to Remain in Dormant State	34
	Specifying the Maximum Triggers to Buffer for an L2TP Dial-Out Session	34
	Deleting an L2TP Dial-Out Session	35
	Resetting an L2TP Dial-Out Session	35
Chapter 8	Configuring a LAC Device in an L2TP Tunnel	37
	Mapping User Domain Names to L2TP Tunnels from Domain Map Tunnel Mode	37
	Mapping User Domain Names to L2TP Tunnels from Tunnel Group Tunnel Mode	41
Chapter 9	Configuring an LNS Device in an L2TP Tunnel	45
	Configuring an LNS	45
Chapter 10	Configuration Commands	49
	aaa domain-map	50
	aaa tunnel assignment-id-format	51
	aaa tunnel client-name	52
	aaa tunnel ignore	53
	aaa tunnel password	54
	address	55
	bundled-group-id	56
	bundled-group-id-overrides-mlppp-ed	57
	client-name	58
	identification	59
	default-upper-type mlppp	60
	disable proxy lcp	61
	enable proxy authenticate	62

	l2tp destination profile	63
	l2tp disable challenge	64
	l2tp ignore-receive-data-sequencing	65
	local host	66
	local ip address	67
	max-sessions	69
	medium ipv4	70
	password	71
	preference	73
	radius connect-info-format	74
	remote host	75
	router-name	76
	server-name	77
	session-out-of-resource-result-code-override	78
	source-address	79
	tunnel	80
	tunnel group	81
	type	82
	tunnel password	83
Part 3	Administration	
Chapter 11	Monitoring L2TP Dial-Out	87
	Monitoring Chassis-wide Configuration for L2TP Dial-out	87
	Monitoring Dial-out Targets within the Current VR Context	92
	Monitoring Operational Status within the Current VR Context	93
	Monitoring Status of Dial-out Sessions	94
Chapter 12	Verifying the Cause Codes for Termination of L2TP Sessions	97
	L2TP Disconnect Cause Codes	97
	L2TP Terminate Reasons	101
	PPP Terminate Reasons	118
	Configuring Custom Mappings for PPP Terminate Reasons	125
Chapter 13	Monitoring Consolidated L2TP Details	127
	Monitoring Detailed Configuration Information for Specified Destinations	127
	Monitoring Global Configuration Status on E Series Routers	129
	Monitoring Locked Out Destinations	131
Chapter 14	Monitoring L2TP Disconnect Cause-Codes	133
	Monitoring Statistics on the Cause of a Session Disconnection	133
Chapter 15	Monitoring L2TP Sessions	135
	Monitoring Detailed Configuration Information about Specified Sessions	135
	Monitoring Configured and Operational Summary Status	136
Chapter 16	Monitoring Commands	139
	show l2tp	140
	show l2tp destination	141
	show l2tp destination lockout	142
	show l2tp destination profile	143

show l2tp received-disconnect-cause-summary	144
show l2tp dial-out	145
show l2tp dial-out session	146
show l2tp dial-out target	147
show l2tp dial-out virtual-router	148
show l2tp session	149

Part 4

Index

Index	153
-----------------	-----

List of Figures

Part 1	Overview	
Chapter 1	L2TP Functionalities	3
	Figure 1: Using the E Series Router as an LAC	3
	Figure 2: Using the E Series Router as an LNS	4
Chapter 6	How L2TP Dial-Out Works	21
	Figure 3: Network Model for Dial-Out	21

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xii
	Table 2: Text and Syntax Conventions	xii
Part 1	Overview	
Chapter 1	L2TP Functionalities	3
	Table 3: L2TP Terms	4
Chapter 5	Termination of PPP and L2TP Subscriber Sessions	15
	Table 4: VSAs That Apply to Dynamic IP Interfaces	15
	Table 5: Traffic-Shaping VSAs That Apply to Dynamic IP Interfaces	17
	Table 6: Supported RADIUS Acct-Terminate-Cause Codes	18
Chapter 6	How L2TP Dial-Out Works	21
	Table 7: Chassis Operational States	24
	Table 8: Virtual Router Operational States	24
	Table 9: Target Operational States	25
	Table 10: Session Operational States	25
	Table 11: Additions to RADIUS Attributes in Access-Accept Messages	27
Part 3	Administration	
Chapter 11	Monitoring L2TP Dial-Out	87
	Table 12: show l2tp dial-out Output Fields	89
	Table 13: show l2tp dial-out target Output Fields	93
	Table 14: show l2tp dial-out virtual-router Output Fields	94
	Table 15: show l2tp dial-out session Output Fields	95
Chapter 12	Verifying the Cause Codes for Termination of L2TP Sessions	97
	Table 16: PPP Disconnect Cause Codes	98
	Table 17: Default L2TP Mappings	101
	Table 18: Default PPP Mappings	118
Chapter 13	Monitoring Consolidated L2TP Details	127
	Table 19: show l2tp destination Output Fields	128
	Table 20: show l2tp Output Fields	129
	Table 21: show l2tp destination lockout Output Fields	131
Chapter 14	Monitoring L2TP Disconnect Cause-Codes	133
	Table 22: show l2tp received-disconnect-cause-summary Output Fields	134
Chapter 15	Monitoring L2TP Sessions	135

Table 23: show l2tp session Output Fields	136
Table 24: show l2tp session summary Output Fields	137

About the Documentation

- E Series and JunosE Documentation and Release Notes on page xi
- Audience on page xi
- E Series and JunosE Text and Syntax Conventions on page xi
- Obtaining Documentation on page xiii
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiii

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 xii 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 xii 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.	<ul style="list-style-type: none"> 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)
<i>Italic text like this</i>	<ul style="list-style-type: none"> Emphasizes words. Identifies variables. Identifies chapter, appendix, and book names. 	<ul style="list-style-type: none"> There are two levels of access: <i>user</i> and <i>privileged</i>. <i>clusterId</i>, <i>ipAddress</i>. <i>Appendix A, System Specifications</i>
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
<i>Italic text like this</i>	Represents variables.	<i>mask</i> , <i>accessListName</i>

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 at <http://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

- [L2TP Functionalities on page 3](#)
- [L2TP Deployment on page 7](#)
- [L2TP Platform and Module Requirements on page 9](#)
- [L2TP Sessions and Tunnels on page 13](#)
- [Termination of PPP and L2TP Subscriber Sessions on page 15](#)
- [How L2TP Dial-Out Works on page 21](#)

CHAPTER 1

L2TP Functionalities

- [L2TP Overview on page 3](#)
- [L2TP Terminology on page 4](#)
- [Packet Fragmentation on page 5](#)

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

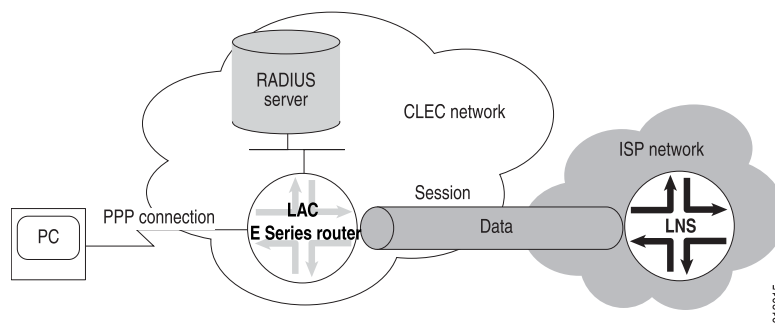
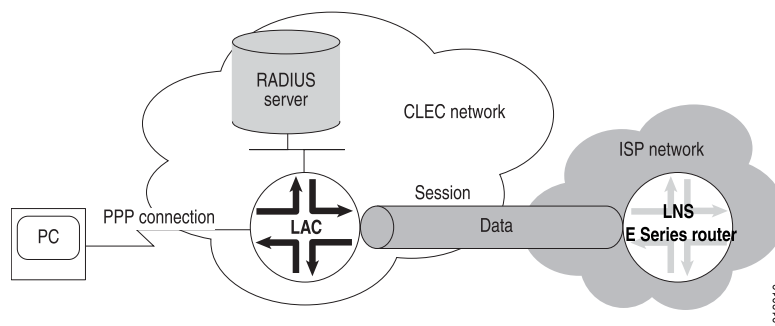


Figure 2: Using the E Series Router as an LNS



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

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.
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.

Table 3: L2TP Terms (*continued*)

Term	Description
Session	<p>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.</p> <p>NOTE: There is a one-to-one relationship between established L2TP sessions and their associated PPP connections.</p>
Tunnel	A connection between an LAC-LNS pair consisting of a control connection and 0 or more L2TP sessions.

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.

CHAPTER 2

L2TP Deployment

- [Implementing L2TP on page 7](#)

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.

CHAPTER 3

L2TP Platform and Module Requirements

- [L2TP Module Requirements on page 9](#)
- [L2TP Platform Considerations on page 10](#)
- [L2TP References on page 10](#)

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*.

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.

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*.

CHAPTER 4

L2TP Sessions and Tunnels

- [Sessions and Tunnels Supported on page 13](#)

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*.

CHAPTER 5

Termination of PPP and L2TP Subscriber Sessions

- [VSAs for Dynamic IP Interfaces Overview on page 15](#)
- [Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 17](#)

VSAs for Dynamic IP Interfaces Overview

[Table 4 on page 15](#) 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 4: 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: <i>input-policy-name</i>
Egress-Policy-Name	Specifies the name of the output (egress) policy	26	len	11	sublen	string: <i>output-policy-name</i>
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 4: 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: <i>qos-profile-name</i>

To use the VSAs shown in [Table 4 on page 15](#):

- 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 16](#)

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 5 on page 17](#) describes VSAs that apply to dynamic IP interfaces and are supported on a per-user basis from RADIUS.

Table 5: 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](#)

Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes

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 6 on page 18](#) 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 6: 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 6: 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 on page 125](#)

CHAPTER 6

How L2TP Dial-Out Works

- [L2TP Dial-Out Overview on page 21](#)
- [L2TP Dial-Out Platform Considerations on page 22](#)
- [L2TP Dial-Out References on page 22](#)
- [L2TP Dial-Out Network Model on page 22](#)
- [L2TP Dial-Out Process on page 23](#)
- [L2TP Dial-Out Operational States on page 24](#)
- [L2TP Dial-Out Outgoing Call Setup Details on page 27](#)

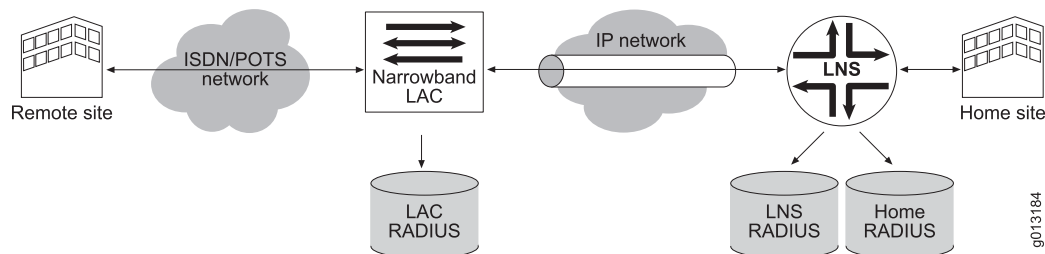
L2TP Dial-Out Overview

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 21](#) 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 22](#)
- [L2TP Dial-Out Operational States on page 24](#)
- [L2TP Dial-Out Process on page 23](#)
- [L2TP Dial-Out Outgoing Call Setup Details on page 27](#)

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 21](#)
- [L2TP Dial-Out Network Model on page 22](#)

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 21](#)
- [L2TP Dial-Out Network Model on page 22](#)

L2TP Dial-Out Network Model

In the figure in “[L2TP Dial-Out Overview](#)” on [page 21](#), 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 21](#)
- [L2TP Dial-Out Terms](#)
- [L2TP Dial-Out Operational States on page 24](#)
- [L2TP Dial-Out Process on page 23](#)
- [L2TP Dial-Out Outgoing Call Setup Details on page 27](#)

L2TP Dial-Out Process

The following is the dial-out process used in the network model illustrated in “[L2TP Dial-Out Overview](#)” on page 21:

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 21](#)
- [L2TP Dial-Out Terms](#)
- [L2TP Dial-Out Network Model on page 22](#)
- [L2TP Dial-Out Operational States on page 24](#)
- [L2TP Dial-Out Outgoing Call Setup Details on page 27](#)

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 7 on page 24](#) describes the operational states of the chassis.

Table 7: 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 8 on page 24](#) describes the operational states of the virtual router.

Table 8: 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 9 on page 25](#) describes the operational states of the targets.

Table 9: Target Operational States

State	Description
inService	Dial-out route is up and operational.
inhibited	<p>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.</p> <p>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.</p>
down	<p>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.</p> <p>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.</p>

Sessions

Table 10 on page 25 describes operational states of the sessions.

Table 10: Session Operational States

State	Description
authenticating	<p>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.</p> <p>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.</p>
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 10: Session Operational States (*continued*)

State	Description
inhibited	<p>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.</p> <p>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.</p> <ul style="list-style-type: none"> • 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	<p>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.</p>
dormant	<p>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.</p>
pending	<p>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.</p>
failed	<p>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.</p> <p>The only way to exit the failed state is with the l2tp dial-out session reset command.</p>

- Related Documentation**
- [L2TP Dial-Out Overview on page 21](#)
 - [L2TP Dial-Out Terms](#)
 - [L2TP Dial-Out Network Model on page 22](#)
 - [L2TP Dial-Out Process on page 23](#)
 - [L2TP Dial-Out Outgoing Call Setup Details on page 27](#)

L2TP Dial-Out Outgoing Call Setup Details

This section details the process described in “[L2TP Dial-Out Process](#)” on page 23.

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 11 on page 27](#). 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 11: 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 11: 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 21](#)
- [L2TP Dial-Out Terms](#)
- [L2TP Dial-Out Network Model on page 22](#)
- [L2TP Dial-Out Operational States on page 24](#)
- [L2TP Dial-Out Process on page 23](#)

PART 2

Configuration

- [Configuring L2TP Dial-Out on page 33](#)
- [Configuring a LAC Device in an L2TP Tunnel on page 37](#)
- [Configuring an LNS Device in an L2TP Tunnel on page 45](#)
- [Configuration Commands on page 49](#)

CHAPTER 7

Configuring L2TP Dial-Out

- [Configuring L2TP Dial-Out on page 33](#)

Configuring L2TP Dial-Out

L2TP dial-out configuration tasks include the following sets of tasks:

- [Creating an L2TP Dial-Out Session on page 33](#)
- [Specifying the Maximum Timeout Period for Establishing an L2TP Dial-Out Session on page 34](#)
- [Specifying the Duration for an L2TP Dial-Out Session to Remain in Dormant State on page 34](#)
- [Specifying the Maximum Triggers to Buffer for an L2TP Dial-Out Session on page 34](#)
- [Deleting an L2TP Dial-Out Session on page 35](#)
- [Resetting an L2TP Dial-Out Session on page 35](#)

Creating an L2TP Dial-Out Session

You can define an L2TP dial-out target by using the **l2tp dial-out target** command. When the router receives packets destined for the target, it creates a dial-out session.

To create a dial-out session:

- Issue the **l2tp dial-out target** command in Global Configuration mode.

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

When you create a target, you must specify the following:

- *ipAddress*—IP address of the target
- *ipAddressMask*—IP address mask of the target
- *domainName*—Domain name used in the outgoing call Access-Request message
- *profileName*—Name of profile used to create the interface stack

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

Specifying the Maximum Timeout Period for Establishing an L2TP Dial-Out Session

You can optionally set the maximum time allowed for successful establishment of an L2TP dial-out session.

To set the maximum time allowed for attempts to establish L2TP dial-out sessions:

- Issue the **l2tp dial-out connecting-timer-value** command in Global Configuration mode.

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

If the session fails to be established before the connecting timer expires, subsequent attempts to establish the dial-out session to the same destination are inhibited temporarily. The range is 30–3600 seconds.

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

Specifying the Duration for an L2TP Dial-Out Session to Remain in Dormant State

You can optionally specify the duration for which the dial-out session stays in the dormant state waiting for a new trigger after the associated L2TP outgoing call ends.

To set how long the dial-out session waits in the dormant state for a new trigger after the associated L2TP outgoing call ends:

- Issue the **l2tp dial-out dormant-timer-value** command in Global Configuration mode.

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

If no trigger is received before the dormant timer expires, the dial-out session is deleted. The range is 0–3600 seconds.

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

Specifying the Maximum Triggers to Buffer for an L2TP Dial-Out Session

You can optionally set the maximum number of buffered trigger packets held for any dial-out session pending the successful establishment of the L2TP session. Once the session is established, the buffered trigger packets are transmitted.

To set the maximum number of trigger packets held in buffer while the dial-out session is being established:

- Issue the **l2tp dial-out max-buffered-triggers** command in Global Configuration mode.

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

If the configured maximum number of buffered trigger packets is exceeded, any new trigger packets received are discarded. The range of values is 0–50.

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

Deleting an L2TP Dial-Out Session

You can manually delete a dial-out session to close any L2TP outgoing call associated with the dial-out session.

To delete a dial-out session:

- Issue the **l2tp dial-out session delete** command in Global Configuration mode.

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

There is no **no** version.

Resetting an L2TP Dial-Out Session

You can reset a dial-out session by forcing it to the dormant state. After you reset a dial-out session, any L2TP outgoing call associated with that session is closed.

To force the dial-out session to the dormant state where it remains until the dormant timer expires or it receives a new trigger:

- Issue the **l2tp dial-out session reset** command in Global Configuration mode.

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

There is no **no** version.

Related Documentation

- [L2TP Dial-Out Network Model on page 22](#)
- [L2TP Dial-Out Process on page 23](#)
- [L2TP Dial-Out Outgoing Call Setup Details on page 27](#)
- [Monitoring Chassis-wide Configuration for L2TP Dial-out on page 87](#)
- [Monitoring Status of Dial-out Sessions on page 94](#)
- [Monitoring Dial-out Targets within the Current VR Context on page 92](#)
- [Monitoring Operational Status within the Current VR Context on page 93](#)
- `l2tp dial-out connecting-timer-value`
- `l2tp dial-out dormant-timer-value`
- `l2tp dial-out max-buffered-triggers`
- `l2tp dial-out session delete`
- `l2tp dial-out session reset`
- `l2tp dial-out target`

CHAPTER 8

Configuring a LAC Device in an L2TP Tunnel

- Mapping User Domain Names to L2TP Tunnels from Domain Map Tunnel Mode on page 37
- Mapping User Domain Names to L2TP Tunnels from Tunnel Group Tunnel Mode on page 41

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

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

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

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

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

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

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

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

4. Specify the LNS endpoint address of a tunnel.

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

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

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

6. Specify a preference for the tunnel.

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

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

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

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



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

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

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

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



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

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

This name specifies the hostname expected from the peer (the LNS) when you set up a tunnel. When this name is specified, the peer must identify itself with this name during tunnel startup. Otherwise, the tunnel is terminated. The server name can be up to 64 characters (no spaces).

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

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

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

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

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

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

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

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

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

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

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

14. (Optional) Specify a default tunnel client name.

```
host1(config-domain-map-tunnel)#exit
host1(config-domain-map)#exit
host1(config)#aaa tunnel client-name boxford
```

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

15. (Optional) Specify a default tunnel password.

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

20. Verify the L2TP tunnel configuration.

```
host1(config)# show aaa domain-map
Domain: westford.com; router-name: default; ipv6-router-name: default
```

```

Tunnel
Tunnel Client
Tag Name Peer Source Type Medium Password Id
-----
3 192.168.2.13 192.168.3.3 l2tp ipv4 temporary acton
host4

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

```

```

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

```

Related Documentation

- [Mapping User Domain Names to L2TP Tunnels from Tunnel Group Tunnel Mode on page 41](#)
- [aaa domain-map on page 50](#)
- [aaa tunnel assignment-id-format on page 51](#)
- [aaa tunnel client-name on page 52](#)
- [aaa tunnel ignore on page 53](#)
- [aaa tunnel password on page 54](#)
- [address on page 55](#)
- [client-name on page 58](#)
- [identification on page 59](#)
- [l2tp disable challenge on page 64](#)
- [l2tp ignore-receive-data-sequencing on page 65](#)
- [medium ipv4 on page 70](#)
- [password on page 71](#)
- [preference on page 73](#)
- [router-name on page 76](#)
- [server-name on page 77](#)
- [source-address on page 79](#)
- [tunnel on page 80](#)
- [tunnel group on page 81](#)

- [type on page 82](#)

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

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

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

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

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

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

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

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

4. Specify the LNS endpoint address of a tunnel.

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

5. Specify a preference for the tunnel.

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

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

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

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



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

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

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

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



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

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

This name specifies the hostname expected from the peer (the LNS) when you set up a tunnel. When this name is specified, the peer must identify itself with this name during tunnel startup. Otherwise, the tunnel is terminated. The server name can be up to 64 characters (no spaces).

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

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

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

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

10. Specify a tunnel identification.

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

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

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

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

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

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

13. Verify the L2TP tunnel configuration.

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

```
Domain: westford.com; router-name: default; ipv6-router-name: default
```

Tunnel Client Tag Name	Tunnel Peer	Tunnel Source	Tunnel Type	Tunnel Medium	Tunnel Password	Tunnel Id
3 host4	192.168.2.13	192.168.3.3	l2tp	ipv4	temporary	acton

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

```
host1#show aaa tunnel-parameters
```

```
Tunnel password is 3&92k%b#q4
```

```
Tunnel client-name is <NULL>
```

```
Tunnel nas-port-method is none
```

```
Tunnel nas-port ignore disabled
```

```
Tunnel nas-port-type ignore disabled
```

tunnel assignmentId format is assignmentId
aaa tunnel calling number format is descriptive

**Related
Documentation**

- [Mapping User Domain Names to L2TP Tunnels from Domain Map Tunnel Mode on page 37](#)
- [aaa tunnel-group](#)
- [address on page 55](#)
- [client-name on page 58](#)
- [identification on page 59](#)
- [medium ipv4 on page 70](#)
- [password on page 71](#)
- [preference on page 73](#)
- [router-name on page 76](#)
- [server-name on page 77](#)
- [source-address on page 79](#)
- [tunnel on page 80](#)
- [type on page 82](#)

CHAPTER 9

Configuring an LNS Device in an L2TP Tunnel

- [Configuring an LNS on page 45](#)

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](#).

```
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*.

```
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 sac0
```

9. (Optional) Specify that the LNS override out-of-resource result codes 4 and 5 with code 2 for interoperability 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 *Overview of Mapping a User Domain to a Virtual Router*.

Related Documentation

- Creating an L2TP Destination Profile
- Creating an L2TP Host Profile
- Configuring the Maximum Number of LNS Sessions
- Configuring the RADIUS Connect-Info Attribute on the LNS
- Overriding LNS Out-of-Resource Result Codes 4 and 5
- Selecting Service Modules for LNS Sessions Using MLPPP
- [bundled-group-id on page 56](#)
- [bundled-group-id-overrides-mlppp-ed on page 57](#)
- [default-upper-type mlppp on page 60](#)
- [disable proxy lcp on page 61](#)
- [enable proxy authenticate on page 62](#)
- [l2tp destination profile on page 63](#)
- [local host on page 66](#)
- [local ip address on page 67](#)
- [max-sessions on page 69](#)
- [radius connect-info-format on page 74](#)
- [remote host on page 75](#)
- [session-out-of-resource-result-code-override on page 78](#)
- [tunnel password on page 83](#)

CHAPTER 10

Configuration Commands

aaa domain-map

Syntax `aaa domain-map domainName`
 `[routerName [loopback interfaceNumber | ipAddress ipMask]]`

 `no aaa domain-map domainName`

Release Information Command introduced before JunosE Release 7.1.0.
 ipAddress and *ipMask* variables added in JunosE Release 9.0.0.

Description Maps a user domain name to a virtual router. When you specify only the domain name, the command sets the mode to Domain Map Configuration. The **no** version deletes the map entry.

- Options**
- *domainName*—User domain name; specify the domain name *none* to assign users without domains to a specific virtual router.
 - *routerName*—Router name associated with the domain name
 - *loopback*—Specifies the loopback interface
 - *interfaceNumber*—Interface number in the range 0–32000
 - *ipAddress*—IP address of the local interface
 - *ipMask*—IPv4 address mask of the local interface

Mode Global Configuration

aaa tunnel assignment-id-format

Syntax aaa tunnel assignment-id-format { assignmentId | client-server-id }
 no aaa tunnel assignment-id-format

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets the format for the tunnel assignment ID. The **no** version sets the tunnel assignment ID to the default, assignmentID.

- Options**
- assignmentId—Configures the format to be assignmentId only
 - client-server-id—Configures the format to be a combination of clientAuthId + serverAuthId + assignmentId

Mode Global Configuration

aaa tunnel client-name

Syntax `aaa tunnel client-name name`
 `no aaa tunnel client-name`

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the default tunnel client name. If the tunnel client name is not included in the tunnel attributes that are returned from the domain map or authentication server, the router uses the default name. The **no** version deletes the client name.

Options • *name*—Default tunnel client name; a string of up to 32 characters

Mode Global Configuration

aaa tunnel ignore

Syntax `aaa tunnel ignore { nas-port | nas-port-type } { enable | disable }`
`no aaa tunnel ignore { nas-port | nas-port-type }`

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies whether to use the tunnel peer's NAS-Port [5] and NAS-Port-Type [61] attributes. The **no** version negates the command or restores the default of enable.

- Options**
- `nas-port`—Configures the tunnel peer's supplied nas-port value
 - `nas-port-type`—Configures the tunnel peer's supplied nas-port-type value
 - `enable`—Implements the feature; this is the default setting
 - `disable`—Disables the feature

Mode Global Configuration

aaa tunnel password

Syntax `aaa tunnel password name`
 `no aaa tunnel password`

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the default tunnel password. If the tunnel password is not included in the tunnel attributes that are returned from the domain map or authentication server, the router uses the default password. The **no** version deletes the password.

Options • *name*—Default tunnel password; a string of up to 32 characters

Mode Global Configuration

address

Syntax To set the tunnel endpoint address:

`address serverAddress`

`no address`

To configure RIP:

`[no] address { ipAddress | unnumbered interfaceType interfaceSpecifier }`

To configure NAT address pool ranges:

`[no] address startIpAddress endIpAddress`

Release Information Command introduced before JunosE Release 7.1.0.

Description From Domain Map Tunnel Configuration mode, sets the tunnel endpoint address of an L2TP tunnel. The **no** version removes the address of the tunnel.

From Tunnel Group Tunnel Configuration mode, sets the tunnel endpoint address of an L2TP tunnel. The **no** version removes the address of the tunnel.

From Interface Configuration or Subinterface Configuration mode, configures RIP to run on the interface specified by the IP address or on an unnumbered interface. Uses the default values: send version is RIP version 1, receive version is RIP version 1 and version 2, authentication is not enabled. The **no** version deletes the RIP interface. Use the **address** commands to configure RIP attributes on the network.

From IP NAT Pool Configuration mode, configures NAT IP address pool ranges. The **no** version removes the range from the current NAT address pool.

- Options**
- *serverAddress*—IP address of the LNS endpoint
 - *ipAddress*—Address of IP interface where RIP will be run
 - unnumbered—Specifies that RIP will be run on an unnumbered interface
 - *interfaceType*—Interface type; see Interface Types and Specifiers
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers
 - *startIpAddress*—Starting IP address (inclusive) of the NAT pool range you are creating
 - *endIpAddress*—Ending IP address (inclusive) of the NAT pool range you are creating

Mode Address Family Configuration (RIP), Domain Map Tunnel Configuration, IP NAT Pool Configuration, Router Configuration (RIP), Tunnel Group Tunnel 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

client-name

Syntax client-name *clientname*
 no client-name

Release Information Command introduced before JunosE Release 7.1.0.

Description From Domain Map Tunnel Configuration or Tunnel Group Tunnel Configuration mode, sets a hostname for a tunnel that the LAC uses when communicating with the LNS about the tunnel. The **no** version removes the hostname from the tunnel.



.....
NOTE: In Domain Map Tunnel Configuration mode, this command is replacing the hostname command. The hostname command may be removed completely from Domain Map Tunnel Configuration mode in a future release.
.....

Options • *clientname*—String of up to 64 characters (no spaces)

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel Configuration

identification

Syntax `identification serverId`

`no identification`

Release Information Command introduced before JunosE Release 7.1.0.

Description From Domain Map Tunnel Configuration or Tunnel Group Tunnel mode, specifies the assignment ID of an L2TP tunnel. The **no** version removes the assignment ID from the tunnel.

Options • *serverId*—L2TP tunnel assignment ID up to 32 characters

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel

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

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

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 disable challenge

Syntax [no] l2tp disable challenge

Release Information Command introduced before JunosE Release 7.1.0.

Description Disables the generation of local tunnel authentication challenges. The **no** version enables local challenge generation, which is the default setting.

Mode Global Configuration

l2tp ignore-receive-data-sequencing

Syntax [no] l2tp ignore-receive-data-sequencing

Release Information Command introduced before JunosE Release 7.1.0.

Description Suppresses sequence number checking for data packets received on all L2TP tunnels in the router. This setting affects only packets received on a tunnel, not packets sent on a tunnel. The L2TP LAC still inserts sequence numbers into data packets if the LAC receives packets from the LNS that contain sequence numbers. The **no** version restores the default, which causes the router to check the sequence numbers in data packets that it receives on L2TP tunnels.



.....
NOTE: If you are using IP reassembly, we recommend that you set up the router to ignore sequence numbers in received data packets. Because IP reassembly may reorder L2TP packets, out-of-order packets may be dropped if sequence numbers are being used on L2TP data packets.
.....

Mode Global Configuration

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

medium ipv4

Syntax medium ipv4
 no medium

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the medium type of a tunnel to IPv4 (the only medium type currently supported).
 The **no** version restores the default value, ipv4.

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel Configuration

password

Syntax Login password:

`password [encryptionType] passwordValue`

`no password`

L2TP tunnel password:

`password tunnelPassword`

`no password`

IP service profile password:

`password servicePassword`

`no password`

Local user database password:

`password [encryptionType] passwordValue`

`no password`

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures a password to be used at login on the console, a line or a range of lines. For L2TP, specifies the password for an AAA domain map or tunnel group tunnel. For IP service profiles, specifies the password for the profile. For the local authentication server feature, adds a password to a user entry in the local user database. If you enable password checking but do not configure a password, the system will not allow you to access virtual terminals. Specify a password in plain text (unencrypted) or cipher text (encrypted). In either case, the system stores the password as encrypted. The **no** version removes the password.



NOTE: To use an encrypted password, you must follow the procedure in *Creating Encrypted Passwords* in the *JunosE System Basics Configuration Guide* to obtain the encrypted password. You cannot create your own encrypted password; you must use a router-generated password or secret.

- Options**
- *encryptionType*—One of the following types:
 - 0—Unencrypted (the default)
 - 5—Secret

- 7—Encrypted
- *passwordValue*—Character string that specifies the line password. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 50 characters. The password checking is case sensitive.
- *tunnelPassword*—Password of up to 32 characters
- *servicePassword*—Password of up to 32 characters
- *encryptionType*—One of the following types:
 - 0—Unencrypted password (the default)
 - 8—Two-way encrypted password
- *passwordValue*—Character string that specifies the password. The string can contain any alphanumeric character, including spaces, up to 64 characters. Passwords are case sensitive.

Mode Domain Map Tunnel Configuration (for a tunnel password), IP Service Profile Configuration (for a service profile password), Line Configuration (for a login password), Local User Configuration (for a local user database password), Tunnel Group Tunnel Configuration (for a tunnel group tunnel password)

preference

Syntax `preference tunnelPreference`

`no preference`

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the preference value for an L2TP tunnel. The **no** version restores the default value, 2000.

Options • *tunnelPreference*—Tunnel preference, in the range 0–2000; 0 is the highest preference

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel 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

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

router-name

Syntax `router-name vrName`
 `no router-name [vrName]`

Release Information Command introduced before JunosE Release 7.1.0.

Description Maps a virtual router to a user domain name. The **no** version deletes the router name parameter, and the router defaults to the default virtual router.



.....
NOTE: This command is deprecated and might be removed completely in a future release. The functionality provided by this command has been replaced by the **auth-router-name** and **ip-router-name** commands.
.....

Options • *vrName*—Name of the virtual router to map to the user domain name

Mode Domain Map Configuration, Tunnel Group Tunnel Configuration

server-name

Syntax `server-name serverName`

`no server-name`

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the hostname expected from the L2TP LNS when you set up a tunnel. The **no** version removes the server name.

Options • *serverName*—Hostname; can be up to 64 characters in length (no spaces)

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel Configuration

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

source-address

Syntax `source-address sourceAddress`
`no source-address`

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies a source IP address for the LAC tunnel endpoint. The **no** version removes the source address.

Options • *sourceAddress*—Address of the local tunnel endpoint (the LAC); can be up to 32 characters (no spaces)

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel Configuration

tunnel

Syntax [no] tunnel *tag*

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies an L2TP tunnel and changes the mode to Domain Map Tunnel Configuration. In Domain Map Tunnel Configuration mode, you can set the attributes of the tunnel. The **no** version deletes the L2TP tunnel configuration from the router.

From Tunnel Group Configuration mode, adds up to 31 tunnel definitions to the L2TP tunnel group and changes the mode to Tunnel Group Tunnel Configuration mode. In Tunnel Group Tunnel Configuration mode, you can set tunnel attributes. The **no** version deletes the L2TP tunnel group configuration from the router.

Options • *tag*—Number in the range 1–31

Mode Domain Map Configuration, Tunnel Group Configuration

tunnel group

Syntax `tunnel group tunnelGroupName`
`no tunnel group`

Release Information Command introduced before JunosE Release 7.1.0.

Description Assigns the specified tunnel group to the domain map. The **no** version deletes the tunnel group.



.....
NOTE: By default, no tunnel group is assigned to the domain map. You can assign a tunnel group to the domain map only if tunnels are not currently defined for the domain map in Domain Map Tunnel mode.
.....

Options • *tunnelGroupName*—String of up to 64 characters (no spaces)

Mode Domain Map Configuration

type

Syntax To configure the RTR operation:

```
[ no ] type rtrType protocol ipicmpEcho destination  
[ source-ipaddr srcAddr | source interfaceType interfaceSpecifier ]
```

To specify the L2TP tunnel type:

```
type tunnelType
```

```
no type
```

Release Information Command introduced before JunosE Release 7.1.0.

Description From RTR Configuration mode, configures an RTR operation. The **no** version removes the configured type from the operation and resets all configuration for an RTR index.



NOTE: You must configure the operation's type before you can configure any other characteristics of the operation.

From Domain Map Configuration and Tunnel Group Tunnel Configuration modes, specifies the L2TP tunnel type (RADIUS attribute 64, Tunnel-Type).

- Options**
- *rtrType*—One of the following types of operation:
 - *echo*—Performs end-to-end operation only
 - *pathEcho*—Discovers a path to the destination and echoes each device on the path
 - *destination*—IP address or an IP hostname or domain name
 - *srcAddr*—Source IP address
 - *interfaceType*—Interface type; see Interface Types and Specifiers
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers
 - *tunnelType*—L2TP tunnel type

Mode Domain Map Configuration, RTR Configuration, Tunnel Group Tunnel 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

PART 3

Administration

- [Monitoring L2TP Dial-Out on page 87](#)
- [Verifying the Cause Codes for Termination of L2TP Sessions on page 97](#)
- [Monitoring Consolidated L2TP Details on page 127](#)
- [Monitoring L2TP Disconnect Cause-Codes on page 133](#)
- [Monitoring L2TP Sessions on page 135](#)
- [Monitoring Commands on page 139](#)

Monitoring L2TP Dial-Out

- [Monitoring Chassis-wide Configuration for L2TP Dial-out on page 87](#)
- [Monitoring Dial-out Targets within the Current VR Context on page 92](#)
- [Monitoring Operational Status within the Current VR Context on page 93](#)
- [Monitoring Status of Dial-out Sessions on page 94](#)

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 12 on page 89 lists the **show l2tp dial-out** command output fields.

Table 12: 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 12: 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 12: 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 24](#)
 - [show l2tp dial-out on page 145](#)
 - [show l2tp dial-out virtual-router on page 148](#)

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 13 on page 93 lists the **show l2tp dial-out target** command output fields.

Table 13: 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 24](#)
 - [show l2tp dial-out target on page 147](#)

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 14 on page 94](#) lists the `show l2tp dial-out virtual-router` command output fields.

Table 14: 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 24](#)
 - [show l2tp dial-out virtual-router on page 148](#)

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 15 on page 95](#) lists the **show l2tp dial-out session** command output fields.

Table 15: 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 24](#)
 - [show l2tp dial-out session on page 146](#)

CHAPTER 12

Verifying the Cause Codes for Termination of L2TP Sessions

- [L2TP Disconnect Cause Codes on page 97](#)
- [L2TP Terminate Reasons on page 101](#)
- [PPP Terminate Reasons on page 118](#)
- [Configuring Custom Mappings for PPP Terminate Reasons on page 125](#)

L2TP Disconnect Cause Codes

[Table 16 on page 98](#) describes the Point-to-Point Protocol (PPP) disconnect cause codes that are displayed by the **show l2tp received-disconnect-cause-summary** command, sorted by code number. For additional information, see RFC 3145.

Table 16: PPP Disconnect Cause Codes

Code	Name	Description
0	no info	<p>Code 0 includes disconnect causes that are not specifically identified by other codes. This code is generated in the following circumstances:</p> <ul style="list-style-type: none"> Internal resource constraints (for example, excessive load or reduced resource availability) have prevented the generation of a more specific disconnect code. RFC 3145 does not define a disconnect code that corresponds to the cause of the disconnection. <p>The following list shows current disconnection causes on an E Series LNS that do not have a specific disconnect cause codes:</p> <ul style="list-style-type: none"> The peer initiated termination of LCP after the completion of LCP negotiations, but prior to proceeding to authentication of NCP negotiation. No conditions occurred that enabled the LNS to infer a more informative disconnect code. The peer initiated renegotiation of LCP. Invalid local MRU (for example, MRU negotiation has been disabled, but the lower MRU is less than the default MRU of 1500). Unexpected local MLPPP MRRU for existing bundle (RFC 3145 code 10 covers peer MRRU mismatches, but not local mismatches). Authentication failures not covered by any of the authentication-related codes (codes 13-16), such as: <ul style="list-style-type: none"> Authentication denial of the local LCP by the peer Local authentication failure due to no resources Local authentication failure due to no authenticator
1	admin disconnect	<p>The disconnection was a result of direct administrative action, including:</p> <ul style="list-style-type: none"> The administrator shut down the network or link interface. The administrator logged out the subscriber.
2	renegotiation disabled	Code 2 is not used; the E Series LNS is always capable of renegotiating LCP if proxy data is not available.
3	normal disconnect	<p>Indicates that one of the following events occurred:</p> <ul style="list-style-type: none"> user-initiated logout (direction 1) session timeout (direction 2) inactivity timeout (direction 2) address lease expired (direction 2) <p>The E Series LNS determines by inference that a normal disconnect has occurred for direction 1. The LNS does this when the peer initiates LCP termination after proceeding beyond the successful negotiation of LCP (that is, after starting authentication signaling or NCP negotiation).</p> <p>NOTE: The Error-code field is included by default in the Result Error Code attribute value pair (AVP) in L2TP Call-Disconnect-Notify (CDN) messages, even in normal disconnect cases when the peer initiates LCP termination after proceeding beyond LCP negotiation.</p>

Table 16: PPP Disconnect Cause Codes (*continued*)

Code	Name	Description
4	compulsory encryption refused	<p>Code 4 with direction 2 is generated if the following conditions are met:</p> <ul style="list-style-type: none"> The peer initiates LCP termination without having proceeded beyond the completion of LCP negotiation, and Prior to receiving the terminate request from the peer, the local LCP has sent a Protocol Reject in response to any packet for Encryption Control Protocol (ECP) protocols (protocol codes 0x8053, 0x8055) from the peer. <p>Code 4 with direction 1 is never generated, because the E Series LNS never requests ECP.</p>
5	lcp failed to converge	An LCP configuration error prevented LCP from converging; the two peers attempted to negotiate but did not agree on acceptable LCP parameters.
6	lcp peer silent	LCP negotiation timed out; the LNS did not receive any LCP packets from the LAC.
7	lcp magic number error	A magic number error was detected; this indicates a possible looped back link.
8	lcp keepalive error	The keepalive drop count was exceeded.
9	lcp mlppp endpoint discriminator mismatch	Code 9 is not used. Dynamic MLPPP bundling, which is the only kind of MLPPP bundling supported for MLPPP/L2TP, uses the endpoint discriminator as part of the key for bundle selection. Therefore, there will never be an unexpected endpoint discriminator for an existing MLPPP bundle.
10	lcp mlppp mrru not valid	The link attempted to join an existing MLPPP bundle whose peer maximum received reconstructed unit (MRRU) did not match the peer MRRU negotiated by the link.
11	lcp mlppp peer ssn invalid	Code 11 is not used; the short sequence number (SSN) option is not supported.
12	lcp callback refused	<p>Code 12 with direction 2 is generated when the following conditions are met:</p> <ul style="list-style-type: none"> The peer initiates LCP termination without having proceeded to NCP negotiation, and Prior to the termination, the local LCP has responded with a negative acknowledgement (NAK) to a callback option (LCP option 13) from the peer. <p>The E Series LNS never generates code 12 with direction 1 because the LNS never requests callback.</p>

Table 16: PPP Disconnect Cause Codes (*continued*)

Code	Name	Description
13	authenticate timed out	Authentication failed because the authentication protocol timed out; either the CHAP Authenticate Response or the PAP Authenticate Request was not received.
14	authenticate mlppp name mismatch	Code 14 is not used. Dynamic MLPPP bundling, which is the only kind of MLPPP bundling supported for MLPPP/L2TP, uses the authenticated name as part of the key for bundle selection. Therefore, there will never be an unexpected authenticated name for an existing MLPPP bundle.
15	authenticate protocol refused	<p>No acceptable authentication protocol was negotiated by LCP.</p> <ul style="list-style-type: none"> Code 15 with direction 1 is generated if the peer rejected all of the authentication protocols requested by the local LCP. Code 15 with direction 2 is generated if the following conditions are met: <ul style="list-style-type: none"> The peer initiates LCP termination without having proceeded beyond completion of NCP negotiation, and During LCP negotiation, the local LCP responded with a NAK to the final authentication protocol requested by the peer.
16	authenticate failure	<ul style="list-style-type: none"> Code 16 with direction 1 is generated if the local authentication of the peer fails (that is, the authenticator sent a PAP NAK or CHAP Failure packet) Code 16 with direction 2 is generated if the peer authentication of the local LCP fails (that is, the authenticator received a PAP NAK or CHAP Failure packet). <p>Note that there are a variety of causes for authentication failures, including bad credentials (bad name, password or secret) and resource problems.</p>
17	ncp no negotiation completed	<p>Code 17 is generated only if an NCP configuration error has prevented NCP negotiation from converging. This occurs when the two peers do not agree on acceptable NCP parameters within the time allowed for upper-layer negotiation.</p> <p>Code 19 takes precedence over code 17 in situations related to address convergence failure.</p>
18	ncp no ncps available	No NCPs were successfully enabled within the time allowed for upper-layer negotiation.

Table 16: PPP Disconnect Cause Codes (*continued*)

Code	Name	Description
19	ncp addresses failed to converge	<p>An NCP configuration error has prevented NCP negotiation from converging on acceptable addresses. This occurs if the two peers never agree on acceptable NCP addresses within the time allowed for upper-layer negotiation.</p> <ul style="list-style-type: none"> Code 19 with direction 1 is generated if the peer denies address parameters requested by the local NCP. Code 19 with direction 2 is generated if the local NCP denies address parameters requested by the peer. <p>The IPv6 interface identifier is considered an address for the purposes of code 19.</p> <p>Code 19 takes precedence over code 17 in situations related to address convergence failure.</p>
20	ncp negotiation inhibited	<ul style="list-style-type: none"> Code 20 with direction 2 indicates that an upper layer negotiation was inhibited for any enabled NCP because the required network-layer parameters were not available as a result of the authentication stage. Code 20 with direction 1 is never generated; the NCPs are never enabled if there is no non-null local address.

Related Documentation

- [L2TP Terminate Reasons on page 101](#)
- [PPP Terminate Reasons on page 118](#)
- [disconnect-cause](#)
- [l2tp disconnect-cause](#)
- [show l2tp received-disconnect-cause-summary on page 144](#)

L2TP Terminate Reasons

Table 17 on page 101 lists the default L2TP terminate mappings. The table indicates the supported L2TP terminate reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 17: Default L2TP Mappings

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session access interface down	8	port error
session admin close	6	admin reset

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session admin drain	6	admin reset
session call down	10	nas request
session call failed	15	service unavailable
session create failed limit reached	9	nas error
session create failed no resources	9	nas error
session create failed single shot tunnel already fired	9	nas error
session create failed too busy	9	nas error
session failover protocol resync disconnect	6	admin reset
session hardware unavailable	8	port error
session no resources server port	9	nas error
session not ready	9	nas error
session rx cdn	10	nas request
session rx cdn avp bad hidden	10	nas request
session rx cdn avp bad value assigned session id	10	nas request
session rx cdn avp duplicate value assigned session id	10	nas request
session rx cdn avp malformed bad length	10	nas request
session rx cdn avp malformed truncated	10	nas request
session rx cdn avp missing mandatory assigned session id	10	nas request
session rx cdn avp missing mandatory result code	10	nas request
session rx cdn avp missing random vector	10	nas request
session rx cdn avp missing secret	10	nas request
session rx cdn avp unknown	10	nas request
session rx cdn no resources	10	nas request

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx iccn avp bad hidden	10	nas request
session rx iccn avp bad value framing type	10	nas request
session rx iccn avp bad value proxy authen type	10	nas request
session rx iccn avp bad value unsupported proxy authen type	10	nas request
session rx iccn avp malformed bad length	10	nas request
session rx iccn avp malformed truncated	10	nas request
session rx iccn avp missing mandatory connect speed	10	nas request
session rx iccn avp missing mandatory framing type	10	nas request
session rx iccn avp missing mandatory proxy authen challenge	10	nas request
session rx iccn avp missing mandatory proxy authen id	10	nas request
session rx iccn avp missing mandatory proxy authen name	10	nas request
session rx iccn avp missing mandatory proxy authen response	10	nas request
session rx iccn avp missing random vector	10	nas request
session rx iccn avp missing secret	10	nas request
session rx iccn avp unknown	10	nas request
session rx iccn no resources	10	nas request
session rx iccn unexpected	10	nas request
session rx icrp avp bad hidden	10	nas request
session rx icrp avp bad value assigned session id	10	nas request
session rx icrp avp duplicate value assigned session id	10	nas request
session rx icrp avp malformed bad length	10	nas request
session rx icrp avp malformed truncated	10	nas request
session rx icrp avp missing mandatory assigned session id	10	nas request

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx icrp avp missing random vector	10	nas request
session rx icrp avp missing secret	10	nas request
session rx icrp avp unknown	10	nas request
session rx icrp no resources	10	nas request
session rx icrp unexpected	10	nas request
session rx icrq admin close	6	admin reset
session rx icrq authenticate failed host	10	nas request
session rx icrq avp bad hidden	10	nas request
session rx icrq avp bad value assigned session id	10	nas request
session rx icrq avp bad value bearer type	10	nas request
session rx icrq avp bad value cisco nas port	10	nas request
session rx icrq avp duplicate value assigned session id	10	nas request
session rx icrq avp malformed bad length	10	nas request
session rx icrq avp malformed truncated	10	nas request
session rx icrq avp missing mandatory assigned session id	10	nas request
session rx icrq avp missing mandatory call serial number	10	nas request
session rx icrq avp missing random vector	10	nas request
session rx icrq avp missing secret	10	nas request
session rx icrq avp unknown	10	nas request
session rx icrq no resources	10	nas request
session rx icrq unexpected	10	nas request
session rx occn avp bad hidden	10	nas request
session rx occn avp bad value framing type	10	nas request

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx occn avp malformed bad length	10	nas request
session rx occn avp malformed truncated	10	nas request
session rx occn avp missing mandatory connect speed	10	nas request
session rx occn avp missing mandatory framing type	10	nas request
session rx occn avp missing random vector	10	nas request
session rx occn avp missing secret	10	nas request
session rx occn avp unknown	10	nas request
session rx occn no resources	10	nas request
session rx occn unexpected	10	nas request
session rx ocrp avp bad hidden	10	nas request
session rx ocrp avp bad value assigned session id	10	nas request
session rx ocrp avp duplicate value assigned session id	10	nas request
session rx ocrp avp malformed bad length	10	nas request
session rx ocrp avp malformed truncated	10	nas request
session rx ocrp avp missing mandatory assigned session id	10	nas request
session rx ocrp avp missing random vector	10	nas request
session rx ocrp avp missing secret	10	nas request
session rx ocrp avp unknown	10	nas request
session rx ocrp no resources	10	nas request
session rx ocrp unexpected	10	nas request
session rx ocrq admin close	10	admin reset
session rx ocrq authenticate failed host	10	nas request
session rx ocrq avp bad hidden	10	nas request

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx ocrq avp bad value assigned session id	10	nas request
session rx ocrq avp bad value bearer type	10	nas request
session rx ocrq avp bad value framing type	10	nas request
session rx ocrq avp duplicate value assigned session id	10	nas request
session rx ocrq avp malformed bad length	10	nas request
session rx ocrq avp malformed truncated	10	nas request
session rx ocrq avp missing mandatory assigned session id	10	nas request
session rx ocrq avp missing mandatory bearer type	10	nas request
session rx ocrq avp missing mandatory call serial number	10	nas request
session rx ocrq avp missing mandatory called number	10	nas request
session rx ocrq avp missing mandatory framing type	10	nas request
session rx ocrq avp missing mandatory maximum bps	10	nas request
session rx ocrq avp missing mandatory minimum bps	10	nas request
session rx ocrq avp missing random vector	10	nas request
session rx ocrq avp missing secret	10	nas request
session rx ocrq avp unknown	10	nas request
session rx ocrq no resources	10	nas request
session rx ocrq unexpected	10	nas request
session rx ocrq unsupported	9	nas error
session rx sli avp bad hidden	10	nas request
session rx sli avp bad value accm	10	nas request
session rx sli avp malformed bad length	10	nas request
session rx sli avp malformed truncated	10	nas request

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx sli avp missing mandatory accm	10	nas request
session rx sli avp missing random vector	10	nas request
session rx sli avp missing secret	10	nas request
session rx sli avp unknown	10	nas request
session rx sli no resources	10	nas request
session rx unexpected packet lac incoming	10	nas request
session rx unexpected packet lac outgoing	10	nas request
session rx unexpected packet lns incoming	10	nas request
session rx unexpected packet lns outgoing	10	nas request
session rx unknown session id	10	nas request
session rx wen avp bad hidden	10	nas request
session rx wen avp malformed bad length	10	nas request
session rx wen avp malformed truncated	10	nas request
session rx wen avp missing mandatory call errors	10	nas request
session rx wen avp missing random vector	10	nas request
session rx wen avp missing secret	10	nas request
session rx wen avp unknown	10	nas request
session rx wen no resources	10	nas request
session timeout connection	10	nas request
session timeout inactivity	4	idle timeout
session timeout session	5	session timeout
session timeout upper create	9	nas error
session transmit speed unavailable	9	nas error

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session tunnel down	15	service unavailable
session tunnel failed	15	service unavailable
session tunnel switch profile deleted	6	admin reset
session tunneled interface down	8	port error
session unknown cause	9	nas error
session upper create failed	9	nas error
session upper removed	15	service unavailable
session warmstart not operational	15	service unavailable
session warmstart recovery error	15	service unavailable
session warmstart upper not restacked	10	nas request
tunnel admin close	6	admin reset
tunnel admin drain	6	admin reset
tunnel control channel failed	15	service unavailable
tunnel created no sessions	1	user request
tunnel destination address changed	6	admin reset
tunnel destination down	10	nas request
tunnel failover protocol no resources for recovery tunnel	15	service unavailable
tunnel failover protocol no resources for session resync	15	service unavailable
tunnel failover protocol not supported	15	service unavailable
tunnel failover protocol not supported by peer	15	service unavailable
tunnel failover protocol recovery control channel failed	15	service unavailable
tunnel failover protocol recovery tunnel failed	15	service unavailable
tunnel failover protocol recovery tunnel finished	1	user request

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel failover protocol recovery tunnel primary down	1	user request
tunnel failover protocol session resync failed	15	service unavailable
tunnel host profile changed	6	admin reset
tunnel host profile deleted	6	admin reset
tunnel rx scccn authenticate failed challenge	17	user error
tunnel rx scccn avp bad hidden	15	service unavailable
tunnel rx scccn avp bad value challenge response	15	service unavailable
tunnel rx scccn avp malformed bad length	15	service unavailable
tunnel rx scccn avp malformed truncated	15	service unavailable
tunnel rx scccn avp missing challenge response	17	user error
tunnel rx scccn avp missing random vector	15	service unavailable
tunnel rx scccn avp missing secret	15	service unavailable
tunnel rx scccn avp unexpected challenge response	15	service unavailable
tunnel rx scccn avp unknown	15	service unavailable
tunnel rx scccn no resources	15	service unavailable
tunnel rx scccn session id not null	15	service unavailable
tunnel rx scccn unexpected	15	service unavailable
tunnel rx sccrp authenticate failed challenge	17	user error
tunnel rx sccrp authenticate failed host	17	user error
tunnel rx sccrp avp bad hidden	15	service unavailable
tunnel rx sccrp avp bad value assigned tunnel id	15	service unavailable
tunnel rx sccrp avp bad value bearer capabilities	15	service unavailable
tunnel rx sccrp avp bad value challenge	15	service unavailable

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx sccrp avp bad value challenge response	15	service unavailable
tunnel rx sccrp avp bad value failover capability	15	service unavailable
tunnel rx sccrp avp bad value framing capabilities	15	service unavailable
tunnel rx sccrp avp bad value protocol version	15	service unavailable
tunnel rx sccrp avp bad value receive window size	15	service unavailable
tunnel rx sccrp avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx sccrp avp malformed bad length	15	service unavailable
tunnel rx sccrp avp malformed truncated	15	service unavailable
tunnel rx sccrp avp missing challenge response	17	user error
tunnel rx sccrp avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx sccrp avp missing mandatory framing capabilities	15	service unavailable
tunnel rx sccrp avp missing mandatory host name	15	service unavailable
tunnel rx sccrp avp missing mandatory protocol version	15	service unavailable
tunnel rx sccrp avp missing random vector	15	service unavailable
tunnel rx sccrp avp missing secret	15	service unavailable
tunnel rx sccrp avp unexpected challenge response	15	service unavailable
tunnel rx sccrp avp unexpected challenge without secret	15	service unavailable
tunnel rx sccrp avp unknown	15	service unavailable
tunnel rx sccrp no resources	15	service unavailable
tunnel rx sccrp session id not null	15	service unavailable
tunnel rx sccrp unexpected	15	service unavailable
tunnel rx sccrp admin close	6	admin reset
tunnel rx sccrp authenticate failed host	17	user error

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx sccrq avp bad hidden	15	service unavailable
tunnel rx sccrq avp bad value assigned tunnel id	15	service unavailable
tunnel rx sccrq avp bad value bearer capabilities	15	service unavailable
tunnel rx sccrq avp bad value challenge	15	service unavailable
tunnel rx sccrq avp bad value failover capability	15	service unavailable
tunnel rx sccrq avp bad value framing capabilities	15	service unavailable
tunnel rx sccrq avp bad value protocol version	15	service unavailable
tunnel rx sccrq avp bad value receive window size	15	service unavailable
tunnel rx sccrq avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx sccrq avp malformed bad length	15	service unavailable
tunnel rx sccrq avp malformed truncated	15	service unavailable
tunnel rx sccrq avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx sccrq avp missing mandatory framing capabilities	15	service unavailable
tunnel rx sccrq avp missing mandatory host name	15	service unavailable
tunnel rx sccrq avp missing mandatory protocol version	15	service unavailable
tunnel rx sccrq avp missing random vector	15	service unavailable
tunnel rx sccrq avp missing secret	15	service unavailable
tunnel rx sccrq avp unexpected challenge without secret	15	service unavailable
tunnel rx sccrq avp unknown	15	service unavailable
tunnel rx sccrq bad address	15	service unavailable
tunnel rx sccrq no resources	15	service unavailable
tunnel rx sccrq no resources max tunnels	15	service unavailable
tunnel rx sccrq session id not null	15	service unavailable

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx sccrq unexpected	15	service unavailable
tunnel rx stopccn	1	user request
tunnel rx stopccn avp bad hidden	15	service unavailable
tunnel rx stopccn avp bad value assigned tunnel id	15	service unavailable
tunnel rx stopccn avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx stopccn avp malformed bad length	15	service unavailable
tunnel rx stopccn avp malformed truncated	15	service unavailable
tunnel rx stopccn avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx stopccn avp missing mandatory result code	15	service unavailable
tunnel rx stopccn avp missing random vector	15	service unavailable
tunnel rx stopccn avp missing secret	15	service unavailable
tunnel rx stopccn avp unknown	15	service unavailable
tunnel rx stopccn no resources	15	service unavailable
tunnel rx stopccn session id not null	15	service unavailable
tunnel rx frs avp malformed truncated	15	service unavailable
tunnel rx frs avp missing mandatory failover session state	15	service unavailable
tunnel rx frs avp missing random vector	15	service unavailable
tunnel rx frs avp missing secret	15	service unavailable
tunnel rx frs avp unknown	15	service unavailable
tunnel rx frs no resources	15	service unavailable
tunnel rx frs session id not null	15	service unavailable
tunnel rx fsq avp bad hidden	15	service unavailable
tunnel rx fsq avp malformed bad length	15	service unavailable

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx fsq avp malformed truncated	15	service unavailable
tunnel rx fsq avp missing mandatory failover session state	15	service unavailable
tunnel rx fsq avp missing random vector	15	service unavailable
tunnel rx fsq avp missing secret	15	service unavailable
tunnel rx fsq avp unknown	15	service unavailable
tunnel rx fsq no resources	15	service unavailable
tunnel rx fsq session id not null	15	service unavailable
tunnel rx fsr avp bad hidden	15	service unavailable
tunnel rx fsr avp malformed bad length	15	service unavailable
tunnel rx unexpected packet	15	service unavailable
tunnel rx unexpected packet for session	15	service unavailable
tunnel rx unknown packet message type indecipherable	15	service unavailable
tunnel rx unknown packet message type unrecognized	15	service unavailable
tunnel rx recovery sccn authenticate failed challenge	17	user error
tunnel rx recovery sccn avp bad hidden	15	service unavailable
tunnel rx recovery sccn avp bad value challenge response	15	service unavailable
tunnel rx recovery sccn avp malformed bad length	15	service unavailable
tunnel rx recovery sccn avp malformed truncated	15	service unavailable
tunnel rx recovery sccn avp missing challenge response	17	user error
tunnel rx recovery sccn avp missing random vector	15	service unavailable
tunnel rx recovery sccn avp missing secret	15	service unavailable
tunnel rx recovery sccn avp unexpected challenge response	15	service unavailable
tunnel rx recovery sccn avp unknown	15	service unavailable

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx recovery sccn no resources	15	service unavailable
tunnel rx recovery sccn session id not null	15	service unavailable
tunnel rx recovery sccrp authenticate failed challenge	17	user error
tunnel rx recovery sccrp avp bad hidden	15	service unavailable
tunnel rx recovery sccrp avp bad value assigned tunnel id	15	service unavailable
tunnel rx recovery sccrp avp bad value bearer capabilities	15	service unavailable
tunnel rx recovery sccrp avp bad value challenge	15	service unavailable
tunnel rx recovery sccrp avp bad value challenge response	15	service unavailable
tunnel rx recovery sccrp avp bad value framing capabilities	15	service unavailable
tunnel rx recovery sccrp avp bad value protocol version	15	service unavailable
tunnel rx recovery sccrp avp bad value receive window size	15	service unavailable
tunnel rx recovery sccrp avp bad value suggested control sequence	15	service unavailable
tunnel rx recovery sccrp avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx recovery sccrp avp malformed bad length	15	service unavailable
tunnel rx recovery sccrp avp malformed truncated	15	service unavailable
tunnel rx recovery sccrp avp mismatched host name	15	service unavailable
tunnel rx recovery sccrp avp mismatched vendor name	15	service unavailable
tunnel rx recovery sccrp avp missing challenge response	17	user error
tunnel rx recovery sccrp avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx recovery sccrp avp missing mandatory framing capabilities	15	service unavailable
tunnel rx recovery sccrp avp missing mandatory host name	15	service unavailable

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx recovery sccrp avp missing mandatory protocol version	15	service unavailable
tunnel rx recovery sccrp avp missing random vector	15	service unavailable
tunnel rx recovery sccrp avp missing secret	15	service unavailable
tunnel rx recovery sccrp avp unexpected challenge response	15	service unavailable
tunnel rx recovery sccrp avp unexpected challenge without secret	15	service unavailable
tunnel rx recovery sccrp avp unknown	15	service unavailable
tunnel rx recovery sccrp no resources	15	service unavailable
tunnel rx recovery sccrp session id not null	15	service unavailable
tunnel rx recovery sccrq admin close	6	admin reset
tunnel rx recovery sccrq avp bad hidden	15	service unavailable
tunnel rx recovery sccrq avp bad value assigned tunnel id	15	service unavailable
tunnel rx recovery sccrq avp bad value bearer capabilities	15	service unavailable
tunnel rx recovery sccrq avp bad value challenge	15	service unavailable
tunnel rx recovery sccrq avp bad value framing capabilities	15	service unavailable
tunnel rx recovery sccrq avp bad value protocol version	15	service unavailable
tunnel rx recovery sccrq avp bad value receive window size	15	service unavailable
tunnel rx recovery sccrq avp bad value tunnel recovery	15	service unavailable
tunnel rx recovery sccrq avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx recovery sccrq avp duplicate value tie breaker	15	service unavailable
tunnel rx recovery sccrq avp malformed bad length	15	service unavailable
tunnel rx recovery sccrq avp malformed truncated	15	service unavailable

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx recovery sccrq avp mismatched host name	15	service unavailable
tunnel rx recovery sccrq avp mismatched vendor name	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory framing capabilities	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory host name	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory protocol version	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory tunnel recovery	15	service unavailable
tunnel rx recovery sccrq avp missing random vector	15	service unavailable
tunnel rx recovery sccrq avp missing secret	15	service unavailable
tunnel rx recovery sccrq avp missing tie breaker	15	service unavailable
tunnel rx recovery sccrq avp unexpected challenge without secret	15	service unavailable
tunnel rx recovery sccrq avp unknown	15	service unavailable
tunnel rx recovery sccrq no resources	15	service unavailable
tunnel rx recovery sccrq session id not null	15	service unavailable
tunnel rx recovery sccrq tunnel id not null	15	service unavailable
tunnel rx recovery stopccn avp bad hidden	15	service unavailable
tunnel rx recovery stopccn avp bad value assigned tunnel id	15	service unavailable
tunnel rx recovery stopccn avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx recovery stopccn avp malformed bad length	15	service unavailable
tunnel rx recovery stopccn avp malformed truncated	15	service unavailable

Table 17: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx recovery stopccn avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx recovery stopccn avp missing mandatory result code	15	service unavailable
tunnel rx recovery stopccn avp missing random vector	15	service unavailable
tunnel rx recovery stopccn avp missing secret	15	service unavailable
tunnel rx recovery stopccn avp unknown	15	service unavailable
tunnel rx recovery stopccn no resources	15	service unavailable
tunnel rx recovery stopccn session id not null	15	service unavailable
tunnel rx recovery unexpected packet	15	service unavailable
tunnel rx recovery unknown packet message type indecipherable	15	service unavailable
tunnel rx recovery unknown packet message type unrecognized	15	service unavailable
tunnel rx session packet null sid invalid	15	service unavailable
tunnel rx session packet null sid without assigned session id	15	service unavailable
tunnel timeout connection	15	service unavailable
tunnel timeout connection recovery tunnel	15	service unavailable
tunnel timeout idle	1	user request
tunnel unknown cause	9	nas error
tunnel warmstart not operational	15	service unavailable
tunnel warmstart recovery error	15	service unavailable

Related Documentation

- [Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 17](#)
- [Configuring Custom Mappings for PPP Terminate Reasons on page 125](#)
- [Monitoring Application Terminate Reason Mappings](#)

PPP Terminate Reasons

Table 18 on page 118 lists the default PPP terminate mappings. The table indicates the supported PPP terminate reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 18: Default PPP Mappings

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
authenticate authenticator timeout	17	user error
authenticate challenge timeout	10	nas request
authenticate chap no resources	10	nas request
authenticate chap peer authenticator timeout	17	user error
authenticate deny by peer	17	user error
authenticate inactivity timeout	4	idle timeout
authenticate max requests	10	nas request
authenticate no authenticator	10	nas request
authenticate pap peer authenticator timeout	17	user error
authenticate pap request timeout	10	nas request
authenticate session timeout	5	session timeout
authenticate too many requests	10	nas request
authenticate tunnel fail immediate	10	nas request
authenticate tunnel unsupported tunnel type	10	nas request
bundle fail create	10	nas request
bundle fail engine add	10	nas request
bundle fail fragment size mismatch	10	nas request
bundle fail fragmentation location	10	nas request
bundle fail fragmentation mismatch	10	nas request

Table 18: Default PPP Mappings (*continued*)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
bundle fail join	10	nas request
bundle fail link selection mismatch	10	nas request
bundle fail local mped not set yet	10	nas request
bundle fail local mrru mismatch	10	nas request
bundle fail local mru mismatch	10	nas request
bundle fail peer mrru mismatch	10	nas request
bundle fail reassembly location	10	nas request
bundle fail reassembly mismatch	10	nas request
bundle fail record network	10	nas request
bundle fail server location mismatch	10	nas request
bundle fail static link	10	nas request
failover during authentication	6	admin reset
interface admin disable	6	admin reset
interface down	2	lost carrier
interface no hardware	8	port error
ip admin disable	10	nas request
ip inhibited by authentication	10	nas request
ip link down	10	nas request
ip max configure exceeded	10	nas request
ip no local ip address	10	nas request
ip no local ip address mask	10	nas request
ip no local primary dns address	10	nas request
ip no local primary nbns address	10	nas request

Table 18: Default PPP Mappings (*continued*)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
ip no local secondary dns address	10	nas request
ip no local secondary nbns address	10	nas request
ip no peer ip address	10	nas request
ip no peer ip address mask	10	nas request
ip no peer primary dns address	10	nas request
ip no peer primary nbns address	10	nas request
ip no peer secondary dns address	10	nas request
ip no peer secondary nbns address	10	nas request
ip no service	10	nas request
ip peer renegotiate rx conf ack	10	nas request
ip peer renegotiate rx conf nak	10	nas request
ip peer renegotiate rx conf rej	10	nas request
ip peer renegotiate rx conf req	10	nas request
ip peer terminate term ack	10	nas request
ip peer terminate code rej	10	nas request
ip peer terminate term req	10	nas request
ip service disable	10	nas request
ip stale stacking	10	nas request
ipv6 admin disable	10	nas request
ipv6 inhibited by authentication	10	nas request
ipv6 link down	10	nas request
ipv6 local and peer interface ids identical	10	nas request
ipv6 max configure exceeded	10	nas request

Table 18: Default PPP Mappings (*continued*)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
ipv6 no local ipv6 interface id	10	nas request
ipv6 no peer ipv6 interface id	10	nas request
ipv6 no service	10	nas request
ipv6 peer renegotiate rx conf ack	10	nas request
ipv6 peer renegotiate rx conf nak	10	nas request
ipv6 peer renegotiate rx conf rej	10	nas request
ipv6 peer renegotiate rx conf req	10	nas request
ipv6 peer terminate code rej	10	nas request
ipv6 peer terminate term ack	10	nas request
ipv6 peer terminate term req	10	nas request
ipv6 service disable	10	nas request
ipv6 stale stacking	10	nas request
lcp authenticate terminate hold	10	nas request
lcp configured mrru too small	10	nas request
lcp configured mru invalid	10	nas request
lcp configured mru too small	10	nas request
lcp dynamic interface hold	10	nas request
lcp keepalive failure	10	nas request
lcp loopback rx conf req	10	nas request
lcp loopback rx echo reply	10	nas request
lcp loopback rx echo req	10	nas request
lcp max configure exceeded	10	nas request
lcp mru changed	10	nas request

Table 18: Default PPP Mappings (*continued*)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
lcp negotiation timeout	10	nas request
lcp no localaccm	10	nas request
lcp no localacfc	10	nas request
lcp no local authentication	10	nas request
lcp no local endpoint discriminator	10	nas request
lcp no local magic number	10	nas request
lcp no local mrru	10	nas request
lcp no local mru	10	nas request
lcp no localpfc	10	nas request
lcp no peer accm	10	nas request
lcp no peer authentication	10	nas request
lcp no peer endpoint discriminator	10	nas request
lcp no peer magicnumber	10	nas request
lcp no peer mrru	10	nas request
lcp no peer mru	10	nas request
lcp no peer pfc	10	nas request
lcp peer terminate code rej	1	user request
lcp peer terminate term ack	1	user request
lcp peer terminate term req	1	user request
lcp peer terminate protocol reject	1	user request
lcp peer renegotiate rx conf ack	1	user request
lcp peer renegotiate rx conf nak	1	user request
lcp peer renegotiate rx conf rej	1	user request

Table 18: Default PPP Mappings (*continued*)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
lcp peer renegotiate rx conf req	1	user request
lcp tunnel disconnected	10	nas request
lcp tunnel failed	10	nas request
link interface no hardware	8	port error
lower interface attach failed	2	lost carrier
lower interface teardown	2	lost carrier
mpls admin disable	10	nas request
mpls link down	10	nas request
mpls max configure exceeded	10	nas request
mpls no service	10	nas request
mpls peer renegotiate rx conf ack	10	nas request
mpls peer renegotiate rx conf nak	10	nas request
mpls peer renegotiate rx conf rej	10	nas request
mpls peer renegotiate rx conf req	10	nas request
mpls peer terminate code rej	10	nas request
mpls peer terminate term ack	10	nas request
mpls peer terminate term req	10	nas request
mpls service disable	10	nas request
mpls stale stacking	10	nas request
network interface admin disable	6	admin reset
no bundle	10	nas request
no interface	8	port error
no link interface	8	port error

Table 18: Default PPP Mappings (*continued*)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
no ncps available	10	nas request
no network interface	10	nas request
no upper interface	9	nas error
osi admin disable	10	nas request
osi link down	10	nas request
osi max configure exceeded	10	nas request
osi no local align npdu	10	nas request
osi no peer align npdu	10	nas request
osi no service	10	nas request
osi peer renegotiate rx conf ack	10	nas request
osi peer renegotiate rx conf nak	10	nas request
osi peer renegotiate rx conf rej	10	nas request
osi peer renegotiate rx conf req	10	nas request
osi peer terminate code rej	10	nas request
osi peer terminate term ack	10	nas request
osi peer terminate term req	10	nas request
osi service disable	10	nas request
osi stale stacking	10	nas request

**Related
Documentation**

- [Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 17](#)
- [Configuring Custom Mappings for PPP Terminate Reasons on page 125](#)
- [L2TP Terminate Reasons on page 101](#)
- [Monitoring Application Terminate Reason Mappings](#)

ppp	authenticate-challenge-timeout	authenticate challenge timeout	4
ppp	authenticate-chap-no-resources	authenticate chap no resources	10
ppp	authenticate-chap-peer-authenticator-timeout	authenticate chap peer authenticator timeout	17
ppp	authenticate-deny-by-peer	authenticate deny by peer	17
ppp	authenticate-inactivity-timeout	authenticate inactivity timeout	4
ppp	authenticate-max-requests	authenticate max requests	10
--More--			

- Related Documentation**
- radius include
 - show terminate-code
 - terminate-code

Table 19: show l2tp destination Output Fields

Field Name	Field Description
Configuration	Configured status of the destination
Administrative state	Administrative status of the destination: <ul style="list-style-type: none"> • 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 141](#)

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 129](#) 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

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

Field Name	Field Description
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
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

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

Field Name	Field Description
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 140](#)

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 21 on page 131](#) lists the **show l2tp destination lockout** command output fields.

Table 21: 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 142](#)

Table 22: 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 144](#)

Monitoring L2TP Sessions

- [Monitoring Detailed Configuration Information about Specified Sessions on page 135](#)
- [Monitoring Configured and Operational Summary Status on page 136](#)

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 23 on page 136](#) lists the **show l2tp session** command output fields.

Table 23: show l2tp session Output Fields

Field Name	Field Description
Configuration	Configured status of the session
Administrative state	Administrative status of the destination: <ul style="list-style-type: none"> 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 149](#)

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 24 on page 137](#) lists the **show l2tp session summary** command output fields.

Table 24: show l2tp session summary Output Fields

Field Name	Field Description
Administrative status:	Administrative status of the session: <ul style="list-style-type: none">• enabled—No restrictions on the creation of sessions• disabled—Router disabled these sessions
Operational status:	Operational status of the session: <ul style="list-style-type: none">• 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 149](#) summary

CHAPTER 16

Monitoring Commands

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 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 [*triggerIp*Address | 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**
- *triggerIp*Address—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

PART 4

Index

- [Index on page 153](#)

