



---

Junos<sup>®</sup> OS

# L2TP Feature Guide for Subscriber Management

Release

14.1



---

Published: 2014-05-19

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

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.

*Junos<sup>®</sup> OS L2TP Feature Guide for Subscriber Management*

14.1

Copyright © 2014, Juniper Networks, Inc.

All rights reserved.

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 . . . . .	xiii
	Documentation and Release Notes . . . . .	xiii
	Supported Platforms . . . . .	xiii
	Using the Examples in This Manual . . . . .	xiii
	Merging a Full Example . . . . .	xiv
	Merging a Snippet . . . . .	xiv
	Documentation Conventions . . . . .	xv
	Documentation Feedback . . . . .	xvii
	Requesting Technical Support . . . . .	xvii
	Self-Help Online Tools and Resources . . . . .	xvii
	Opening a Case with JTAC . . . . .	xviii
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>L2TP in Subscriber Access Networks . . . . .</b>	<b>3</b>
	L2TP for Subscriber Access Overview . . . . .	3
	L2TP Terminology . . . . .	5
	L2TP Implementation . . . . .	6
	Sequence of Events on the LAC . . . . .	7
	Sequence of Events on the LNS . . . . .	8
	Retransmission of L2TP Control Messages . . . . .	8
	L2TP and Graceful Routing Engine Switchover . . . . .	10
	L2TP Tunnel Switching Overview . . . . .	11
	Application of Tunnel Switch Profiles . . . . .	13
	Termination of Tunnel-Switched Sessions on the LTS . . . . .	13
	Tunnel Switching Actions for L2TP AVPs at the Switching Boundary . . . . .	15
	LAC Interoperation with Third-Party LNS Devices . . . . .	17
<b>Chapter 2</b>	<b>L2TP LAC . . . . .</b>	<b>19</b>
	Subscriber Secure Policy and L2TP LAC Subscribers . . . . .	19
	LAC Tunnel Selection Overview . . . . .	19
	Tunnel Selection Failover Between Preference Levels . . . . .	20
	Tunnel Selection Failover Within a Preference Level . . . . .	22
	Session Failover and Tunnel Selection Behavior . . . . .	23
	Tunnel Selection and Maximum Sessions per Tunnel . . . . .	23
	Tunnel Selection with Weighted Load Balancing . . . . .	24
	L2TP Failover and Peer Resynchronization . . . . .	24
	IP Packet Fragment Reassembly for L2TP Overview . . . . .	26
	Transmission of Tx Connect-Speed and Rx Connect-Speed AVPs from LAC to LNS . . . . .	26
	Subscriber Access Line Information Forwarding by the LAC Overview . . . . .	28

<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 3</b>	<b>Configuration Overview</b>	<b>35</b>
	Configuring an L2TP LAC	35
<b>Chapter 4</b>	<b>Configuration Tasks for L2TP LAC</b>	<b>37</b>
	Configuring a Tunnel Profile for Subscriber Access	37
	Configuring the L2TP LAC Tunnel Selection Parameters	40
	Configuring LAC Tunnel Selection Failover Within a Preference Level	40
	Configuring Weighted Load Balancing for LAC Tunnel Sessions	41
	Preventing the LAC from Sending Calling Number AVP 22 to the LNS	42
	Configuring the Method to Set the LAC Connection Speeds to the LNS	42
	Transmission of the Receive Connect Speed AVP When Transmit and Receive Connect Speeds are Equal	44
	Preventing the LAC From Negotiating L2TP Failover Protocol	44
	Setting the Format for the Tunnel Name	45
	Configuring the LAC to Ignore Address and Port Changes Requested by the LNS	46
	Globally Configuring the LAC to Interoperate with Cisco LNS Devices	47
	Configuring the LAC to Report Access Line Information to the LNS	48
<b>Chapter 5</b>	<b>Configuration Tasks for L2TP LNS</b>	<b>51</b>
	Configuring an L2TP LNS with Inline Service Interfaces	51
	Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile	53
	Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface	54
	Configuring an L2TP Access Profile on the LNS	56
	Configuring a AAA Local Access Profile on the LNS	57
	Configuring an Address-Assignment Pool for L2TP LNS with Inline Services	58
	Configuring the L2TP LNS Peer Interface	60
	Enabling Inline Service Interfaces	61
	Configuring IP Inline Reassembly for L2TP	61
	Configuring an Inline Service Interface for L2TP LNS	63
	Configuring Options for the LNS Inline Services Logical Interface	64
	Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces	64
	Configuring a Pool of Inline Services Interfaces for Dynamic LNS Sessions	66
	Configuring a Dynamic Profile for Dynamic LNS Sessions	67
	Configuring the L2TP Destination Lockout Timeout	69
	Removing an L2TP Destination from the Destination Lockout List	69
	Configuring L2TP Tunnel Switching	70
<b>Chapter 6</b>	<b>Configuration Tasks for Both LAC and LNS</b>	<b>73</b>
	Configuring Retransmission Attributes for L2TP Control Messages	73
	Setting the L2TP Tunnel Idle Timeout	75
	Setting the L2TP Receive Window Size	76
	Setting the L2TP Destruct Timeout	76
	Enabling Tunnel and Global Counters for SNMP Statistics Collection	77
<b>Chapter 7</b>	<b>Example</b>	<b>79</b>
	Example: Configuring an L2TP LNS	79

<b>Chapter 8</b>	<b>Configuration Statements</b>	<b>91</b>
	[edit access tunnel-profile] Hierarchy Level	93
	[edit access tunnel-switch-profile] Hierarchy Level	94
	[edit services l2tp] Hierarchy Level	94
	aaa-access-profile (L2TP LNS)	96
	access-line-information (L2TP LAC)	97
	address (LNS Local Gateway)	97
	address (Tunnel Profile Remote Gateway)	98
	address (Tunnel Profile Source Gateway)	98
	assignment-id-format (L2TP LAC)	99
	avp (L2TP Tunnel Switching)	100
	bandwidth (Inline Services)	100
	bearer-type (L2TP Tunnel Switching)	101
	calling-number (L2TP Tunnel Switching)	102
	chap	103
	chap (Dynamic PPP)	104
	chap (L2TP)	104
	cisco-nas-port-info (L2TP Tunnel Switching)	105
	client	106
	destination (L2TP)	107
	destruct-timeout (L2TP)	108
	dial-options	109
	dial-options (Dynamic Profiles)	110
	disable-calling-number-avp (L2TP LAC)	110
	disable-failover-protocol (L2TP LAC)	111
	dynamic-profile (L2TP)	111
	enable-snmp-tunnel-statistics (L2TP)	112
	failover-within-preference (L2TP LAC)	112
	fpc (MX Series 3D Universal Edge Routers)	113
	gateway-name (LNS Local Gateway)	114
	gateway-name (Tunnel Profile Remote Gateway)	114
	gateway-name (Tunnel Profile Source Gateway)	115
	group-profile (Group Profile)	116
	hello-interval	117
	identification (Tunnel Profile)	117
	idle-timeout (Access)	118
	idle-timeout (L2TP)	119
	inline-services (FPC Level)	120
	inline-services (PIC level)	120
	interface (L2TP Service Interfaces)	121
	interface-id	122
	ip-reassembly	123
	ip-reassembly-rules (Service Set)	124
	ip-reassembly (L2TP)	125
	keepalive	126
	keepalives	127
	keepalives (Dynamic Profiles)	128
	l2tp	129
	l2tp-access-profile	131

lcp-renegotiation	131
local-gateway (L2TP LNS)	132
lockout-timeout (L2TP Destination Lockout)	133
logical-system (Tunnel Profile)	134
match-direction (IP Reassembly Rule)	134
maximum-sessions-per-tunnel	135
max-sessions (Tunnel Profile)	135
medium (Tunnel Profile)	136
minimum-retransmission-timeout (L2TP Tunnel)	136
nas-port-method (L2TP LAC)	137
nas-port-method (Tunnel Profile)	137
next-hop-service	138
pap	139
pap (Dynamic PPP)	140
pap (L2TP)	140
pic (M Series and T Series Routers)	141
pool (L2TP Service Interfaces)	142
ppp (Group Profile)	143
ppp-options	144
ppp-options (Dynamic PPP)	145
ppp-options (L2TP)	146
preference (Tunnel Profile)	146
remote-gateway (Tunnel Profile)	147
request services l2tp destination unlock	148
retransmission-count-established (L2TP)	149
retransmission-count-not-established (L2TP)	150
routing-instance (Tunnel Profile)	150
rule (IP Reassembly)	151
rx-connect-speed-when-equal (L2TP LAC)	152
rx-window-size (L2TP)	152
secret (Tunnel Profile)	153
service-device-pool (L2TP)	153
service-device-pools (L2TP Service Interfaces)	154
service-interface	155
shared-secret	155
source-gateway (Tunnel Profile)	156
tos-reflect (L2TP)	156
traceoptions (L2TP)	157
tunnel (Tunnel Profile)	162
tunnel (L2TP)	163
tunnel-group	164
tunnel-profile (L2TP Tunnel Switching)	165
tunnel-profile (Tunnel Profile)	166
tunnel-switch-profile (L2TP Tunnel Switching, Application)	167
tunnel-switch-profile (L2TP Tunnel Switching, Definition)	167
tx-address-change (L2TP LAC)	168
tx-connect-speed-method (L2TP LAC)	169
type (Tunnel Profile)	170
user-group-profile	170

	weighted-load-balancing (L2TP LAC) . . . . .	171
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 9</b>	<b>Verifying and Monitoring Configurations . . . . .</b>	<b>175</b>
	Verifying and Managing L2TP for Subscriber Access . . . . .	175
	Testing L2TP Tunnel Configurations from the LAC . . . . .	176
<b>Chapter 10</b>	<b>Monitoring Commands . . . . .</b>	<b>179</b>
	clear services l2tp destination . . . . .	180
	clear services l2tp session . . . . .	181
	clear services l2tp session statistics . . . . .	183
	clear services l2tp tunnel . . . . .	185
	clear services l2tp tunnel statistics . . . . .	187
	restart . . . . .	189
	show ppp interface . . . . .	200
	show services inline ip-reassembly statistics . . . . .	209
	show services l2tp destination . . . . .	215
	show services l2tp destination lockout . . . . .	219
	show services l2tp session . . . . .	220
	show services l2tp tunnel-switch destination . . . . .	228
	show services l2tp tunnel-switch session . . . . .	232
	show services l2tp tunnel-switch tunnel . . . . .	237
	show services l2tp tunnel-switch summary . . . . .	242
	show services l2tp summary . . . . .	244
	show services l2tp tunnel . . . . .	249
	show subscribers . . . . .	255
	show subscribers summary . . . . .	273
	test services l2tp tunnel . . . . .	278
<b>Part 4</b>	<b>Troubleshooting</b>	
<b>Chapter 11</b>	<b>Acquiring Troubleshooting Information . . . . .</b>	<b>283</b>
	Tracing L2TP Operations for Subscriber Access . . . . .	283
	Configuring the L2TP Trace Log Filename . . . . .	284
	Configuring the Number and Size of L2TP Log Files . . . . .	285
	Configuring Access to the L2TP Log File . . . . .	285
	Configuring a Regular Expression for L2TP Messages to Be Logged . . . . .	286
	Configuring the L2TP Tracing Flags . . . . .	286
	Configuring Subscriber Filtering for L2TP Trace Operations . . . . .	287
	Configuring the Severity Level to Filter Which L2TP Messages Are Logged . . . . .	288
	Collecting Subscriber Access Logs Before Contacting Juniper Technical Support . . . . .	289
<b>Chapter 12</b>	<b>Troubleshooting Configuration Statement . . . . .</b>	<b>293</b>
	traceoptions (L2TP) . . . . .	294
<b>Part 5</b>	<b>Index</b>	
	Index . . . . .	301





# List of Figures

<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>L2TP in Subscriber Access Networks . . . . .</b>	<b>3</b>
	Figure 1: Typical L2TP Topology . . . . .	3
	Figure 2: Protocol Stacking for L2TP Subscribers in Pass-Through Mode . . . . .	4
	Figure 3: L2TP Tunnel Switching Network Topology . . . . .	11
	Figure 4: L2TP Tunnel Switching for Incoming Calls . . . . .	13
<b>Chapter 2</b>	<b>L2TP LAC . . . . .</b>	<b>19</b>
	Figure 5: Sample L2TP Network Topology . . . . .	29



# List of Tables

	<b>About the Documentation</b> . . . . .	<b>xiii</b>
	Table 1: Notice Icons . . . . .	xv
	Table 2: Text and Syntax Conventions . . . . .	xvi
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>L2TP in Subscriber Access Networks</b> . . . . .	<b>3</b>
	Table 3: L2TP Terms . . . . .	5
	Table 4: Cause of CDN Message . . . . .	14
	Table 5: Cause of StopCCN Message . . . . .	14
	Table 6: LAC, LNS, and LTS Actions Taken for Switched Tunnels in Response to Administrative clear Commands . . . . .	15
	Table 7: Default Action for Handling L2TP AVPs at the Switching Boundary . . . . .	16
<b>Chapter 2</b>	<b>L2TP LAC</b> . . . . .	<b>19</b>
	Table 8: L2TP AVPs That Provide Subscriber Access Line Information . . . . .	29
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 6</b>	<b>Configuration Tasks for Both LAC and LNS</b> . . . . .	<b>73</b>
	Table 9: SNMP Counters for L2TP Statistics . . . . .	77
<b>Chapter 7</b>	<b>Example</b> . . . . .	<b>79</b>
	Table 10: VSA and Standard RADIUS Attribute Names, Order, and Values Required for Example . . . . .	79
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 10</b>	<b>Monitoring Commands</b> . . . . .	<b>179</b>
	Table 11: show ppp interface Output Fields . . . . .	200
	Table 12: show services inline ip-reassembly statistics Output Fields . . . . .	209
	Table 13: show services l2tp destination Output Fields . . . . .	215
	Table 14: show services l2tp destination lockout Output Fields . . . . .	219
	Table 15: show services l2tp session Output Fields . . . . .	221
	Table 16: show services l2tp tunnel-switch destination Output Fields . . . . .	228
	Table 17: show services l2tp tunnel-switch session Output Fields . . . . .	232
	Table 18: show services l2tp tunnel-switch tunnel Output Fields . . . . .	237
	Table 19: show services l2tp tunnel-switch summary Output Fields . . . . .	242
	Table 20: show services l2tp summary Output Fields . . . . .	244
	Table 21: show services l2tp tunnel Output Fields . . . . .	250
	Table 22: show subscribers Output Fields . . . . .	258
	Table 23: show subscribers Output Fields . . . . .	274

Table 24: test services l2tp tunnel Output Fields . . . . . 278

# About the Documentation

- Documentation and Release Notes on page xiii
- Supported Platforms on page xiii
- Using the Examples in This Manual on page xiii
- Documentation Conventions on page xv
- Documentation Feedback on page xvii
- Requesting Technical Support on page xvii

## Documentation and 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/>.

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

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

## Supported Platforms

---

For the features described in this document, the following platforms are supported:

- MX Series

## Using the Examples in This Manual

---

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

## Merging a Full Example

To merge a full example, follow these steps:

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xsl;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

## Merging a Snippet

To merge a snippet, follow these steps:

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
```

```
file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

## Documentation Conventions

Table 1 on page xv defines notice icons used in this guide.

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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xvi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols ospf area area-id] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub</b> <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast</b>   <b>multicast</b>  ( <i>string1</i>   <i>string2</i>   <i>string3</i> )
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members</b> [ <i>community-ids</i> ]
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

---

#### GUI Conventions

---



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

Convention	Description	Examples
<b>Bold text like this</b>	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto: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 (if applicable)

## 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: <http://kb.juniper.net/InfoCenter/>
- 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 in Subscriber Access Networks on page 3](#)
- [L2TP LAC on page 19](#)



## CHAPTER 1

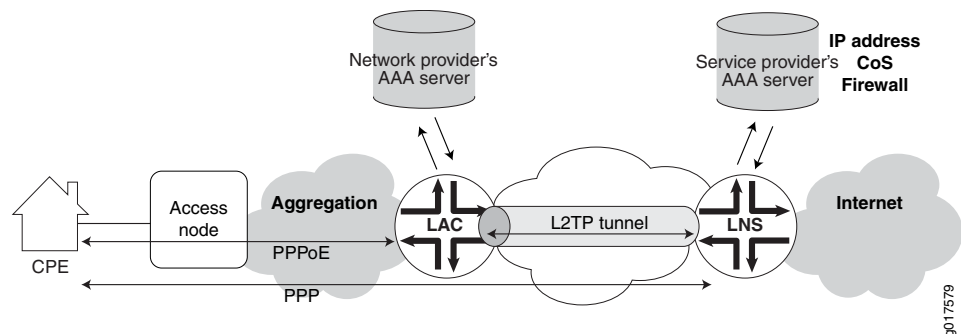
# L2TP in Subscriber Access Networks

- [L2TP for Subscriber Access Overview on page 3](#)
- [L2TP Terminology on page 5](#)
- [L2TP Implementation on page 6](#)
- [Retransmission of L2TP Control Messages on page 8](#)
- [L2TP and Graceful Routing Engine Switchover on page 10](#)
- [L2TP Tunnel Switching Overview on page 11](#)
- [Tunnel Switching Actions for L2TP AVPs at the Switching Boundary on page 15](#)
- [LAC Interoperation with Third-Party LNS Devices on page 17](#)

## L2TP for Subscriber Access Overview

The Layer 2 Tunneling Protocol (L2TP) is a client-server protocol that allows the Point-to-Point Protocol (PPP) to be tunneled across a network. L2TP encapsulates Layer 2 packets, such as PPP, for transmission across a network. An L2TP access concentrator (LAC), configured on an access device, receives packets from a remote client and forwards them to an L2TP network server (LNS) on a remote network. The LNS functions as the logical termination point of the PPP session tunneled by the LAC from the remote client. [Figure 1 on page 3](#) shows a simple L2TP topology.

Figure 1: Typical L2TP Topology

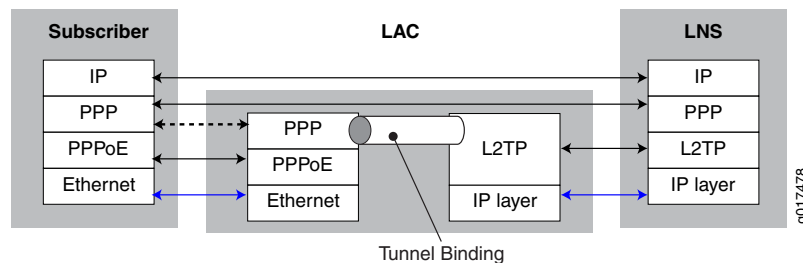


L2TP separates the termination of access technologies, such as cable or xDSL, from the termination of PPP and subsequent access to a network. This separation enables public ISPs to outsource their access technologies to competitive local exchange carriers

(CLECs). L2TP provides ISPs the capability to supply VPN service; private enterprises can reduce or avoid investment in access technologies for remote workers.

You can configure your router to act as the LAC in PPP 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 PPP session is terminated on the LNS. This LAC implementation supports only Point-to-Point Protocol over Ethernet (PPPoE) subscribers over dynamic or static logical interfaces. [Figure 2 on page 4](#) shows the protocol layer stacking for an L2TP pass-through connection.

**Figure 2: Protocol Stacking for L2TP Subscribers in Pass-Through Mode**



**NOTE:** On MX Series routers, the LAC and LNS functions are supported only on MPCs; they are not supported on any services PIC or MS-DPC. For details about MPC support for L2TP, see the [MX Series Interface Module Reference](#)

Certain M Series routers support LNS functions on services PICs. For more information about the L2TP implementation on M Series routers, see [L2TP Services Configuration Overview](#).

The LAC dynamically creates tunnels based on AAA authentication parameters and transmits L2TP packets to the LNS by means of the IP/User Datagram Protocol (UDP). Traffic travels in an L2TP *session*; a tunnel is an aggregation of one or more sessions. You can also provision a domain map that is used by AAA to determine whether to tunnel or terminate the PPPoE subscriber on the LAC. A one-to-one mapping exists between each PPP subscriber tunneled to the LNS and an L2TP session.

When the LNS is an MX Series router, a LAC-facing peer interface on an MPC provides an IP address for the exchange of IP packets between the tunnel endpoints; the Routing Engine maintains the L2TP tunnels. The Packet Forwarding Engine hosts one or more inline services (si) interfaces. These interfaces function like a virtual physical interface and *anchor* the L2TP sessions on the LNS. The si interface enables L2TP services without requiring a special services PIC. Finally, another interface is used to transmit the subscriber data to and from the Internet.

The characteristics of the tunnel can originate either from a tunnel profile that you configure or from RADIUS tunnel attributes and vendor-specific attributes (VSAs) from the AAA server accessible at the LAC. You can include a tunnel profile in a domain map, which applies the tunnel profile before RADIUS authentication takes place. You can use RADIUS standard attributes and VSAs to override any or all characteristics configured

by the tunnel profile in a domain map. Alternatively, RADIUS can itself apply a tunnel profile when the RADIUS Tunnel-Group VSA [26-64] is specified in the RADIUS login.

The Virtual-Router VSA [26-1] in the subscriber profile on the service provider AAA server (accessible from the LNS) determines the routing instance in which the L2TP session is brought up on the LNS. When this VSA is not present, the subscriber session comes up in the same routing instance as the tunnel, because the AAA server can be accessed only from the routing instance in which the tunnel terminates on the LNS.

This behavior is different than for DHCP and non-tunneled PPPoE subscribers, which come up in the default routing instance in the absence of the Virtual-Router VSA. For L2TP subscribers, you must include this VSA in the subscriber profile when you want the subscriber session to come up in a different routing instance than the tunnel routing instance.

The LAC supports RADIUS-initiated mirroring, which creates secure policies based on certain RADIUS VSAs, and uses RADIUS attributes to identify a subscriber whose traffic is to be mirrored. (This feature is not supported for an LNS configured on an MX Series router.)

The LAC and the LNS support unified ISSU. When an upgrade is initiated, the LAC completes any L2TP negotiations that are in progress but rejects any new negotiations until the upgrade has completed. No new tunnels or sessions are established during the upgrade. Subscriber logouts are recorded during the upgrade and are completed after the upgrade has completed.

#### Related Documentation

- *RADIUS IETF Attributes Supported by the AAA Service Framework*
- *Juniper Networks VSAs Supported by the AAA Service Framework*
- [Configuring a Tunnel Profile for Subscriber Access on page 37](#)
- *Domain Mapping Overview*
- [Subscriber Secure Policy and L2TP LAC Subscribers on page 19](#)
- *Unified ISSU Concepts*

## L2TP Terminology

Table 3 on page 5 describes the basic terms for L2TP.

**Table 3: L2TP Terms**

Term	Description
AVP	Attribute value pair (AVP)—Combination of a unique attribute—represented by an integer—and a value containing the actual value identified by the attribute.
Call	A connection (or attempted connection) between a remote system and the LAC.

Table 3: L2TP Terms (*continued*)

Term	Description
LAC	L2TP access concentrator (LAC)—A node that acts as one side of an L2TP tunnel endpoint and is a peer to the LNS. The LAC sits between an LNS and a remote system and forwards packets to and from each.
LNS	L2TP network server (LNS)—A node that acts as one side of an L2TP tunnel endpoint and is a peer to the LAC. The 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, either the LAC or LNS. The LAC's peer is an LNS, and vice versa.
Proxy authentication	PPP pre-authentication performed by the LAC on behalf of the LNS. The proxy data is sent by the LAC to the LNS containing attributes such as authentication type, authentication name, and authentication challenge. The LNS responds with the authentication results.
Proxy LCP	Link Control Protocol (LCP) negotiation that is performed by the LAC on behalf of the LNS. The proxy is sent by the LAC to the LNS containing attributes such as the last configuration attributes sent and received from the client.
Remote system	An end system or router attached to a remote access network, which is either the initiator or recipient of a call.
Session	A logical connection created between the LAC and the LNS when an end-to-end PPP connection is established between a remote system and the LNS.  <b>NOTE:</b> There is a one-to-one relationship between established L2TP sessions and their associated PPP connections.
Tunnel	A connection between the LAC-LNS pair consisting of a control connection and 0 or more L2TP sessions.

**Related Documentation**

- [L2TP for Subscriber Access Overview on page 3](#)

## L2TP Implementation

L2TP is implemented on four levels:

L2TP is implemented on four levels:

- Source—The local router acting as the LAC.
- Destination—The remote router acting as the LNS.
- 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 router acting as the LAC creates destinations, tunnels, and sessions dynamically, as follows:

The router acting as the LAC 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. The LAC negotiates on behalf of the LNS; this is known as *proxy LCP*.
3. The LAC authenticates the client on behalf of the LNS; this is known as *proxy authentication*. 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.

When a shared secret is configured in either the tunnel profile or the RADIUS attribute Tunnel-Password [69]—depending on which method is used to configure the tunnel—the secret is used to authenticate the tunnel during the establishment phase. The LAC includes the Challenge AVP in the SCCRP message sent to the LNS. The LNS returns the Challenge Response AVP in the SCCRP message. If the response from the LNS does not match the value expected by the LAC, then tunnel authentication fails and the tunnel is not established.

- 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

A router acting as an LNS might be set up as follows:

A router acting as an LNS might be set up as follows:

1. The LAC initiates a tunnel with the router acting as the LNS.
2. The LNS verifies that a tunnel with this LAC is valid: the destination is configured, the hostname and the tunnel password are correct.
3. The LNS completes the tunnel setup with the LAC.
4. The LAC sets up a session and initiates a session request to the LNS.
5. The LNS uses a static interface or creates a dynamic interface to anchor the PPP session.
6. If they are enabled and present, the LNS accepts the proxy LCP and the proxy authentication data and passes them to PPP.
7. PPP processes the proxy LCP, if it is present, and, if the proxy LCP is acceptable, places LCP on the LNS in opened state without renegotiation of LCP.
8. PPP processes the proxy authentication data, if it is present, and passes the data to AAA for verification. (If the data is not present, PPP requests the data from the peer.)



**NOTE:** When the proxy LCP is not present or not acceptable, the LNS negotiates LCP with the peer. When LCP renegotiation is enabled on the LNS, the LNS ignores any pre-negotiated LCP parameters and renegotiates both the LCP parameters and PPP authentication with the PPP client.

9. The LNS passes the authentication results to the peer.

### Related Documentation

- [L2TP for Subscriber Access Overview on page 3](#)

---

## Retransmission of L2TP Control Messages

L2TP peers maintain a queue of control messages that must be sent to the peer device. After the local peer (LAC or LNS) sends a message, it waits for a response from the remote peer. If a response is not received, the local peer retransmits the message. This behavior allows the remote peer more time to respond to the message.

You can control the retransmission behavior in the following two ways:

You can control the retransmission behavior in the following two ways:

- **Retransmission count**—You can configure how many times an unacknowledged message is retransmitted by the local peer. Increasing the count provides more opportunities for the remote peer to respond, but also increases the amount of control traffic. For tunnels that have been established, include the

**retransmission-count-established** statement at the **[edit services l2tp tunnel]** hierarchy level. For tunnels that are not yet established, include the **retransmission-count-not-established** statement.

- **Retransmission interval**—You can configure how long the local peer waits for the first response to a control message. If a response is not received within the first timeout interval, then the retransmission timer doubles the interval between each successive retransmission up to a maximum of 16 seconds. Increasing the interval gives the remote peer more time to respond, but also spends more resources on a potentially unavailable peer. Include the **minimum-retransmission-interval** statement at the **[edit services l2tp tunnel]** hierarchy level.

The local peer continues retransmitting the control message until one of the following occurs:

The local peer continues retransmitting the control message until one of the following occurs:

- A response is received within the current waiting period.
- The maximum retransmission count is reached.

If the maximum count is reached and no response has been received, the tunnel and all its sessions are cleared.



**NOTE:** Reaching the maximum interval of 16 seconds does not halt retransmissions. The local peer continues to wait 16 seconds after each subsequent retransmission.

The following examples describe the retransmission behavior in different circumstances:

The following examples describe the retransmission behavior in different circumstances:

- **Example 1**—The retransmission count is three and the minimum retransmission interval is 1 second.
  1. The local peer sends a control message.
  2. The local peer waits 1 second, but receives no response.
  3. The local peer retransmits the control message. This is the first retransmission.
  4. The local peer waits 2 seconds, but receives a response before the interval expires.
  5. Retransmission stops because a response is received within the interval.
- **Example 2**—The retransmission count is two and the minimum retransmission interval is 8 seconds.
  1. The local peer sends a control message.
  2. The local peer waits 8 seconds, but receives no response.

3. The local peer retransmits the control message. This is the first retransmission.
4. The local peer waits 16 seconds, but receives no response.
5. The local peer retransmits the control message. This is the second retransmission.
6. The local peer again waits 16 seconds, because the interval cannot increase beyond 16, but receives no response.
7. Retransmission stops because the maximum retransmission count of two was reached.
8. The tunnel and all its sessions are cleared.

**Related  
Documentation**

- [Configuring Retransmission Attributes for L2TP Control Messages on page 73](#)
- [L2TP for Subscriber Access Overview on page 3](#)

---

## L2TP and Graceful Routing Engine Switchover

Graceful Routing Engine switchover (GRES) is supported on MX Series routers acting as either the L2TP LAC or LNS. In the event that L2TP (the l2tp-universal-edge process) restarts or that the router fails over from the active routing engine (RE) to the standby RE, L2TP graceful Routing Engine switchover ensures that the following occurs:

Graceful Routing Engine switchover (GRES) is supported on MX Series routers acting as either the L2TP LAC or LNS. In the event that L2TP (the l2tp-universal-edge process) restarts or that the router fails over from the active routing engine (RE) to the standby RE, L2TP graceful Routing Engine switchover ensures that the following occurs:

- The LAC and the LNS recover destinations, tunnels, and sessions that were already established at the time of the failure or restart.
- The LAC and the LNS respond to tunnel keepalive requests received during the switchover for established tunnels, but do not generate any keepalives until the switchover is complete.
- The LAC and the LNS delete all the tunnels and sessions that are not in the Established state.
- The LAC and the LNS reject requests to create new tunnels and sessions.
- The LAC and the LNS send another disconnect notification to the peer for sessions and tunnels that are already in the Disconnecting state at the time of the failure or restart. For sessions and tunnels that were coming up at that time, the LAC and LNS send a disconnect notification to the peer.
- The LAC and the LNS restart timers for the full timeout period for recovered L2TP destinations, tunnels, and sessions.



**NOTE:** Graceful Routing Engine switchover is supported only by L2TP LAC and LNS on MX Series routers. It is not supported by L2TP LNS on M Series routers.

**Related Documentation**

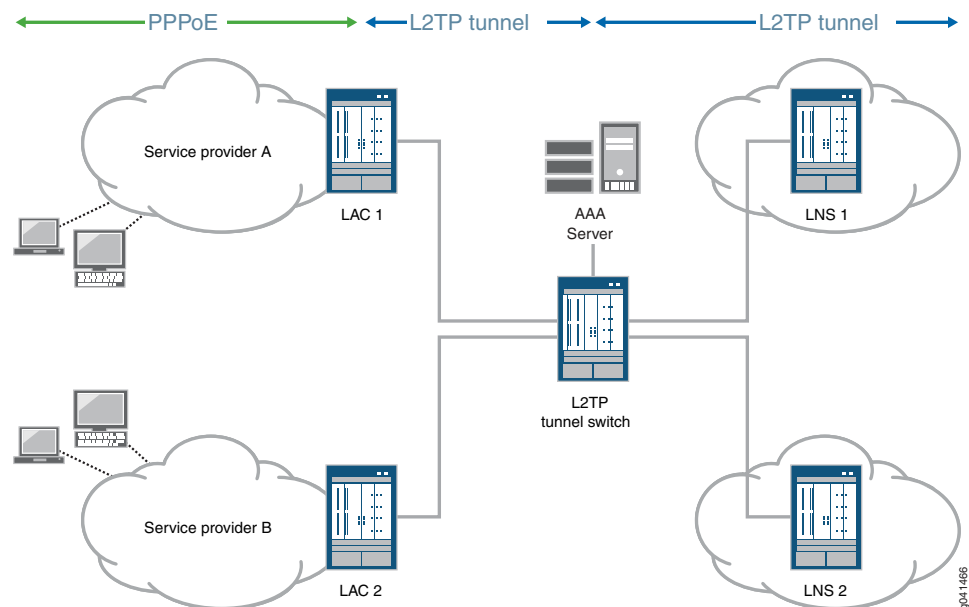
- [L2TP Failover and Peer Resynchronization on page 24](#)
- [L2TP for Subscriber Access Overview on page 3](#)

## L2TP Tunnel Switching Overview

L2TP tunnel switching, also known as L2TP multihop, simplifies the deployment of an L2TP network across multiple domains. A router that lies between a LAC and an LNS is configured as an *L2TP tunnel switch* (LTS)—sometimes referred to simply as a *tunnel switch* or a *tunnel switching aggregator* (TSA)—as shown in [Figure 3 on page 11](#). The LTS is configured as both an LNS and a LAC. When a remote LAC sends encapsulated PPP packets to the LNS configured on the LTS, the LTS can forward or redirect the packets through a different tunnel to a different LNS beyond the LTS. The logical termination point of the original L2TP session is switched to a different endpoint.

For example, in the network shown in [Figure 3 on page 11](#), packets from the subscriber provisioned by service provider A are initially targeted at the LNS configured on the LTS. The LTS might redirect those packets to LNS1.

**Figure 3: L2TP Tunnel Switching Network Topology**



L2TP tunnel switching simplifies network configuration when the administrative domain of a LAC is different from that of the desired LNS. For example:

L2TP tunnel switching simplifies network configuration when the administrative domain of a LAC is different from that of the desired LNS. For example:

- The LTS acts as the LNS for multiple LACs. The individual LACs do not have to have the administrative control or capability required to identify the most appropriate LNS on which to terminate their sessions. The LTS performs that function is centralized in the LTS.
- The LTS acts as the LAC for multiple LNSs. When a new remote LAC is added to an ISP's network, the ISP does not have to reconfigure its LNS routers to accommodate the new LAC, because they connect to the LAC on the LTS.

In a Layer 2 wholesale network, the wholesaler can use L2TP tunnel switching to create a flatter network configuration that is easier to manage. The wholesaler bundles Layer 2 sessions from a LAC that are destined for different ISPs—and therefore different LNSs—onto a single L2TP tunnel. This configuration enables a common L2TP control connection to be used for the LAC.

[Figure 4 on page 13](#) shows an example of L2TP tunnel switching for incoming calls with the following sequence of events:

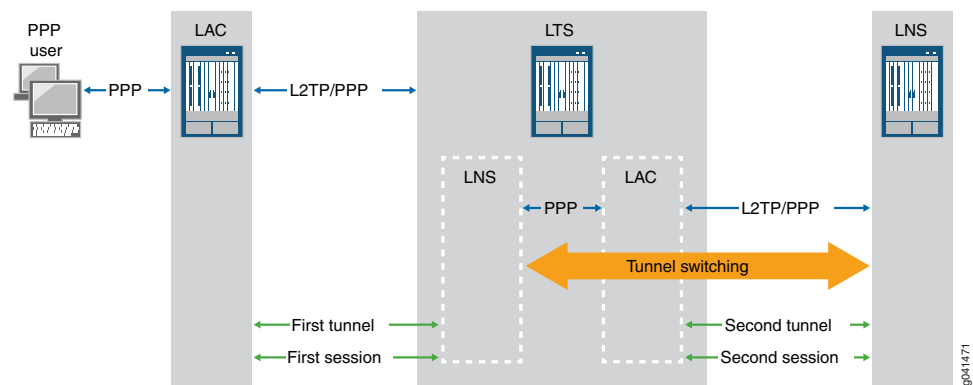
[Figure 4 on page 13](#) shows an example of L2TP tunnel switching for incoming calls with the following sequence of events:

1. The subscriber opens a PPP session to the LAC.
2. The LAC creates the first L2TP tunnel to the LNS configured on the LTS and the first L2TP session to carry the encapsulated PPP packets.
3. During authentication of this first session, the LTS determines whether to retunnel the session to an LNS beyond the LTS, based on the presence or absence of a tunnel switch profile configured on the LTS.

The tunnel switch profile can be a default profile or it can be applied by the RADIUS server, a domain map configuration, or a tunnel group configuration.

4. If a tunnel switch profile is configured, the LTS creates a second tunnel (if it does not already exist) to the LNS beyond the LTS as specified in the profile and creates the second session in this tunnel.

Figure 4: L2TP Tunnel Switching for Incoming Calls



## Application of Tunnel Switch Profiles

You can configure a tunnel switch profile to be applied in several ways:

You can configure a tunnel switch profile to be applied in several ways:

- As a default profile applied globally to traffic received from all LACs
- With a domain map applied to a subscriber session
- With a tunnel group applied to a subscriber session
- In your RADIUS server configuration

You can configure more than one of these methods of application. When multiple tunnel switch profiles are present, the following order of precedence establishes which profile the LTS uses; the order is from highest (RADIUS) to lowest (default profile):

You can configure more than one of these methods of application. When multiple tunnel switch profiles are present, the following order of precedence establishes which profile the LTS uses; the order is from highest (RADIUS) to lowest (default profile):

RADIUS > domain map > tunnel group > default tunnel switch profile

The tunnel switch profile must also reference a tunnel profile. This tunnel profile specifies the characteristics of the second tunnel, to which the subscriber packets are switched.

## Termination of Tunnel-Switched Sessions on the LTS

Tunnel switched sessions are terminated on the LTS when any of the following happens:

Tunnel switched sessions are terminated on the LTS when any of the following happens:

- Either the LAC or LNS interface on the LTS receives a Call-Disconnect-Notify (CDN) message ([Table 4 on page 14](#)).

Table 4: Cause of CDN Message

CDN Message Is Received On	When
LAC interface	<p>Either of the following occurs:</p> <p>Either of the following occurs:</p> <ul style="list-style-type: none"> <li>The second session cannot be established.</li> <li>The remote LNS terminates the second session.</li> </ul>
LNS interface	<p>Either of the following occurs:</p> <p>Either of the following occurs:</p> <ul style="list-style-type: none"> <li>The PPPoE client initiates a logout.</li> <li>The originating LAC initiates termination of the tunnel</li> </ul>

Both the first and second sessions are terminated because the LTS relays the CDN to the interface that did not receive the CDN. The disconnect cause is the same for both sessions.

- Either the LAC or LNS interface on the LTS receives a Stop-Control-Connection-Notification (StopCCN) message ([Table 5 on page 14](#)).

Table 5: Cause of StopCCN Message

StopCCN Message Is Received On	When
LAC interface	<p>Either of the following occurs:</p> <p>Either of the following occurs:</p> <ul style="list-style-type: none"> <li>The second session cannot be established.</li> <li>The remote LNS terminates the second tunnel.</li> </ul>
LNS interface	The originating LAC initiates termination of the tunnel.

The LTS does not relay the StopCCN message, because a given tunnel can contain both switched and nonswitched sessions. Another reason in a wholesale scenario is that the tunnel ending on the LNS on the LTS can contain sessions from LACs from different providers. Instead, the LTS sends a CDN message to the interface that did not receive the StopCCN to terminate the tunnel-switched session. This CDN relays the error code carried in the StopCCN.

- An administrative **clear** command is issued on the LTS.

[Table 6 on page 15](#) lists the actions taken when an administrative **clear** command is issued on the LTS.



Table 6: LAC, LNS, and LTS Actions Taken for Switched Tunnels in Response to Administrative clear Commands

Command	LAC or LNS Action	LTS Action
<code>clear services l2tp destination</code>	Clear the destination and all associated tunnels and sessions.	For each switched session in a tunnel to the destination, clear the corresponding mapped switched session by sending it a CDN message with the cause set to Administrative.
<code>clear services l2tp destination all</code>	Clear all destinations and all associated tunnels and sessions.	None.
<code>clear services l2tp session</code>	Clear the session.	Clear the corresponding mapped switched session for this session by sending it a CDN message with the cause set to Administrative.
<code>clear services l2tp session all</code>	Clear all sessions.	None.
<code>clear services l2tp tunnel</code>	Clear the tunnel and all its sessions.	For each switched session in the tunnel, clear the corresponding mapped switched session by sending it a CDN message with the cause set to Administrative.
<code>clear services l2tp tunnel all</code>	Clear all tunnels.	None.

#### Related Documentation

- [Configuring L2TP Tunnel Switching on page 70](#)
- [Tunnel Switching Actions for L2TP AVPs at the Switching Boundary on page 15](#)
- [L2TP for Subscriber Access Overview on page 3](#)

## Tunnel Switching Actions for L2TP AVPs at the Switching Boundary

When L2TP tunnel switching redirects packets to a different LNS, it performs one of the following default actions at the switching boundary for each AVP carried in the L2TP messages:

When L2TP tunnel switching redirects packets to a different LNS, it performs one of the following default actions at the switching boundary for each AVP carried in the L2TP messages:

- **regenerate**—L2TP regenerates the AVP based on the local policy at the LTS and sent in the switched packet. The local policy may or may not use the value for the AVP received during negotiation for the first session.
- **relay**—L2TP transparently forwards the AVP in the switched packet with no alteration.

[Table 7 on page 16](#) lists the default action for each AVP. Mandatory AVPs are always included in the L2TP messages from the LAC; optional AVPs might be included in the messages.

You can optionally override the default action taken at the switching boundary for the Bearer Type AVP (18), Calling Number AVP (22), or Cisco NAS Port Info AVP (100). You

can configure any of these three AVPs to be dropped from the switched packets or regenerated, or you can restore the default relay action.



**NOTE:** L2TP AVPs that have their attribute values hidden are always regenerated at the switching boundary. The value is decoded and sent in clear text when the packet is forwarded to the remote LNS.

**Table 7: Default Action for Handling L2TP AVPs at the Switching Boundary**

AVP Name	AVP Type	L2TP Message Type	Default Action
Assigned Session Id	Mandatory	ICRQ, CDN	Regenerate
Assigned Tunnel Id	Mandatory	SCCRQ, CDN	Regenerate
Bearer Capabilities	Optional	SCCRQ	Regenerate
Bearer Type	Optional	ICRQ	Relay
Call Serial Number	Mandatory	ICRQ	Relay
Called Number	Optional	ICRQ	Relay
Calling Number	Optional	ICRQ	Relay
Challenge	Optional	SCCRQ	Regenerate
Challenge Response	Optional	SCCCN	Regenerate
Cisco NAS Port	Optional	ICRQ	Relay
Failover Capability	Optional	SCCRQ	Regenerate
Firmware Revision	Optional	SCCRQ	Regenerate
Framing Capabilities	Mandatory	SCCRQ	Regenerate
Framing Type	Mandatory	ICCN	Relay
Host Name	Mandatory	SCCRQ	Regenerate
Message Type	Mandatory	All	Regenerate
Physical Channel Id	Optional	ICRQ	Regenerate
Private Group Id	Optional	ICCN	Relay
Protocol Version	Mandatory	SCCRQ	Regenerate

Table 7: Default Action for Handling L2TP AVPs at the Switching Boundary (*continued*)

AVP Name	AVP Type	L2TP Message Type	Default Action
Proxy Authentication	Optional	ICCN	Relay if acceptable; otherwise regenerate
Proxy LCP	Optional	ICCN	Relay if acceptable; otherwise regenerate
Receive Window Size	Optional	SCCRQ	Regenerate
Rx Connect Speed	Optional	ICCN	Relay
Sequencing Required	Optional	ICCN	Regenerate
Sub-Address	Optional	ICRQ	Relay
Tie Breaker	Optional	SCCRQ	Regenerate
Tunnel Recovery	Optional	SCCRQ	Regenerate
Tx Connect Speed	Mandatory	ICCN	Relay
Vendor Name	Optional	SCCRQ	Regenerate

- Related Documentation**
- [L2TP Tunnel Switching Overview on page 11](#)
  - [Configuring L2TP Tunnel Switching on page 70](#)

## LAC Interoperation with Third-Party LNS Devices

In some network environments, the LAC may need to interoperate with an LNS configured on a device from another vendor that does not run Junos OS. Interoperation with Cisco Systems devices requires the LAC to communicate a NAS port type, but the LAC does not provide this information by default.

You can enable interoperation with Cisco Systems devices by configuring the NAS port method as **cisco-avp**, which causes the LAC to include the Cisco Systems NAS Port Info AVP (100) when it sends an incoming call request (ICRQ) to the LNS. The AVP includes information that identifies the NAS port and indicates whether the port type is ATM or Ethernet.

You can configure the NAS port method globally for all tunnels on the LAC or in a tunnel profile for only the tunnels instantiated by the profile.

You can also include the Tunnel-Nas-Port-Method VSA [26–30] in your RADIUS server configuration with the value set to 1 to indicate Cisco Systems CLID. In this case, RADIUS can override the global value by modifying or creating a tunnel profile. The RADIUS

configuration has precedence over the tunnel profile configuration, which in turn has precedence over the global LAC configuration.

If the LNS receiving the AVP is an MX Series router instead of a Cisco Systems device, the LNS simply ignores the AVP, unless the LNS is configured for L2TP tunnel switching. In that case, the LNS preserves the value of the AVP and passes it along when it switches tunnels for the LAC.

**Related  
Documentation**

- [Globally Configuring the LAC to Interoperate with Cisco LNS Devices on page 47](#)
- [Configuring a Tunnel Profile for Subscriber Access on page 37](#)
- [Configuring an L2TP LAC on page 35](#)
- *Juniper Networks VSAs Supported by the AAA Service Framework*
- [L2TP for Subscriber Access Overview on page 3](#)

## CHAPTER 2

# L2TP LAC

- [Subscriber Secure Policy and L2TP LAC Subscribers on page 19](#)
- [LAC Tunnel Selection Overview on page 19](#)
- [L2TP Failover and Peer Resynchronization on page 24](#)
- [IP Packet Fragment Reassembly for L2TP Overview on page 26](#)
- [Transmission of Tx Connect-Speed and Rx Connect-Speed AVPs from LAC to LNS on page 26](#)
- [Subscriber Access Line Information Forwarding by the LAC Overview on page 28](#)

### Subscriber Secure Policy and L2TP LAC Subscribers

---

RADIUS-initiated per-subscriber traffic mirroring can be applied to subscribers whose traffic is tunneled with L2TP. Both subscriber ingress traffic (from the subscriber into the tunnel) and subscriber egress traffic (from the tunnel to the subscriber) are mirrored at the subscriber-facing ingress interface on the LAC. The ingress traffic is mirrored after PPPoE decapsulation and before L2TP encapsulation. The egress traffic is mirrored after L2TP decapsulation. The mirrored packet includes the complete HDLC frame sent to the LNS rather than only the IP datagram.

#### Related Documentation

- [Subscriber Secure Policy Overview](#)
- [Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview](#)
- [RADIUS Attributes Used for Subscriber Secure Policy](#)

### LAC Tunnel Selection Overview

---

L2TP enables you to specify:

L2TP enables you to specify:

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

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

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

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

### Tunnel Selection Failover Between Preference Levels

When a user tries to log in to a domain, in the default method, the LAC attempts to connect to a destination in that domain by means of the associated tunnel with the highest preference level. If more than one destination in the domain is considered reachable by a tunnel in that preference level, the LAC randomly selects a destination and attempts to contact it through its associated tunnel at that level. If the LAC is unsuccessful, it marks the destination as unreachable—*locks out the destination*—and does not try to connect to that destination for a period of time called the *destination lockout timeout*. The timeout is configurable with a default value of five minutes. The LAC then moves to the next lower preference level and repeats the process.

For example, suppose that there are three destinations for a domain and a tunnel has been defined for each destination: A, B, and C. All destinations are considered reachable, and the preference levels for the tunnels are assigned as follows:

For example, suppose that there are three destinations for a domain and a tunnel has been defined for each destination: A, B, and C. All destinations are considered reachable, and the preference levels for the tunnels are assigned as follows:

- A at preference 0
- B at preference 1
- C at preference 2

When a PPP user tries to connect to the domain, the LAC acts as follows:

When a PPP user tries to connect to the domain, the LAC acts as follows:

1. The LAC initially attempts to reach a destination by a tunnel at preference level 0, destination A in this example.
2. If this connection attempt fails, the LAC excludes destination A from consideration for the length of the destination lockout timeout.
3. The LAC goes to the next level, preference level 1, to reach a destination for the domain. At preference level 1, it attempts to connect to destination B.

4. If the connection attempt to destination B fails, the LAC excludes destination B from consideration for the length of the destination lockout timeout.
5. The LAC goes to the next level, preference level 2, and attempts to connect to destination C, the only destination in the domain that is still available.
6. If that attempt also fails, the LAC excludes destination C from consideration for the length of the destination lockout timeout.
7. At this point, the LAC has attempted to connect to every destination through every tunnel available for the domain and cycles back to preference level 0. When the destination lockout timeout for destination A expires, the LAC can attempt again to connect to destination A, and so on.

Although the destination lockout timeout typically prevents an unreachable destination from being tried until the period expires, the timeout is ignored in some circumstances. For example, if all destinations at a preference level are marked as unreachable when a user tries to log in to a domain, the LAC chooses and attempts to connect to the destination that failed first and therefore has the shortest time remaining until the destination lockout timeout expires. The key is to understand that the LAC always chooses a single destination at each level of preference, even if all destinations have recently failed.

If more than one destination for the domain is present at a preference level, the LAC randomly selects among them. If the LAC fails to connect to a destination at all preference levels with destinations for the domain, it cycles back to the highest level that still has a destination not excluded by an attempt.

For example, suppose that again there are three destinations for a domain and a tunnel has been defined for each destination: A, B, and C. All destinations are considered reachable, but the tunnels are distributed among the preference levels as follows:

For example, suppose that again there are three destinations for a domain and a tunnel has been defined for each destination: A, B, and C. All destinations are considered reachable, but the tunnels are distributed among the preference levels as follows:

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

In this example, when a PPP user tries to connect to the domain, the LAC randomly selects between A and B at preference level 0 and chooses destination B.

In this example, when a PPP user tries to connect to the domain, the LAC randomly selects between A and B at preference level 0 and chooses destination B.

1. If the connection attempt to destination B fails, the LAC excludes destination B from consideration for the length of the destination lockout timeout.
2. The LAC goes to the next level, preference level 1, to reach a destination for the domain. At preference level 1, it attempts to connect to destination C.

3. If the connection attempt to destination C also fails, the LAC excludes destination C from consideration for the length of the destination lockout timeout.
4. The LAC cycles back to preference level 0.

The LAC cycles back to preference level 0.

- If destination B is still locked out, the LAC attempts to connect to destination A.
- If the lockout for destination B has expired, then the selection process starts over and the LAC again randomly selects between A and B to attempt a connection.

## Tunnel Selection Failover Within a Preference Level

When tunnel selection failover within a preference level is configured, if the LAC tries to connect to a destination and is unsuccessful, it selects a new destination at the same preference level. If all destinations at a preference level are marked as unreachable, the LAC does not attempt to connect to a destination at that level. It drops to the next lower preference level to select a destination.

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

For example, suppose that there are four destinations for a domain and a tunnel has been defined for each destination: A, B, C, and D. All destinations are considered reachable, and the preference levels for the tunnels are assigned as follows:

For example, suppose that there are four destinations for a domain and a tunnel has been defined for each destination: A, B, C, and D. All destinations are considered reachable, and the preference levels for the tunnels are assigned as follows:

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

In this example, when a PPP user tries to connect to the domain, the LAC randomly selects between A and B at preference level 0 and chooses destination B.

In this example, when a PPP user tries to connect to the domain, the LAC randomly selects between A and B at preference level 0 and chooses destination B.

1. If the connection attempt to destination B fails, the LAC excludes tunnel B from consideration for the length of the destination lockout timeout.
2. The LAC attempts to connect to destination A at preference level 0.
3. If the connection attempt to destination A fails, the LAC excludes destination A from consideration for the length of the destination lockout timeout.
4. The LAC goes to the next level, preference level 1, to reach a destination for the domain. At preference level 1, the LAC randomly selects tunnel C.
5. If the connection attempt to destination C fails, the LAC excludes destination C from consideration for the length of the destination lockout timeout.



6. The LAC attempts to connect to destination D at preference level 1.
7. If the connection attempt to destination D fails, the LAC attempts again to connect to destination B again, its original selection.
8. If this second connection attempt to destination B fails, the user session is rejected.

## Session Failover and Tunnel Selection Behavior

If the destinations in the tunnel selected by the LAC are all unreachable, then the client fails to establish a PPP session over that tunnel. If no other tunnels exist for the domain that also match the tunnel selection criteria, the LAC sends a failure notification to the client, which results in a log-in failure and requires the client to retry the log-in attempt. However, if more tunnels are available, then the LAC attempts to establish an alternate tunnel and client session until either it succeeds or no more tunnels are available for selection. The tunnel with the highest preference that can reach the destination is selected, unless the destination is locked out.

If the destination is unreachable or if the destination is locked out, the tunnel with the next higher preference is selected. The tunnel selection process continues until either a session is successfully created or no more tunnels are available. If the destinations are locked out on all the available tunnels, then when the LAC attempts to establish a connection to the destination for the tunnel with the lowest preference, it selects a destination from the list of tunnels with the shorted remaining lockout time.

This session failover behavior applies only when the destination is unreachable in the following instances:

This session failover behavior applies only when the destination is unreachable in the following instances:

- The LNS fails to return an SCCRP message in response to the SCCRQ message from the LAC after the maximum number of retransmission attempts.
- The tunnel is established, but the LNS does not return an ICRP message in response to the ICRQ from the LAC after the maximum number of retransmission attempts.

This session failover behavior does not apply in the following circumstances:

This session failover behavior does not apply in the following circumstances:

- The client terminates the connection.
- The tunnel is established, but the LNS sends a CDN message while the LAC is attempting to establish the session with the LNS. As a result, the subscriber login attempt fails.

## Tunnel Selection and Maximum Sessions per Tunnel

When the maximum number of sessions allowed per tunnel is configured, the LAC takes that setting into consideration during the tunnel selection process. The maximum number of sessions per tunnel can be configured through a RADIUS Tunnel-Max-Sessions VSA [26-64] or by including the **max-sessions** statement in a tunnel profile.

If a randomly selected tunnel has a current session count equal to its maximum session count, the LAC does not attempt to connect to a destination with that tunnel. Instead, it selects an alternate tunnel from the set of reachable tunnels at the same preference level. If no additional reachable tunnels exist at the current preference level, the LAC drops to the next lower preference level to make the selection. This process is consistent, regardless of which failover scheme is currently running on the LAC.

If the maximum number of sessions is not configured for a tunnel, then that tunnel has no upper limit on the number of sessions it can support. By default, the maximum sessions value is 0 (zero), which allows unlimited sessions in the tunnel.

### Tunnel Selection with Weighted Load Balancing

The maximum sessions value for a tunnel is used for weighted load balancing to select among multiple tunnels with the same preference level.

The weight of a tunnel is determined by the tunnel's maximum session limit and the maximum session limits of the other tunnels at the same preference level. The tunnel with the largest maximum session value has the largest weight. The tunnel with the next largest maximum session value has the next largest weight, and so on. The tunnel with the smallest maximum session value has the smallest weight.

#### Related Documentation

- [Configuring the L2TP LAC Tunnel Selection Parameters on page 40](#)
- [Configuring the L2TP Destination Lockout Timeout on page 69](#)

### L2TP Failover and Peer Resynchronization

---

L2TP failover enables a failed L2TP endpoint to resynchronize with its nonfailed peer during recovery and restart of the L2TP protocol on the failed endpoint. L2TP failover is enabled by default.

The failover and L2TP peer resynchronization process does all of the following:

The failover and L2TP peer resynchronization process does all of the following:

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

The router supports both the L2TP failover protocol method (described in *RFC 4951, Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover"*) and the L2TP silent failover method. The differences between these two methods are as follows:

The router supports both the L2TP failover protocol method (described in *RFC 4951, Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover"*) and the L2TP silent failover method. The differences between these two methods are as follows:

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

The default resynchronization method in Junos OS is *failover-protocol-fall-back-to-silent-failover*. The recovery method used depends on the results of the failover capability negotiation that takes place between L2TP peers when they establish a tunnel, which works as follows:

The default resynchronization method in Junos OS is *failover-protocol-fall-back-to-silent-failover*. The recovery method used depends on the results of the failover capability negotiation that takes place between L2TP peers when they establish a tunnel, which works as follows:

- L2TP on the LAC by default attempts to negotiate the L2TP failover protocol first. When L2TP determines that the remote peer supports the L2TP failover protocol, then the L2TP failover protocol method is used.
- When L2TP determines that the remote peer does not support the L2TP failover protocol, then the L2TP silent failover method is used. Falling back on this secondary method prevents the failover from forcing a disconnection of the tunnel to the peer and all its sessions.

You can change the default behavior by including the **disable-failover-protocol** statement at the **[edit services l2tp]** hierarchy level. This statement forces the LAC to operate only in silent failover mode. This configuration can be useful when routers that act as the LNS either are configured for silent failover or incorrectly negotiate use of the failover protocol even though they do not support it. However, when you issue this statement and the LNS supports only failover protocol, then the LAC cannot negotiate failover protocol, and recovery (failover protocol recovery initiated by the LNS) always fails.

#### Related Documentation

- [L2TP and Graceful Routing Engine Switchover on page 10](#)
- [L2TP for Subscriber Access Overview on page 3](#)

## IP Packet Fragment Reassembly for L2TP Overview

---

You can configure the service interfaces on the MX Series routers with modular port concentrators (MPCs) to support reassemble fragmented IP packets for an L2TP connection. When packets are transmitted over an L2TP connection, the packets may be fragmented during transmission and need to be reassembled before they are processed further. Efficient reassembly is important for network throughput, scalability, and graceful response to congestion.

Fragmentation of IP packets for transmission and the need to reassemble the IP packets at a destination is a feature of how Layer 2 (the frame layer) and Layer 3 (the packet layer) operate. The maximum size of a frame, set by the Maximum Transmission Unit (MTU) value, and the maximum size of a packet are determined independently. Typically the packet size can far exceed the MTU size defined for the outgoing connection. If the packet size (data plus IP and other headers) exceeds the configured frame size (usually set by the transport medium limits), the packet must be fragmented and split across multiple frames for transmission. Frames are always processed immediately, when they arrive (if error-free), but packet fragments cannot be processed until the whole packet has been reassembled. Each packet fragment inside a frame series, except the last packet fragment, has the more fragments (MF) IP header bit set, indicating that this packet is part of a whole. The last packet fragment inside a frame does not have this MF bit set and therefore ends the fragment sequence. After all of the fragments of a packet have arrived, the entire packet can be reassembled.

In an L2TP connection, packets are transmitted between the L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS). For an IP packet being transmitted over an L2TP connection, the packet is fragmented at the LAC, at an LNS, or at any intermediate router. IP reassembly parameters configured on the service interfaces of the LAC and the LNS determine how the fragments are reassembled at the service interfaces to ensure efficient reassembly over an L2TP connection.

- Related Documentation**
- [Configuring IP Inline Reassembly for L2TP on page 61](#)
  - *Protocols and Applications Supported by MX240, MX480, MX960, MX2010, and MX2020 Enhanced MPCs (MPCEs)*
  - [ip-reassembly on page 123](#)

## Transmission of Tx Connect-Speed and Rx Connect-Speed AVPs from LAC to LNS

---

An L2TP access concentrator (LAC) uses Incoming-Call-Connected (ICCN) messages to send the attribute-value pair (AVP) 24 (which represents the transmit connect speed) and the AVP 38 (which represents the receive connect speed) to the L2TP network server (LNS).

The value of speed in AVP 24 and AVP 38 is typically not greater than the value that is enforced by CoS on the LAC side of the network. Any difference between the speed reported in these AVPs and that enforced by CoS can occur because of differences

between the CoS configuration (of the source that is used to enforce a downstream speed) and the transmit connect speed method used to establish these AVPs.

When you include the **tx-connect-speed-method** statement at the **[edit services l2tp]** hierarchy level, the transmit connect speed method selected for the downstream speed, AVP 24, also applies to the selection of the upstream speed, AVP 38. You can configure the transmit and receive connect speeds to be derived from Point-to-Point Protocol over Ethernet (PPPoE) intermediate agent tags that are sent from the digital subscriber line access multiplexer (DSLAM) to the LAC, the Access Node Control Protocol (ANCP) settings of the underlying interface, or the recommended (advisory) shaping rate. When the method you specify as ANCP, PPPoE intermediate agent tags (PPPoE IA tags), or advisory shaping rate does not support an upstream speed, the static or advisory speed is used.

A fallback method is adopted to derive the transmit and receive connect speed values when these values cannot be determined from any of the configured methods, such as from the ANCP settings, the PPPoE IA tags, or the advisory shaping rate, or if the speed value is determined to be 0 from any of the configured methods.

If you configure the ANCP method to calculate the connect speed, the following sequence of events takes place:

1. The upstream and downstream connect speed values are derived from ANCP.
2. If the values cannot be derived from ANCP, the PPPoE IA tags are used to determine the values. If the PPPoE IA tags are present for either or both transmit and receive connect speeds, these values are used.
3. If the values cannot be derived from the PPPoE IA tags, the recommended (advisory) shaping rate configured on the PPPoE logical interface is used. If the advisory shaping rate is present for either or both transmit and receive connect speeds, these values are used.
4. If the values cannot be derived from the advisory shaping rate, the configured or default port speed is used for transmit and receive connect speeds.

If you configure the PPPoE IA tags method to calculate the connect speed, the following sequence of events takes place:

1. The upstream and downstream connect speed values are derived from PPPoE IA tags.
2. If the values cannot be derived from the PPPoE IA tags, the recommended (advisory) shaping rate configured on the PPPoE logical interface is used. If the advisory shaping rate is present for either or both transmit and receive connect speeds, these values are used.
3. If the values cannot be derived from the advisory shaping rate, the configured or default port speed is used for transmit and receive connect speeds.

If you configure the static or advisory downstream shaping rate method to calculate the connect speed, the following sequence of events takes place:

1. The upstream and downstream connect speed values are derived from the advisory shaping rate.
2. If the values cannot be derived from the advisory shaping rate, the default port speed is used for transmit and receive connect speeds.

The transmit connect speed, AVP 24, is set in the ICCN messages on the basis of the method for determining the transmit connect speed configured using the **tx-connect-speed-method** statement at the **[edit services l2tp]** hierarchy level. You can configure the method for determining the transmit connect speed in the following order of precedence:

1. **ancp**—The speed is derived from the configured ANCP value for the underlying interface. You can change this speed after a subscriber has logged in, but those changes do not affect the actual speed used by the LNS.
2. **pppoe-ia-tags**—PPPoE IA tags sent from the DSLAM to the LAC. This speed value is transmitted when a subscriber logs in and it cannot be subsequently changed. This value is used when the **ancp** value is not available. This speed does not apply to the subscribers that are already logged in; it is effective only for subscribers that log in after this setting has been saved.
3. **static**—The speed is derived from the recommended (advisory) shaping rate configured on the PPPoE logical interface underlying the subscriber interface. If the advisory shaping rate is not configured on the underlying interface, then the actual port speed is used.

If you do not configure the transmit connect speed using the CLI interface, and if the advisory speed is also not available, then the actual port speed is used. For ge and xe interfaces, the speed value is set to 10,000,000 and for ae interfaces, the speed value is set to 0 and sent in both AVP 24 and AVP 38.

**Related Documentation**

- [Transmission of the Receive Connect Speed AVP When Transmit and Receive Connect Speeds are Equal on page 44](#)
- [Configuring an L2TP LAC on page 35](#)

---

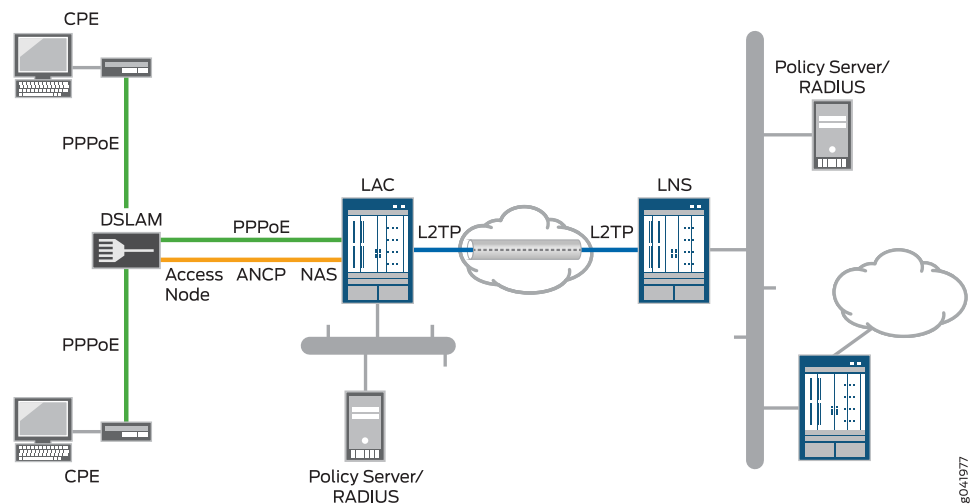
## Subscriber Access Line Information Forwarding by the LAC Overview

L2TP supports a set of AVPs that convey information about subscriber access lines from the LAC to the LNS. The information originates from an ANCP access node (DSLAM) and is distributed to the LAC by means of either DSL Forum VSAs in ANCP messages or PPPoE intermediate agent tags included in the PPPoE PADI and PADR messages.

In the network topology shown in [Figure 5 on page 29](#), when a subscriber initiates a connection through the CPE, the DSLAM relays the subscriber's PPPoE session to the router configured as a LAC. When the router has established the PPPoE session, the LAC initiates an L2TP tunnel to forward the subscriber's encapsulated PPP packets into the provider network.

In parallel to the PPPoE session, an ANCP connection between the DSLAM and the ANCP agent on the router conveys information about the subscriber's local loop as well as the link speeds of the PPPoE sessions on the local loop. The DSLAM sends the router Agent Circuit Id (ACI) and Agent Remote Id (ARI) strings that uniquely identify the DSLAM's receiving interface; this information is encoded in the ANCP Port Up and Port Down messages as Access Line Identifying TLVs. The ANCP messages can also include line attributes such as minimum, maximum, and actual net upstream and downstream data rates in the DSL Line Attributes TLV. The DSLAM can also send the access line attributes in vendor-specific tags that it inserts in the PADI and PADR messages.

**Figure 5: Sample L2TP Network Topology**



You can include the **access-line-information** statement at the **[edit services l2tp destination ip-address]** hierarchy level to configure the LAC to forward this access line information in the ICRQ message that it sends to the LNS. L2TP supports the AVPs listed in [Table 8 on page 29](#) to carry this information. The access line information is not required for the L2TP session to be initiated, and the establishment of that session is not delayed waiting for the values to be sent from the DSLAM.

**Table 8: L2TP AVPs That Provide Subscriber Access Line Information**

Attribute Value Pair	AVP Type (Corresponding DSL Forum VSA)	Description	L2TP Message Type
Actual Data Rate Downstream	130 (26–130)	64-bit unsigned integer; data rate in bits per sec.	ICRQ
Actual Data Rate Upstream	129 (26–129)	64-bit unsigned integer; data rate in bits per sec.	ICRQ
Actual Interleaving Delay Downstream	142 (26–142)	32-bit unsigned integer; maximum delay in milliseconds.	ICRQ

Table 8: L2TP AVPs That Provide Subscriber Access Line Information (*continued*)

Attribute Value Pair	AVP Type (Corresponding DSL Forum VSA)	Description	L2TP Message Type
Actual Interleaving Delay Upstream	140 (26–140)	32-bit unsigned integer; maximum delay in milliseconds.	ICRQ
Access Loop Encapsulation	144 (26–144)	Three one-octet encodings for data link, encapsulation 1, and encapsulation 2.	ICRQ
Agent Circuit ID	1 (26–1)	2-63 octet string; ACL of the logical access loop port on the DSLAM/access node.	ICRQ
Agent Remote ID	2 (26–2)	2-63 octet statically configured string; uniquely identifies subscriber on the DSLAM (access node).	ICRQ
ANCP Access Line Type	145 (none)	One octet encoding for transmission system type, followed by three MBZ (must be zero) octets (total 4 bytes). This value is not supplied in the ICRQ when the access line parameters are sourced from PPPoE-IA, because the ANCP-sourced information may not be immediately available.	ICRQ
Attainable Data Rate Upstream	133 (26–133)	64-bit unsigned integer; data rate in bits per sec.	ICRQ
Attainable Data Rate Downstream	134 (26–134)	64-bit unsigned integer; data rate in bits per sec.	ICRQ
Connect Speed Update Enable	98 (none)	Value does not matter: presence indicates support for CSUN, CSURQ message types for this session.	ICRQ
Connect Speed Update	97 (none)	Data structure listing remote session id and the current transmit and receive connection speeds in bits per second.	CSUN, CSURQ
IWF Session	254 (26–254)	Four-octet field indicating whether or not the internetworking function has been performed.	ICRQ



Table 8: L2TP AVPs That Provide Subscriber Access Line Information (*continued*)

Attribute Value Pair	AVP Type (Corresponding DSL Forum VSA)	Description	L2TP Message Type
Maximum Data Rate Downstream	136 (26–136)	64-bit unsigned integer; data rate in bits per sec.	ICRQ
Maximum Data Rate Upstream	135 (26–135)	64-bit unsigned integer; data rate in bits per sec.	ICRQ
Maximum Interleaving Delay Downstream	141 (26–141)	32-bit unsigned integer; maximum delay in milliseconds.	ICRQ
Maximum Interleaving Delay Upstream	139 (26–139)	32-bit unsigned integer; maximum delay in milliseconds.	ICRQ
Minimum Data Rate Downstream	132 (26–132)	64-bit unsigned integer; data rate in bits per sec.	ICRQ
Minimum Data Rate Downstream Low Power	138 (26–138)	64-bit unsigned integer; data rate in bits per sec.	ICRQ
Minimum Data Rate Upstream	131 (26–131)	64-bit unsigned integer; data rate in bits per sec.	ICRQ
Minimum Data Rate Upstream Low Power	137 (26–137)	64-bit unsigned integer; data rate in bits per sec.	ICRQ

You can also configure the LAC to notify the LNS when the speed of the subscriber connection changes from the values initially communicated to the LNS by AVP 24 and AVP 38 in ICCN messages. To do so, specify the **connection-speed-update** option with the **access-line-information** statement. When configured, the LAC informs the LNS that it can send these updates by including the Connect Speed Update Enable AVP (98) in the ICRQ message when the L2TP session starts up.

If the connection speed changes, the DSLAM notifies the ANCP agent. The ANCP agent then notifies the LAC, and the LAC in turn relays this information to the LNS by sending a Connect-Speed-Update-Notification (CSUN) message that includes a Connect Speed Update AVP (97) for each session. The LAC collects connection speed updates and sends them in a batch to minimize both the performance overhead on the LAC and the amount of traffic generated as a result of these notifications.

The presence of the Connect Speed Update Enable AVP (98) in the ICRQ message also informs the LNS that the LAC does respond if the LNS sends it a Connect-Speed-Update-Request (CSURQ) message. A third-party LNS can send this message type at any time during the life of a tunnel to request the current transmit and receive connection speed for one or more L2TP sessions. The LNS includes the session IDs in the CSURQ message. The LNS sends the CSURQ as part of failover recovery, for

example, when the LAC restarts. If the LAC has previously sent the Connect Speed Update Enable AVP (98) for the requested sessions, then it responds with a CSUN message that includes the Connect Speed Update AVP (97) for each session. If no changes to connection speeds have occurred by this time, the LAC simply includes the initial connection speed values that were reported in AVP 24 and AVP 38.

The absence of the Connect Speed Update Enable AVP (98) in the ICRQ message indicates that the LAC does not send updates for the life of the session. The LNS does not send a CSURQ to a LAC unless it has received AVP 98 from that LAC.



**BEST PRACTICE:** When you enable connection speed updates, we recommend that you also specify `ancp` with the `tx-connect-speed` statement as the source for the initial connection speeds reported in AVP 24 and AVP 38. This configuration aligns the initial source of connection speed with the preferred update source. The ANCP agent is the preferred source for both connection speed updates and access line characteristics.

If ANCP is not intended to be used for connection speed updates to the LAC, then we recommend that you do not enable connection speed updates. In the absence of access line information from the ANCP agent, the LAC forwards the speeds from the PPPoE-IA tags in the PPPOE PADR message. However, because these are only initial speed values and do not change, enabling connection speed updates is of no value.

---

**Related  
Documentation**

- [Configuring the LAC to Report Access Line Information to the LNS on page 48](#)
- [L2TP for Subscriber Access Overview on page 3](#)
- [\*DSL Forum Vendor-Specific Attributes\*](#)
- [Transmission of Tx Connect-Speed and Rx Connect-Speed AVPs from LAC to LNS on page 26](#)

## PART 2

# Configuration

- [Configuration Overview on page 35](#)
- [Configuration Tasks for L2TP LAC on page 37](#)
- [Configuration Tasks for L2TP LNS on page 51](#)
- [Configuration Tasks for Both LAC and LNS on page 73](#)
- [Example on page 79](#)
- [Configuration Statements on page 91](#)



## CHAPTER 3

# Configuration Overview

- [Configuring an L2TP LAC on page 35](#)

### Configuring an L2TP LAC

---

To configure an L2TP LAC:

To configure an L2TP LAC:

1. Configure a tunnel profile to apply to subscribers.  
[See “Configuring a Tunnel Profile for Subscriber Access” on page 37.](#)
2. (Optional) Configure the method used for selecting among multiple tunnels.
  - [See “Configuring the L2TP LAC Tunnel Selection Parameters” on page 40.](#)
  - [See “Configuring Weighted Load Balancing for LAC Tunnel Sessions” on page 41.](#)
  - [See “Configuring LAC Tunnel Selection Failover Within a Preference Level” on page 40.](#)
3. (Optional) Configure the LAC to not send Calling Number AVP 22 to the LNS.  
[See “Preventing the LAC from Sending Calling Number AVP 22 to the LNS” on page 42.](#)
4. (Optional) Specify the method for setting the transmit and receive connect speeds.  
[See “Configuring the Method to Set the LAC Connection Speeds to the LNS” on page 42.](#)
5. (Optional) Disable negotiation of the L2TP failover protocol to force use of only the silent failover resynchronization mechanism.  
[See “Preventing the LAC From Negotiating L2TP Failover Protocol” on page 44.](#)
6. (Optional) Specify the format for the tunnel name.  
[“Setting the Format for the Tunnel Name” on page 45.](#)
7. (Optional) Specify when and how many times L2TP retransmits unacknowledged control messages.  
[See “Configuring Retransmission Attributes for L2TP Control Messages” on page 73.](#)
8. (Optional) Specify how long a tunnel can remain idle before being torn down.  
[See “Setting the L2TP Tunnel Idle Timeout” on page 75.](#)

9. (Optional) Specify the L2TP receive window size for the L2TP tunnel. The receive window size specifies the number of packets a peer can send before waiting for an acknowledgment from the router.

See [“Setting the L2TP Receive Window Size” on page 76](#)

10. (Optional) Specify how long the L2TP retains information about terminated dynamic tunnels, sessions, and destinations.

See [“Setting the L2TP Destruct Timeout” on page 76](#).

11. (Optional) Specify how the LAC handles IP address or UDP port change requests.

See [“Configuring the LAC to Ignore Address and Port Changes Requested by the LNS” on page 46](#)

12. (Optional) Configure all tunnels on the LAC for interoperation with Cisco LNS devices.

See [“Globally Configuring the LAC to Interoperate with Cisco LNS Devices” on page 47](#).

13. (Optional) Specify that the LAC sends information to the LNS about subscriber access lines.

See [“Configuring the LAC to Report Access Line Information to the LNS” on page 48](#).

14. (Optional) Enable SNMP statistics counters.

See [“Enabling Tunnel and Global Counters for SNMP Statistics Collection” on page 77](#)

15. (Optional) Configure trace options for troubleshooting the configuration.

See [“Tracing L2TP Operations for Subscriber Access” on page 283](#)

**Related  
Documentation**

- [L2TP for Subscriber Access Overview on page 3](#)

## CHAPTER 4

# Configuration Tasks for L2TP LAC

- [Configuring a Tunnel Profile for Subscriber Access on page 37](#)
- [Configuring the L2TP LAC Tunnel Selection Parameters on page 40](#)
- [Configuring LAC Tunnel Selection Failover Within a Preference Level on page 40](#)
- [Configuring Weighted Load Balancing for LAC Tunnel Sessions on page 41](#)
- [Preventing the LAC from Sending Calling Number AVP 22 to the LNS on page 42](#)
- [Configuring the Method to Set the LAC Connection Speeds to the LNS on page 42](#)
- [Transmission of the Receive Connect Speed AVP When Transmit and Receive Connect Speeds are Equal on page 44](#)
- [Preventing the LAC From Negotiating L2TP Failover Protocol on page 44](#)
- [Setting the Format for the Tunnel Name on page 45](#)
- [Configuring the LAC to Ignore Address and Port Changes Requested by the LNS on page 46](#)
- [Globally Configuring the LAC to Interoperate with Cisco LNS Devices on page 47](#)
- [Configuring the LAC to Report Access Line Information to the LNS on page 48](#)

### Configuring a Tunnel Profile for Subscriber Access

The tunnel profile specifies a set of attributes to characterize the tunnel. The profile can be applied by a domain map or automatically when the tunnel is created.



**NOTE:** RADIUS attributes and VSAs can override the values you configured by a tunnel profile in a domain map. In the absence of a domain map, RADIUS can supply all the characteristics of a tunnel. The steps in the following procedure list the corresponding standard RADIUS attribute or VSA that you can configure on your RADIUS server to modify or configure the tunnel profile.

RADIUS-supplied attributes are associated with a tunnel by a tag carried in the attribute, which matches the tunnel identifier. A tag of 0 indicates the tag is not used. If L2TP receives a RADIUS attribute with a tag of 0, the attribute cannot be merged with the tunnel profile configuration corresponding to the subscriber domain because a tunnel profile cannot provide a tunnel tag (tunnel identifier) of 0. Only tags in the range of 1 through 31 are supported.

---

To configure a tunnel definition for a tunnel profile:

To configure a tunnel definition for a tunnel profile:

1. Specify the tunnel profile for which you are defining a tunnel. (Tunnel-Group [26-64])

```
[edit access]
user@host# set tunnel-profile profile-name
```

2. Specify an identifier (name) for the L2TP control connection for the tunnel.

```
[edit access tunnel-profile profile-name]
user@host# set tunnel tunnel-id
```

3. Configure the IP address of the local L2TP tunnel endpoint, the LAC. (Tunnel-Client-Endpoint [66])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set source-gateway address client-ip-address
```

4. Configure the IP address of the remote L2TP tunnel endpoint, the LNS. (Tunnel-Server-Endpoint [67])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set remote-gateway address server-ip-address
```

5. (Optional) Configure the preference level for the tunnel. (Tunnel-Preference [83])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set preference number
```

6. (Optional) Configure the hostname of the local client (LAC). (Tunnel-Client-Auth-Id [90])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set source-gateway gateway-name client-name
```

7. (Optional) Configure the hostname of the remote server (LNS). (Tunnel-Server-Auth-Id [91])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set remote-gateway gateway-name server-name
```



8. (Optional) Specify the medium (network) type for the tunnel. (Tunnel-Medium-Type [65])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set medium type
```

9. (Optional) Specify the protocol type for the tunnel. (Tunnel-Type [64])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set type tunnel-type
```

10. (Optional) Configure the assignment ID for the tunnel. (Tunnel-Assignment-Id [82])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set identification name
```

11. (Optional) Configure the maximum number of sessions allowed in the tunnel. (Tunnel-Max-Sessions [26-33])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set max-sessions number
```

12. (Optional) Configure the password for remote server authentication. (Standard RADIUS attribute Tunnel-Password [69] or VSA Tunnel-Password [26-9])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set secret password
```

13. (Optional) Configure the logical system to use for the tunnel.

If you configure a logical system, you must also configure a routing instance.

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set logical-system logical-system-name
```

14. (Optional) Configure the routing instance to use for the tunnel. (Tunnel-Virtual-Router [26-8])

If you configure a routing instance, configuring a logical system is optional.

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set routing-instance routing-instance-name
```

15. (Optional) Enable the LAC to interoperate with Cisco LNS devices. (Tunnel-Nas-Port-Method [26-30])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set nas-port-method cisco-avp
```

The following example shows a complete configuration for a tunnel profile:

```
tunnel-profile marketing {
  tunnel 1 {
    preference 5;
    remote-gateway {
      address 172.16.98.4;
      gateway-name work;
    }
    source-gateway {
      address 192.168.4.10;
      gateway-name local;
    }
  }
}
```

```
    }  
    secret mk5Sn$3k%V;  
    logical-system bos-metro-5;  
    routing-instance rox-12-32;  
    medium ipv4;  
    type l2tp;  
    identification tunnel_to_work;  
    max-sessions 32;  
    nas-port-method cisco avp;  
  }  
}
```

**Related  
Documentation**

- [Configuring an L2TP LAC on page 35](#)
- [Domain Mapping Overview](#)
- [LAC Interoperation with Third-Party LNS Devices on page 17](#)

---

## Configuring the L2TP LAC Tunnel Selection Parameters

When the LAC determines that a PPP session should be tunneled, it selects a tunnel from the set of tunnels associated with either the PPP user or the PPP user's domain. You can configure how a tunnel is selected and whether certain information is sent by the LAC to the LNS.

To configure tunnel selection parameters:

To configure tunnel selection parameters:

1. (Optional) Configure how a tunnel is selected when a connection attempt fails.  
See "[Configuring LAC Tunnel Selection Failover Within a Preference Level](#)" on page 40.
2. (Optional) Configure how sessions are load-balanced among tunnels.  
See "[Configuring Weighted Load Balancing for LAC Tunnel Sessions](#)" on page 41.

**Related  
Documentation**

- [LAC Tunnel Selection Overview on page 19](#)

---

## Configuring LAC Tunnel Selection Failover Within a Preference Level

You can configure how LAC tunnel selection continues in the event of a failure to connect. By default, when the router is unable to connect to a destination at a given preference level, it attempts to connect at the next lower level. You can specify that the router instead attempt to connect to another destination at the same level as the failed attempt.

If all destinations at a preference level are marked as unreachable, the router does not attempt to connect to a destination at that level. It drops to the next lower preference level to select a destination.

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

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

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

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

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

You configure the preference level used for this tunnel selection method in the tunnel profile or the RADIUS Tunnel-Preference [83] attribute.

To enable tunnel selection failover within a preference level:

To enable tunnel selection failover within a preference level:

- Specify failover within preference.

```
[edit services l2tp]
user@host# set failover-within-preference
```

#### Related Documentation

- [LAC Tunnel Selection Overview on page 19](#)
- [Configuring the L2TP LAC Tunnel Selection Parameters on page 40](#)
- [Configuring a Tunnel Profile for Subscriber Access on page 37](#)
- [Configuring How RADIUS Attributes Are Used for Subscriber Access](#)

## Configuring Weighted Load Balancing for LAC Tunnel Sessions

You can configure how L2TP LAC sessions are distributed across tunnels. You can specify that the router uses the maximum sessions per tunnel to choose among multiple tunnels that share the same preference level.

The weight of a tunnel is proportional to its maximum session limit and the maximum session limits of the other tunnels at the same preference level. The tunnel with the largest maximum session value has the highest weight. The tunnel with the next larger maximum session value has the next higher weight, and so on. The tunnel with the smallest maximum session value has the lowest weight.

When you configure weighted load balancing, the tunnel with the highest weight in the preference level is selected until the maximum number of sessions for the tunnel is reached. Then the router selects the tunnel with the next higher weight to establish connections until that tunnel's maximum session limit is reached, and so on.

To configure weighted load balancing:

To configure weighted load balancing:

- Specify load balancing.

```
[edit services l2tp]
user@host# set weighted-load-balancing
```

**Related  
Documentation**

- [LAC Tunnel Selection Overview on page 19](#)
- [Configuring the L2TP LAC Tunnel Selection Parameters on page 40](#)

---

## Preventing the LAC from Sending Calling Number AVP 22 to the LNS

Calling Number AVP 22 typically identifies the interface that is connected to the customer in the access network. When RADIUS includes the Calling-Station-Id in the Access-Accept message, that value is used for the Calling Number AVP. Otherwise, the underlying interface (for example, the S-VLAN IFL) on which the PPPoE session is established is used for the Calling Number AVP value.

By default, the LAC includes this AVP in the incoming-call request (ICRQ) packets that it sends to the LNS. However, you may wish to hide your network access interface information. To do so, you can configure the tunnel so that the LAC does not send the Calling Number AVP to the LNS.

To disable sending the Calling Number AVP:

To disable sending the Calling Number AVP:

- Configure disabling.

```
[edit services l2tp]
user@host# set disable-calling-number-avp
```

**Related  
Documentation**

- [LAC Tunnel Selection Overview on page 19](#)

---

## Configuring the Method to Set the LAC Connection Speeds to the LNS

During the establishment of an L2TP tunnel session, the LAC sends the L2TP transmit connect speed in bits per second (BPS) using AVP 24 to the LNS in Incoming-Call-Connected (ICCN) messages. AVP 24 conveys the transmit connect speed of the subscriber's access interface; that is, it represents the speed of the connection from the LAC to the LNS, from the perspective of the LAC. The L2TP receive connect speed, which is represented by AVP 38, is included in the message when the receive connect speed is different from the transmit connect speed. AVP 38 conveys the receive

connect speed of the connection from the LNS to the LAC, again from the perspective of the LAC. When AVP 38 is not sent, it means that the connection speed is the same in both directions; the LNS uses the value in AVP 24 for both transmit and receive connect speeds.

When the Tunnel-Tx-Speed-Method RADIUS VSA [26–94] is configured, RADIUS returns it in the Access-Accept message for individual subscribers. The TX speed is determined by the method set in this VSA: actual, CoS, or static layer 2. The dynamic layer 2 value is not supported, but is translated to static layer two rather than being rejected.

If the RADIUS VSA is not returned for the subscriber, then the TX speed is set according to the method that you configure globally with the **tx-connect-speed-method** statement at the **[edit services l2tp]** hierarchy level. The method configured specifies the resource that the LAC uses to set the speed.

You can configure what the LAC uses as a resource for setting these speeds. To use the recommended (advisory) downstream shaping rate for AVP 24 and the recommended upstream shaping rate for AVP 38, include the **tx-connect-speed-method static** statement at the **[edit services l2tp]** hierarchy level. You configure the advisory rates under the PPPoE logical interface underlying the subscriber interface with the **advisory-options** statement at the **[edit interfaces interface-name unit logical-unit-number]** hierarchy level. When the advisory speed is not configured on the underlying interface, the **tx-connect-speed-method advisory** statement automatically sets the speed to 1 Gbps and sends this value in both AVP 24 and AVP 38.

To derive the speeds from the PPPoE IA tags, use the **tx-connect-speed-method pppoe-ia-tags** statement. In this case, AVP 24 is the value of Actual-Data-Rate-Downstream (VSA 26-129). AVP 38 is the value of Actual-Data-Rate-Upstream (VSA 26-130), and is sent only when the VSA values differ.

To derive the speeds from the ANCP value configured on the PPPoE interface underlying the subscriber interface, use the **tx-connect-speed-method ancp** statement.

To set the method for calculating the transmit connect speed:

To set the method for calculating the transmit connect speed:

- Configure the ANCP method to use the values derived from the configured ANCP value for the underlying interface.

```
[edit services l2tp]
user@host# set tx-connect-speed-method ancp
```

- Configure the PPPoE IA tags method to use the values provided in the PPPoE IA tags.

```
[edit services l2tp]
user@host# set tx-connect-speed-method pppoe-ia-tags
```

- Configure the static (advisory downstream shaping rate) method to use the underlying interface's recommended shaping rates.

```
[edit services l2tp]
user@host# set tx-connect-speed-method static
```

- Related Documentation**
- [Configuring an L2TP LAC on page 35](#)

## Transmission of the Receive Connect Speed AVP When Transmit and Receive Connect Speeds are Equal

---

The L2TP Rx Connect Speed (in bits per second) AVP, which is represented by AVP 38, is included in the ICCN message when the receive connect speed is different from the transmit connect speed. By default, when the connection speed is the same in both directions, AVP 38 is not sent; the LNS uses the value in AVP 24 for both transmit and receive connect speeds.

AVP 38 is generated when the receive connect speed of the access interface is set equal to the calculated transmit connect speed by issuing the **rx-connect-speed-when-equal** statement at the **[edit services l2tp]** hierarchy level. In this scenario, the LAC transmits the same value for transmit and receive connect speeds that are sent to the LNS through the AVP 24 and AVP 38 in the ICCN message.

To configure the sending of AVP 38 when the connection speeds are the same in both the downstream and upstream directions:

To configure the sending of AVP 38 when the connection speeds are the same in both the downstream and upstream directions:

- Configure the transmission of the receive connect speed, AVP 38, when the receive connect speed is set equal to the calculated transmit connect speed.

```
[edit services l2tp]  
user@host# set rx-connect-speed-when-equal
```

- Related Documentation**
- [Transmission of Tx Connect-Speed and Rx Connect-Speed AVPs from LAC to LNS on page 26](#)
  - [Configuring an L2TP LAC on page 35](#)
  - [rx-connect-speed-when-equal on page 152](#)

## Preventing the LAC From Negotiating L2TP Failover Protocol

---

The L2TP LAC implementation on MX Series routers supports L2TP failover and peer resynchronization with a failed remote endpoint. The LAC supports both the L2TP failover protocol method and the L2TP silent failover method. By default, L2TP on the LAC attempts to negotiate the L2TP failover protocol with the LNS. When negotiation determines that the LNS supports this method, then the LAC uses L2TP failover protocol if the LNS fails. When the LNS does not support L2TP failover protocol, then the LAC uses silent failover in the event of an LNS failure. The ability to fall back on silent failover prevents the failover from forcing a disconnection of the tunnel to the peer and all the associated sessions.

You can disable the default behavior to force the LAC to operate only in silent failover mode. This configuration can be useful when routers that act as the LNS either are

configured for silent failover or incorrectly negotiate use of the failover protocol even though they do not support it. However, when you issue this statement and the LNS supports only failover protocol, then the LAC cannot negotiate failover protocol, and recovery (failover protocol recovery initiated by the LNS) always fails.

To disable negotiation of the L2TP failover protocol:

To disable negotiation of the L2TP failover protocol:

- Configure disabling.

```
[edit services l2tp]
user@host# set disable-failover-protocol
```

Related  
Documentation

- [Configuring an L2TP LAC on page 35](#)

## Setting the Format for the Tunnel Name

By default, the name of a tunnel corresponds to the Tunnel-Assignment-Id [82] returned by the AAA server. You can optionally configure the LAC to use more elements in the construction of a tunnel name by including the **assignment-id-format client-server-id** statement at the **[edit services l2tp tunnel]** hierarchy level. This format uses three attributes: Tunnel-Client-Auth-Id [90], Tunnel-Server-Endpoint [67], and Tunnel-Assignment-Id [82]. These attributes correspond, respectively, to the values configured in the tunnel profile for the LAC (source gateway) name, the tunnel endpoint (remote gateway) address on the LNS, and the tunnel ID.

A consequence of the **client-server-id** format is that the LAC automatically creates a new tunnel when the AAA server returns a different Tunnel-Client-Auth-Id than previously returned.



**NOTE:** Before you downgrade to a Junos OS Release that does not support this statement, we recommend that you explicitly unconfigure the feature by including the **no assignment-id-format assignment-id** statement at the **[edit services l2tp tunnel]** hierarchy level.

To change how the tunnel name is formatted:

To change how the tunnel name is formatted:

- Configure the format.

```
[edit services l2tp tunnel]
user@host# set assignment-id-format client-server-id
```

Related  
Documentation

- [Configuring an L2TP LAC on page 35](#)

## Configuring the LAC to Ignore Address and Port Changes Requested by the LNS

---

By default, when the LAC receives a request from the LNS in an SCCRP message to change the destination IP address or the UDP port, the LAC accepts the request and makes the change. If this is not the desired behavior, you can use the **tx-address-change** statement to configure how the LAC handles these change requests.

To configure how the LAC handles change requests for the IP address, the UDP port, or both:

To configure how the LAC handles change requests for the IP address, the UDP port, or both:

- (Optional) Specify the LAC to ignore all change requests.

```
[edit services l2tp tunnel]
user@host# set tx-address-change ignore
```

- (Optional) Specify the LAC to ignore only change requests for the IP address.

```
[edit services l2tp tunnel]
user@host# set tx-address-change ignore-ip-address
```

- (Optional) Specify the LAC to ignore only change requests for the UDP port.

```
[edit services l2tp tunnel]
user@host# set tx-address-change ignore-udp-port
```

- (Optional) Specify the LAC to accept all change requests.

```
[edit services l2tp tunnel]
user@host# set tx-address-change accept
```

Use the **show services l2tp summary** command to display the current behavior of the LAC:

```
show services l2tp summary
Failover within a preference level is Disabled
Weighted load balancing is Disabled
Tunnel authentication challenge is Enabled
Calling number avp is Enabled
Failover Protocol is Disabled
Tx Connect speed method is static
Rx speed avp when equal is Disabled
Tunnel assignment id format is assignment-id
Tunnel Tx Address Change is Ignore IP Address Change
Max Retransmissions for Established Tunnel is 7
Max Retransmissions for Not Established Tunnel is 5
Tunnel Idle Timeout is 60 seconds
Destruct Timeout is 300 seconds
Destination Lockout Timeout is 300 seconds
Destinations: 1, Tunnels: 0, Sessions: 0
```

### Related Documentation

- [Configuring an L2TP LAC on page 35](#)



## Globally Configuring the LAC to Interoperate with Cisco LNS Devices

Cisco LNS devices require from the LAC both the physical NAS port number identifier and the type of the physical port, such as Ethernet or ATM. By default, the LAC does not include this information. You can globally configure the LAC to provide this information by including the NAS Port Info AVP (100) in the ICRQ that it sends to the LNS. This configuration enables the LAC to interoperate with a Cisco LNS.

To globally configure the LAC to include the NAS Port Info AVP:

To globally configure the LAC to include the NAS Port Info AVP:

- Specify the NAS port method.

```
[edit services l2tp tunnel]
user@host# set nas-port-method cisco-avp
```



**NOTE:** This global configuration for the LAC can be overridden by the configuration in a tunnel profile or RADIUS.

Use the **show services l2tp tunnel extensive** command to display the current behavior of the LAC:

```
show services l2tp tunnel extensive
Tunnel local ID: 51872, Tunnel remote ID: 8660
Remote IP: 192.168.1.3:1701
Sessions: 5, State: Established
Tunnel Name: 1/tunnel-test-2
Local IP: 10.1.1.2:1701
Local name: testlac, Remote name: ce-lns
Effective Peer Resync Mechanism: silent failover
Nas Port Method: none
Tunnel Logical System: default, Tunnel Routing Instance: default
Max sessions: 128100, Window size: 4, Hello interval: 60
Create time: Thu Jul 25 12:55:41 2013, Up time: 11:18:14
Idle time: 00:00:00
Statistics since: Thu Jul 25 12:55:41 2013
```

	Packets	Bytes
Control Tx	702	15.5k
Control Rx	690	8.5k
Data Tx	153.3k	6.6M
Data Rx	126.3k	5.9M
Errors Tx	0	
Errors Rx	0	

### Related Documentation

- [LAC Interoperation with Third-Party LNS Devices on page 17](#)
- [Configuring a Tunnel Profile for Subscriber Access on page 37](#)
- [Configuring an L2TP LAC on page 35](#)

## Configuring the LAC to Report Access Line Information to the LNS

---

The L2TP AVP extensions defined in RFC 5515, *Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extension*, enable the LAC to report to the LNS characteristics of the subscriber's access line, such as identification attributes, line type, connection speed, various data rates, and so on. The LAC receives the access line information when the subscriber's CPE initiates a connection request, and forwards the available information in various AVPs included in ICRQ messages to the LNS. The LAC can also signal to the LNS that it is capable of sending updates about the subscriber connection speeds in the CSUN message.

By default, neither the access line information forwarding or connection speed update capability are enabled on the LAC. You must configure the capabilities for a specific LNS endpoint, which enables them for all tunnels with that destination IP address.



**NOTE:** Do not configure the connection-speed-update option when the LNS does not support connection speed changes. Configuring the option for such an LNS generates additional control messages that are ignored.

To configure the LAC to send information about subscriber access lines to the LNS:

To configure the LAC to send information about subscriber access lines to the LNS:

- Configure the capability.

```
[edit services l2tp destination ip-address]
user@host# set access-line-information
```

Alternatively, to configure the LAC to also send updates to the LNS about changes in connection speed:

Alternatively, to configure the LAC to also send updates to the LNS about changes in connection speed:

- Include the update option when you configure the capability.

```
[edit services l2tp destination ip-address]
user@host# set access-line-information connection-speed-update
```

- Typically, when you configure the LAC for updates, you also configure the ANCP agent as the source for the initial connection speed.

```
[edit services l2tp]
user@host# set tx-connect-speed-method ancp
```

Consider the following examples:

Consider the following examples:

- In this example, for all tunnels with an endpoint address of 192.168.1.2, the LAC reports access line characteristics sourced from the ANCP agent or the PPPoE intermediate agent (in that order) to the LNS in the ICRQ message. The Connect Speed Update

Enable AVP is not included in the ICRQ; consequently no CSUN messages are sent to the LNS to report speed changes in the subscriber access lines reported by the ANCP agent. The LAC ignores any CSURQ messages that it receives from the LNS.

```
[edit services l2tp destination 192.168.1.2]
user@host# set access-line-information
```

- In this example, for all tunnels with an endpoint address of 10.2.1.3, the LAC reports access line characteristics sourced from the ANCP agent or the PPPoE intermediate agent (in that order) to the LNS in the ICRQ message. The Connect Speed Update Enable AVP is included in the ICRQ; and CSUN messages are sent to the LNS to report speed changes in the subscriber access lines reported by the ANCP agent. The LAC accepts any CSURQ messages that it receives from the LNS and responds with a CSUN message.

```
[edit services l2tp destination 10.2.1.3]
user@host# set access-line-information connection-speed-update
user@host# up
user@host# set tx-connect-speed-method ancp
```

**Related  
Documentation**

- [Configuring an L2TP LAC on page 35](#)
- [Subscriber Access Line Information Forwarding by the LAC Overview on page 28](#)



## CHAPTER 5

# Configuration Tasks for L2TP LNS

- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)
- [Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile on page 53](#)
- [Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface on page 54](#)
- [Configuring an L2TP Access Profile on the LNS on page 56](#)
- [Configuring a AAA Local Access Profile on the LNS on page 57](#)
- [Configuring an Address-Assignment Pool for L2TP LNS with Inline Services on page 58](#)
- [Configuring the L2TP LNS Peer Interface on page 60](#)
- [Enabling Inline Service Interfaces on page 61](#)
- [Configuring IP Inline Reassembly for L2TP on page 61](#)
- [Configuring an Inline Service Interface for L2TP LNS on page 63](#)
- [Configuring Options for the LNS Inline Services Logical Interface on page 64](#)
- [Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64](#)
- [Configuring a Pool of Inline Services Interfaces for Dynamic LNS Sessions on page 66](#)
- [Configuring a Dynamic Profile for Dynamic LNS Sessions on page 67](#)
- [Configuring the L2TP Destination Lockout Timeout on page 69](#)
- [Removing an L2TP Destination from the Destination Lockout List on page 69](#)
- [Configuring L2TP Tunnel Switching on page 70](#)

### Configuring an L2TP LNS with Inline Service Interfaces

---

The L2TP LNS feature license must be installed before you begin the configuration. Otherwise, a warning message is displayed when the configuration is committed.

To configure an L2TP LNS with inline service interfaces:

To configure an L2TP LNS with inline service interfaces:

1. (Optional) Configure a user group profile that defines the PPP configuration for tunnel subscribers.

See [“Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile” on page 53.](#)

2. (Optional) Configure PPP attributes for subscribers on inline service interfaces.

See [“Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface” on page 54.](#)

3. Configure inline IP reassembly.

See [“Configuring IP Inline Reassembly for L2TP” on page 61.](#)

4. Configure an L2TP access profile that defines the L2TP parameters for each LNS client (LAC).

See [“Configuring an L2TP Access Profile on the LNS” on page 56.](#)

5. (Optional) Configure a AAA access profile to override the access profile configured under the routing instance.

See [“Configuring a AAA Local Access Profile on the LNS” on page 57.](#)

6. Configure a pool of addresses to be dynamically assigned to tunneled PPP subscribers.

See [“Configuring an Address-Assignment Pool for L2TP LNS with Inline Services” on page 58.](#)

7. Configure the peer interface to terminate the tunnel and the PPP server-side IPCP address.

See [“Configuring the L2TP LNS Peer Interface” on page 60.](#)

8. Enable inline service interfaces on an MPC.

See [“Enabling Inline Service Interfaces” on page 61.](#)

9. Configure a service interface.

See [“Configuring an Inline Service Interface for L2TP LNS” on page 63.](#)

10. Configure options for each inline service logical interface.

See [“Configuring Options for the LNS Inline Services Logical Interface” on page 64.](#)

11. Configure the L2TP tunnel group.

See [“Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces” on page 64.](#)

12. (Optional) Configure a dynamic profile that dynamically creates L2TP logical interfaces.

See [“Configuring a Dynamic Profile for Dynamic LNS Sessions” on page 67.](#)

13. (Optional) Configure a service interface pool for dynamic LNS sessions.

See [“Configuring a Pool of Inline Services Interfaces for Dynamic LNS Sessions”](#) on page 66.

14. (Optional) Specify how many times L2TP retransmits unacknowledged control messages.

See [“Configuring Retransmission Attributes for L2TP Control Messages”](#) on page 73.

15. (Optional) Specify how long a tunnel can remain idle before being torn down.

See [“Setting the L2TP Tunnel Idle Timeout”](#) on page 75.

16. (Optional) Specify the L2TP receive window size for the L2TP tunnel. The receive window size specifies the number of packets a peer can send before waiting for an acknowledgment from the router.

See [“Setting the L2TP Receive Window Size”](#) on page 76

17. (Optional) Specify how long the L2TP retains information about terminated dynamic tunnels, sessions, and destinations.

See [“Setting the L2TP Destruct Timeout”](#) on page 76.

18. (Optional) Configure the L2TP destination lockout timeout.

See [“Configuring the L2TP Destination Lockout Timeout”](#) on page 69.

19. (Optional) Configure L2TP tunnel switching.

See [“Configuring L2TP Tunnel Switching”](#) on page 70

20. (Optional) Enable SNMP statistics counters.

See [“Enabling Tunnel and Global Counters for SNMP Statistics Collection”](#) on page 77

21. (Optional) Configure trace options for troubleshooting the configuration.

See [“Tracing L2TP Operations for Subscriber Access”](#) on page 283

You also need to configure CoS for LNS sessions. For more information, see *Configuring Dynamic CoS for an L2TP LNS Inline Service*.

#### **Related Documentation**

- [L2TP for Subscriber Access Overview](#) on page 3
- *Junos OS Feature Licenses*
- *Software Feature Licenses*

---

## **Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile**

You can configure a user group profile that enables the LNS to apply PPP attributes to the PPP subscribers tunneled from the LAC. The user group profile is associated with clients (LACs) in the L2TP access profile. Consequently all subscribers handled by a given client share the same PPP attributes.

To configure a user group profile:

To configure a user group profile:

1. Create the profile.

```
[edit access]
user@host# edit group-profile profile-name
```

2. Configure the interval between PPP keepalive messages for the L2TP tunnel terminating on the LNS.

```
[edit access group-profile profile-name]
user@host# set ppp keepalive seconds
```



**NOTE:** Changes to the keepalive interval in a user group profile affect only new L2TP sessions that come up after the change. Existing sessions are not affected.

3. Configure PPP authentication methods that apply to tunneled PPP subscribers at the LNS.

```
[edit access group-profile profile-name]
user@host# set ppp ppp-options chap
user@host# set ppp ppp-options pap
```

4. Configure how long the PPP subscriber session can be idle before it is considered to have timed out.

```
[edit access group-profile profile-name]
user@host# set ppp idle-timeout 200
```



**NOTE:** You can also configure PPP attributes on a per-interface basis. See [“Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface” on page 54](#) for more information. When you configure the PPP attributes for L2TP LNS subscribers both on the si interface and in user group profiles, the inline service interface configuration takes precedence over the user group profile configuration.

**Related  
Documentation**

- [Configuring an L2TP Access Profile on the LNS on page 56](#)
- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)

---

## Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface

You can configure PPP attributes that are applied by the LNS on the inline service (si) interface to the PPP subscribers tunneled from the LAC. Because you are configuring the attributes per interface rather than with a user group profile, the attributes for subscribers can be varied with a finer granularity. This configuration matches that used for terminated PPPoE subscribers.



To configure the PPP attributes for dynamically created si interfaces:

To configure the PPP attributes for dynamically created si interfaces:

1. Specify the predefined dynamic interface and logical interface variables in the dynamic profile.

```
[edit dynamic-profiles profile-name]
user@host# edit interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit"
```

2. Configure the interval between PPP keepalive messages for the L2TP tunnel terminating on the LNS.

```
[edit dynamic-profiles profile-name interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set keepalives interval seconds
```

3. Configure PPP authentication methods that apply to tunneled PPP subscribers at the LNS.

```
[edit dynamic-profiles profile-name interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set ppp-options chap
user@host# set ppp-options pap
```

To configure the PPP attributes for statically created si interfaces:

To configure the PPP attributes for statically created si interfaces:

1. Specify the logical inline service interface.

```
[edit interfaces si-slot/pic/port]
user@host# edit unit logical-unit-number
```

2. Configure the interval between PPP keepalive messages for the L2TP tunnel terminating on the LNS.

```
[edit interfaces si-slot/pic/port unit logical-unit-number]
user@host# set keepalives interval seconds
```

3. Configure the number of keepalive packets a destination must fail to receive before the network takes down a link.

```
[edit interfaces si-slot/pic/port unit logical-unit-number]
user@host# set keepalives down-count number
```



**NOTE:** The **keepalives up-count** option is typically not used for subscriber management.

4. Configure PPP authentication methods that apply to tunneled PPP subscribers at the LNS.

```
[edit interfaces si-slot/pic/port unit logical-unit-number]
user@host# set ppp-options chap
user@host# set ppp-options pap
```



**BEST PRACTICE:** Although all other statements subordinate to `ppp-options`—including those subordinate to `chap` and `pap`—are supported, they are typically not used for subscriber management. We recommend that you leave these other statements at their default values.



**NOTE:** You can also configure PPP attributes with a user group profile that applies the attributes to all subscribers with that profile on a LAC client. See [“Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile” on page 53](#) for more information. When you configure the PPP attributes for L2TP LNS subscribers both on the `si` interface and in user group profiles, the inline service interface configuration takes precedence over the user group profile configuration.

**Related Documentation**

- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)

## Configuring an L2TP Access Profile on the LNS

Access profiles define how to validate Layer 2 Tunneling Protocol (L2TP) connections and session requests. Within each L2TP access profile, you configure one or more clients (LACs). The client characteristics are used to authenticate LACs with matching passwords, and to establish attributes of the client tunnel and session. You can configure multiple access profiles and multiple clients within each profile.

To configure an L2TP access profile:

To configure an L2TP access profile:

1. Create the access profile.

```
[edit access]
user@host# edit profile access-profile-name
```

2. Configure characteristics for one or more clients (LACs).

```
[edit access profile access-profile-name]
user@host# client client-name
```



**NOTE:** Except for the special case of the default client, the LAC client name that you configure in the access profile must match the hostname of the LAC. In the case of a Juniper Networks router acting as the LAC, the hostname is configured in the LAC tunnel profile with the gateway `gateway-name` statement at the `[edit access tunnel-profile profile-name tunnel tunnel-id source-gateway]` hierarchy level. Alternatively, the client name can be returned from RADIUS in the attribute, Tunnel-Client-Auth-Id [90].



**NOTE:** Use `default` as the client name when you want to define a default tunnel client. The default client enables the authentication of multiple LACs with the same secret and L2TP attributes. This behavior is useful when, for example, many new LACs are added to the network, because it enables the LACs to be used without additional LNS profile configuration.

Use `default` only on MX Series routers. The equivalent client name on M Series routers is `*`.

3. (Optional) Specify a local access profile that overrides the global access profile and the tunnel group AAA access profile to configure RADIUS server settings for the client.

```
[edit access profile access-profile-name client client-name]
user@host# set l2tp aaa-access-profile
```

4. Configure the LNS to renegotiate the link control protocol (LCP) with the PPP client tunneled from the client.

```
[edit access profile access-profile-name client client-name]
user@host# set l2tp lcp-renegotiation
```

5. Configure the maximum number of sessions allowed in a tunnel from the client (LAC).

```
[edit access profile access-profile-name client client-name]
user@host# set l2tp maximum-sessions-per-tunnel number
```

6. Configure the tunnel password used to authenticate the client (LAC).

```
[edit access profile access-profile-name client client-name]
user@host# set l2tp shared-secret shared-secret
```

7. (Optional) Associate a group profile containing PPP attributes to apply for the PPP sessions being tunneled from this LAC client.

```
[edit access profile access-profile-name client client-name]
user@host# set user-group-profile group-profile-name
```



**NOTE:** If `<user-group-profile>` is modified or deleted, the existing LNS subscribers, which were using this Layer 2 Tunneling Protocol client configuration, will go down.

#### Related Documentation

- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)
- [Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64](#)

## Configuring a AAA Local Access Profile on the LNS

For some LNS tunnels, you might wish to override the access profile configured at the routing instance that hosts the tunnel with a particular RADIUS server configuration. You can configure a local access profile to do so. You can subsequently use the

**aaa-access-profile** statement to apply the local access profile to a tunnel group or LAC client.

A local access profile applied to a client overrides a local access profile applied to a tunnel group, which in turn overrides the access profile for the routing instance.

To configure a AAA local access profile:

To configure a AAA local access profile:

1. Create the access profile.

```
[edit access]
user@host# edit profile local-aaa-profile-name
```

2. Configure the order of AAA authentication methods.

```
[edit access profile local-aaa-profile-name]
user@host# set authentication-order radius
```

3. Configure the RADIUS server attributes, such as the authentication password.

```
[edit access profile local-aaa-profile-name]
user@host# set radius-server server-address secret password
```

#### Related Documentation

- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)
- [Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64](#)
- [Configuring an L2TP Access Profile on the LNS on page 56](#)

---

## Configuring an Address-Assignment Pool for L2TP LNS with Inline Services

You can configure pools of addresses that can be dynamically assigned to the tunneled PPP subscribers. The pools must be local to the routing instance where the subscriber comes up. The configured pools are supplied in the RADIUS Framed-Pool and Framed-IPv6-Pool attributes. Pools are optional when Framed-IP-Address is sent by RADIUS.

To configure an address-assignment pool, you must specify the name of the pool and configure the addresses for the pool.

You can optionally configure multiple named ranges, or subsets, of addresses within an address-assignment pool. During dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, you specify a name for the range and define the address range.



**NOTE:** Be sure to use the address-assignment pools (**address-assignment**) statement rather than the address pools (**address-pool**) statement.

---

To configure an IPv4 address-assignment pool for L2TP LNS:

To configure an IPv4 address-assignment pool for L2TP LNS:

1. Configure the name of the pool and specify the IPv4 family.

```
[edit access]
user@host# edit address-assignment pool pool-name family inet
```

2. Configure the network address and the prefix length of the addresses in the pool.

```
[edit access address-assignment pool pool-name family inet]
user@host# set network ip-prefix/<prefix-length>
```

3. Configure the name of the range and the lower and upper boundaries of the addresses in the range.

```
[edit access address-assignment pool pool-name family inet]
user@host# set range range-name low lower-limit high upper-limit
```

For example, to configure an IPv4 address-assignment pool:

```
[edit access]
user@host# edit address-assignment pool lns-v4-pool family inet
[edit access address-assignment pool lns-v4-pool family inet]
user@host# set network 192.168.1.1/16
[edit access address-assignment pool lns-v4-pool family inet]
user@host# set range lns-v4-pool-range low 192.168.1.1 high 192.168.255.255
```



**NOTE:** Dual-stack (IPv4/IPv6) LNS is supported, but IPv6-only subscribers are not supported.

To configure an IPv6 address-assignment pool for L2TP LNS:

To configure an IPv6 address-assignment pool for L2TP LNS:

1. Configure the name of the pool and specify the IPv6 family.

```
[edit access]
user@host# edit address-assignment pool pool-name family inet6
```

2. Configure the IPv6 network prefix for the address pool. The prefix specification is required when you configure an IPv6 address-assignment pool.

```
[edit access address-assignment pool pool-name family inet6]
user@host# set prefix ipv6-prefix
```

3. Configure the name of the range and define the range. You can define the range based on the lower and upper boundaries of the prefixes in the range, or based on the length of the prefixes in the range.

```
[edit access address-assignment pool pool-name family inet6]
user@host# set range range-name low lower-limit high upper-limit
```

For example, to configure an IPv6 address-assignment pool:

```
[edit access]
```

```

user@host# edit address-assignment pool lns-v6-pool family inet6
[edit access address-assignment pool lns-v6-pool family inet6]
user@host# set prefix 2010:DB8::/32
[edit access address-assignment pool lns-v6-pool family inet6]
user@host# set range lns-v6-pool-range low 2010:DB8:1::/48 high 2010:DB8::ffff::/48

```

**Related  
Documentation**

- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)
- [Address-Assignment Pools Overview](#)
- [Configuring Address-Assignment Pools](#)

## Configuring the L2TP LNS Peer Interface

The peer interface connects the LNS to the cloud towards the LACs so that IP packets can be exchanged between the tunnel endpoints. MPLS and aggregated Ethernet can also be used to reach the LACs.



**NOTE:** On MX Series routers, you must configure the peer interface on an MPC.

To configure the LNS peer interface:

To configure the LNS peer interface:

1. Specify the interface name.

```

[edit interfaces]
user@host# edit interface-name

```

2. Enable VLANs.

```

[edit interfaces interface-name]
user@host# set vlan-tagging

```

3. Specify the logical interface, bind a VLAN tag ID to the interface, and configure the address family and the IP address for the logical interface.

```

[edit interfaces interface-name]
user@host# edit unit logical-unit-number
[edit interfaces interface-name unit logical-unit-number]
user@host# set vlan-id number
user@host# set family family address ip-address

```



**NOTE:** The IPv6 address family is not supported as a tunnel endpoint.

**Related  
Documentation**

- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)

## Enabling Inline Service Interfaces

The inline service interface is a virtual physical interface that resides on the Packet Forwarding Engine. This **si** interface, referred to as an *anchor* interface, makes it possible to provide L2TP services without a special services PIC. The inline service interface is supported only by MPCs on MX Series routers. Four inline service interfaces are configurable per MPC-occupied chassis slot.



**NOTE:** On MX80 routers, you can configure only four inline services physical interfaces as anchor interfaces for L2TP LNS sessions: si-1/0/0, si-1/1/0, si-1/2/0, and si-1/3/0. You cannot configure si-0/0/0 for this purpose on MX80 routers.

To enable inline service interfaces:

To enable inline service interfaces:

1. Access an MPC-occupied slot and the PIC where the interface is to be enabled.

```
[edit chassis]
user@host# edit fpc slot-number pic number
```

2. Enable the interface and specify the amount of bandwidth reserved on each Packet Forwarding Engine for tunnel traffic using inline services.

```
[edit chassis fpc slot-number pic number]
user@host# set inline-services bandwidth (1g | 10g)
```

### Related Documentation

- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)

## Configuring IP Inline Reassembly for L2TP

This procedure shows how to configure a service interface on a LAC or LNS to reassemble fragmented IP packets. This example creates a service set that configures the IP reassembly parameters for L2TP fragments. The service set is then associated with the L2TP service.

Before you configure inline IP reassembly, be sure you have:

Before you configure inline IP reassembly, be sure you have:

- Configured L2TP.
- Configured a valid service interface on the LAC or LNS.

To configure inline IP reassembly:

To configure inline IP reassembly:

1. Configure the chassis-level bandwidth used by the inline services interface on the FPC and PIC slot for inline IP fragment reassembly.

```
[edit chassis]
user@host# set fpc 2 pic 1 inline-services bandwidth 10g
```

2. Configure the interface-level logical unit used by the inline services (si-) interface on the FPC and PIC slot for inline IP fragment reassembly.

```
[edit interfaces]
user@host# set si-2/1/0 unit 0 family inet
user@host# set si-2/1/0 unit 0 service-domain inside
```



**NOTE:** This configuration is not unique to L2TP. However, you must configure the family (inet) and service domain (inside) as shown.

3. Configure the service set (**set1**) for IP reassembly in the input match direction. (The **local** option loops the reassembled packets back to the local interface.)

```
[edit services]
user@host# set service-set set1
```

```
[edit services service set ip-reassembly-set]
user@host# set ip-reassembly-rules ipr_rule1
user@host# set next-hop-service inside-service-interface si-9/1/0.0
user@host# set next-hop-service outside-service-interface-type local
```



**NOTE:** You must configure both inside (si- interface) and outside type (local) service interfaces statements. The reassembly rule is not formulated outside of the service set; this statement simply initiates the reassembly process.

4. Configure the IP reassembly rule parameter

```
[edit services ip-reassembly]
user@host# set rule ipr_rule1 match-direction input;
```

5. Configure the service set (**set1**) for IP reassembly to bind to the L2TP service.



**NOTE:**

- The service set must be defined at the [edit services] hierarchy level.
- You cannot delete a service set instance if it is associated with an L2TP service.

```
[edit services l2tp]
user@host# set ip-reassembly service-set set1
```



- Related Documentation**
- [IP Packet Fragment Reassembly for L2TP Overview on page 26](#)
  - [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)
  - *Protocols and Applications Supported by MX240, MX480, MX960, MX2010, and MX2020 Enhanced MPCs (MPCEs)*

---

## Configuring an Inline Service Interface for L2TP LNS

---

The inline service interface is a virtual physical service interface that resides on the Packet Forwarding Engine. This `si` interface, referred to as an *anchor* interface, makes it possible to provide L2TP services without a special services PIC. The inline service interface is supported only by MPCs on MX Series routers. Four inline service interfaces are configurable per MPC-occupied chassis slot.

You can maximize the number of sessions that can be shaped in one service interface by setting the maximum number of hierarchy levels to two. In this case, each LNS session consumes one L3 node in the scheduler hierarchy for shaping.

If you do not specify the number of levels (two is the only option), then the number of LNS sessions that can be shaped on the service interface is limited to the number of L2 nodes, or 4096 sessions. Additional sessions still come up, but they are not shaped.

To configure an inline service interface:

To configure an inline service interface:

1. Access the service interface.

```
[edit interfaces]
user@host# edit si-slot/pic/port
```

2. (Optional; for per-session shaping only) Enable the inline service interface for hierarchical schedulers and limit the number of scheduler levels to two.

```
[edit interfaces si-slot/pic/port]
user@host# set hierarchical-scheduler maximum-hierarchy-levels 2
```

3. (Optional; for per-session shaping only) Configure services encapsulation for inline service interface.

```
[edit interfaces si-slot/pic/port]
user@host# set encapsulation generic-services
```

4. Configure the IPv4 family on the reserved unit 0 logical interface.

```
[edit interfaces si-slot/pic/port]
user@host# set unit 0 family inet
```

- Related Documentation**
- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)

## Configuring Options for the LNS Inline Services Logical Interface

---

You must specify characteristics—**dial-options**—for each of the inline services logical interfaces that you configure for the LNS. LNS on MX Series routers supports only one session per logical interface, so you must configure it as a **dedicated** interface; the **shared** option is not supported. (LNS on M Series routers supports **dedicated** and **shared** options.) You also configure an identifying name for the logical interface that matches the name you specify in the access profile.

You must specify the **inet** address family for each static logical interface. Although the CLI accepts either **inet** or **inet6** for static logical interfaces, the subscriber cannot log in successfully unless the address family is **inet** is configured.

To configure the logical interface options:

To configure the logical interface options:

1. Access the inline services logical interface.

```
[edit]
user@host# edit interfaces si-fpc/pic/port unit logical-unit-number
```

2. Specify an identifier for the logical interface.

```
[edit interfaces si-fpc/pic/port unit logical-unit-number]
user@host# set dial-options l2tp-interface-id name
```

3. Configure the logical interface to be used for only one session at a time.

```
[edit interfaces si-fpc/pic/port unit logical-unit-number]
user@host# set dial-options dedicated
```

4. Configure the address family for each logical interface and enable the local address on the LNS that provides local termination for the L2TP tunnel to be derived from the specified interface name.

```
[edit interfaces si-fpc/pic/port unit logical-unit-number]
user@host# set family inet unnumbered-address lo0.0
```

### Related Documentation

- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)
- [Configuring an L2TP Access Profile on the LNS on page 56](#)

## Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces

---

The L2TP tunnel group specifies attributes that apply to L2TP tunnels and sessions from a group of LAC clients. These attributes include the access profile used to validate L2TP connection requests made to the LNS on the local gateway address, a local access profile that overrides the global access profile, the keepalive timer, and whether the IP ToS value is reflected.



**NOTE:** If you delete a tunnel group, all L2TP sessions in that tunnel group are terminated. If you change the value of the `local-gateway-address`, `service-device-pool`, or `service-interface` statements, all L2TP sessions using those settings are terminated. If you change or delete other statements at the `[edit services l2tp tunnel-group name]` hierarchy level, new tunnels you establish use the updated values but existing tunnels and sessions are not affected.

To configure the LNS tunnel group:

To configure the LNS tunnel group:

1. Create the tunnel group.

```
[edit services l2tp]
user@host# edit tunnel-group name
```

2. Specify the service anchor interface responsible for L2TP processing on the LNS.

```
[edit services l2tp tunnel-group name]
user@host# set service-interface interface-name
```

This service anchor interface is required for static LNS sessions, and for dynamic LNS sessions that do not balance traffic across a pool of anchor interfaces. The interface is configured at the `[edit interfaces]` hierarchy level.

3. (Optional; for load-balancing dynamic LNS sessions only) Specify a pool of inline service anchor interfaces to enable load-balancing of L2TP traffic across the interfaces.

```
[edit services l2tp tunnel-group name]
user@host# set service-device-pool pool-name
```

The pool is defined at the `[edit services service-device-pools]` hierarchy level.

4. (For dynamic LNS sessions only) Specify the name of the dynamic profile that defines and instantiates inline service interfaces for L2TP tunnels

```
[edit services l2tp tunnel-group name]
user@host# set dynamic-profile profile-name
```

The profile is defined at the `[edit dynamic-profiles]` hierarchy level.

5. Specify the access profile that validates all L2TP connection requests to the local gateway address.

```
[edit services l2tp tunnel-group name]
user@host# set l2tp-access-profile profile-name
```

6. Configure the local gateway address on the LNS; corresponds to the IP address that is used by LACs to identify the LNS.

```
[edit services l2tp tunnel-group name]
user@host# set local-gateway address address
```

7. (Optional) Configure the local gateway name on the LNS, returned in the SCCRP message to the LAC. The name must match the remote gateway name configured on the LAC, or the tunnel cannot be created.

```
[edit services l2tp tunnel-group name]  
user@host# set local-gateway gateway-name gateway-name
```

8. (Optional) Configure the interval at which the LNS sends hello messages if it has received no messages from the LAC.

```
[edit services l2tp tunnel-group name]  
user@host# set hello-interval seconds
```

9. (Optional) Specify a local access profile that overrides the global access profile to configure RADIUS server settings for the tunnel group.

```
[edit services l2tp tunnel-group name]  
user@host# set aaa-access-profile profile-name
```

This local profile is configured at the **[edit access profile]** hierarchy level.

10. (Optional) Configure the LNS to reflect the IP ToS value from the inner IP header to the outer IP header (applies to CoS configurations).

```
[edit services l2tp tunnel-group name]  
user@host# set tos-reflect
```

**Related  
Documentation**

- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)
- [Configuring an L2TP Access Profile on the LNS on page 56](#)

---

## Configuring a Pool of Inline Services Interfaces for Dynamic LNS Sessions

---

You can create a pool of inline service interfaces, also known as a *service device pool*, to enable load-balancing of L2TP traffic across the interfaces. The pool is supported for dynamic LNS configurations, where it provides a set of logical interfaces that can be dynamically created and allocated to L2TP sessions on the LNS. The pool is assigned to an LNS tunnel group. L2TP maintains the state of each inline service interface and uses a round-robin method to evenly distribute the load among available interfaces when new session requests are accepted.



**NOTE:** Load balancing is available only for dynamically created subscriber interfaces.

LNS sessions anchored on an MPC are not affected by a MIC failure as long as some other path to the peer LACs exists. If the MPC hosting the peer interface fails and there is no path to peer LACs, the failure initiates termination and clean-up of all the sessions on the MPC.

If the MPC anchoring the LNS sessions itself fails, the Routing Engine does not relocate sessions to another slot and all sessions are terminated immediately. New sessions can come up on another available interface when the client retries.

To configure the service device pool:

To configure the service device pool:

1. Create the pool.

```
[edit services service-device-pools]
user@host# edit pool pool-name
```

2. Specify the inline service interfaces that make up the pool.

```
[edit services service-device-pools pool pool-name]
user@host# set interface service-interface-name
user@host# set interface service-interface-name
```

#### Related Documentation

- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)
- [Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64](#)

## Configuring a Dynamic Profile for Dynamic LNS Sessions

You can configure L2TP to dynamically assign inline service interfaces for L2TP tunnels. You must define one or more dynamic profiles and assign a profile to each tunnel group. Both IPv4-only and dual-stack IPv4/IPv6 interfaces are supported.

To configure the L2TP dynamic profile:

To configure the L2TP dynamic profile:

1. Create the dynamic profile.

```
[edit]
user@host# edit dynamic-profiles profile-name
```

2. Configure the interface to be dynamically assigned to the routing instance used by the tunneled PPP clients.

```
[edit dynamic-profiles profile-name routing-instances "$junos-routing-instance"]
user@host# set interface $junos-interface-name
```

3. Configure the routing options for access routes in the routing instance.

```
[edit dynamic-profiles profile-name routing-instances "$junos-routing-instance"
routing-options access]
user@host# set route next-hop $junos-framed-route-nexthop
user@host# set route metric $junos-framed-route-cost
user@host# set route preference $junos-framed-route-distance
```

4. Configure the routing options for access-internal routes in the routing instance.

```
[edit dynamic-profiles profile-name routing-instances "$junos-routing-instance"
routing-options access-internal]
user@host# set route $junos-subscriber-ip-address
```

5. Define the interfaces used by the dynamic profile. The variable is dynamically replaced by one of the configured inline service interfaces.

```
[edit dynamic-profiles profile-name]  
user@host# set interfaces $junos-interface-ifd-name
```

6. Configure the inline services logical interfaces to be dynamically instantiated.

```
[edit dynamic-profiles profile-name interfaces "$junos-interface-ifd-name"]  
user@host# set unit $junos-interface-unit
```

7. Specify an identifier for the logical interfaces.

```
[edit dynamic-profiles profile-name interfaces "$junos-interface-ifd-name" unit  
"$junos-interface-unit"]  
user@host# set dial-options l2tp-interface-id name
```

8. Configure each logical interface to be used for only one session at a time.

```
[edit dynamic-profiles profile-name interfaces "$junos-interface-ifd-name" unit  
"$junos-interface-unit"]  
user@host# set dial-options dedicated
```

9. Configure **family inet** as the address family for the logical interfaces and enable the local address on the LNS that provides local termination for the L2TP tunnel to be derived from the specified interface name.



**NOTE:** For dynamic interfaces, you must specify the inet address family when you configure dial-options. If you configure an IPv6-only LNS stack, you can omit only the address portion of the inet address family configuration.

```
[edit dynamic-profiles profile-name interfaces "$junos-interface-ifd-name" unit  
"$junos-interface-unit"]  
user@host# set family inet unnumbered-address $junos-loopback-interface
```

**Related  
Documentation**

- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)
- [Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64](#)

## Configuring the L2TP Destination Lockout Timeout

When multiple sets of tunneling parameters are available, L2TP uses a selection process to choose the best tunnel for subscriber traffic. As part of this selection process, L2TP locks out destinations it cannot connect to when a subscriber tries to reach a domain. L2TP places the destination on the destination lockout list and excludes the destination from consideration for a configurable period called the *destination lockout timeout*.

By default, the destination lockout timeout is 300 seconds (5 minutes). You can configure a value from 60 through 3600 seconds (1 minute through 1 hour). When the lockout timeout expires, L2TP assumes that the destination is now available and includes the destination when performing the tunnel selection process. The destination lockout period is a global value and is not individually configurable for particular destinations, tunnels, or tunnel groups.



**BEST PRACTICE:** Configure the lockout timeout to be equal to or shorter than the destruct timeout. Otherwise, the destruct timeout expires before the lockout timeout. In this event, the locked-out destination is destroyed and can be subsequently returned to service before the lockout timeout expires, thus negating the effectiveness of the lockout timeout.

To configure the destination lockout timeout:

To configure the destination lockout timeout:

- Specify the period in seconds.

```
[edit services l2tp destination]
user@host# set lockout-timeout seconds
```

The **show services l2tp destination lockout** command displays the destination lockout list and for each destination indicates how much time remains before its timeout expires. The **show services l2tp destination detail** command indicates for each destination whether it is locked and waiting for the timeout to expire or not locked.

### Related Documentation

- [LAC Tunnel Selection Overview on page 19](#)
- [Setting the L2TP Destruct Timeout on page 76](#)
- [Removing an L2TP Destination from the Destination Lockout List on page 69](#)
- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)

## Removing an L2TP Destination from the Destination Lockout List

When a PPP subscriber tries to log in to a domain, L2TP selects a tunnel associated with a destination in that domain and attempts to access the destination. If the connection attempt fails, L2TP places the destination on the destination lockout list. Destinations

on this list are excluded from being considered for subsequent connections for a configurable period called the *destination lockout timeout*.

You can issue the **request services l2tp destination unlock** command for a particular destination to remove it from the destination lockout list. The result is that this destination is immediately available for consideration when a subscriber logs in to the associated domain.

To remove a destination from the destination lockout list:

To remove a destination from the destination lockout list:

- Specify the name of the destination to be unlocked.

```
user@host> request services l2tp destination unlock destination-name
```

**Related  
Documentation**

- [LAC Tunnel Selection Overview on page 19](#)
- [Configuring the L2TP Destination Lockout Timeout on page 69](#)

---

## Configuring L2TP Tunnel Switching

L2TP tunnel switching enables a router configured as an LTS to forward PPP packets carried on one L2TP session to a second L2TP session terminated on a different LNS. To configure L2TP tunnel switching, you must define a tunnel switch profile and then assign that profile.

To define an L2TP tunnel switch profile:

To define an L2TP tunnel switch profile:

1. Create the profile.

```
[edit access]  
user@host# edit tunnel-switch-profile profile-name
```

2. (Optional) Override the default actions taken for certain L2TP AVPs at the switching boundary.

```
[edit access tunnel-switch-profile profile-name]  
user@host# set avp bearer-type action  
user@host# set avp calling-number action  
user@host# set avp cisco-nas-port-info action
```

3. Specify the tunnel profile that defines the tunnel to which the subscriber traffic is switched.

```
[edit access tunnel-switch-profile profile-name]  
user@host# set tunnel-profile profile-name
```

4. (Optional) Apply the profile as a global default profile to switch packets from all incoming sessions from the LAC.

```
[edit services l2tp]  
user@host1# set tunnel-switch-profile profile-name
```



5. (Optional) Apply the profile as part of a tunnel group to switch packets from all sessions in the tunnel group.

```
[edit services l2tp tunnel-group name]
user@host1# set tunnel-switch-profile profile-name
```



**NOTE:** The tunnel group is part of the LTS configuration that enables it to act as the LNS for the original sessions from the LAC.

A tunnel group with a tunnel switch profile must also contain a dynamic profile, because tunnel switching supports only dynamic subscribers.

6. (Optional) Apply the profile as part of a domain map to switch packets from all sessions that are associated with the domain.

```
[edit access domain map domain-map-name]
user@host1# set tunnel-switch-profile profile-name
```



**NOTE:** A domain map cannot have both a tunnel switch profile and a tunnel profile. You must remove one if you add the other.

7. (Optional) Apply the profile by means of the Tunnel-Switch-Profile VSA [26–91] in the RADIUS Access-Accept message returned when the session from the LAC is authenticated. Refer to the documentation for your RADIUS server to determine how to configure this method.

For example, consider the following configuration:

```
[edit access tunnel-switch-profile l2tp-tunnel-switch-profile]
user@host# set avp bearer-type regenerate
user@host# set avp calling-number regenerate
user@host# set avp cisco-nas-port-info drop
user@host# set tunnel-profile l2tp-tunnel-profile1
```

```
[edit access tunnel-switch-profile lts-profile-groupA]
user@host# set tunnel-profile l2tp-tunnel-profile2
[edit access tunnel-switch-profile lts-profile-example.com]
user@host# set tunnel-profile l2tp-tunnel-profile3
```

```
[edit services l2tp]
user@host1# set tunnel-switch-profile l2tp-tunnel-switch-profile
user@host1# set tunnel-group groupA tunnel-switch-profile lts-profile-groupA
```

```
[edit access domain]
user@host1# set map example.com tunnel-switch-profile lts-profile-example.com
```

This configuration creates three tunnel switch profiles, l2tp-tunnel-switch-profile, lts-profile-groupA, and lts-profile-example-com.

The profile l2tp-tunnel-switch-profile is applied as the global default. When packets are switched according to this profile, the values for the Bearer Type AVP (18) and Calling

Number AVP (22) in the L2TP packets are regenerated based on local policy at the L2TP tunnel switch and then sent with the packets. The Cisco NAS Port Info AVP (100) is simply dropped. Finally, l2tp-tunnel-profile1 provides the configuration characteristics of the tunnel to which the traffic is switched.

Tunnel switch profile lts-profile-groupA is applied by means of a tunnel group, groupA; it specifies a different tunnel profile, l2tp-tunnel-profile2 and it does not override any AVP actions. Tunnel switch profile lts-profile-example.com is applied by means of a domain map for the example.com domain; it specifies a different tunnel profile, l2tp-tunnel-profile3 and it does not override any AVP actions.

- Related Documentation**
- [L2TP Tunnel Switching Overview on page 11](#)
  - [Tunnel Switching Actions for L2TP AVPs at the Switching Boundary on page 15](#)

## CHAPTER 6

# Configuration Tasks for Both LAC and LNS

- [Configuring Retransmission Attributes for L2TP Control Messages on page 73](#)
- [Setting the L2TP Tunnel Idle Timeout on page 75](#)
- [Setting the L2TP Receive Window Size on page 76](#)
- [Setting the L2TP Destruct Timeout on page 76](#)
- [Enabling Tunnel and Global Counters for SNMP Statistics Collection on page 77](#)

### Configuring Retransmission Attributes for L2TP Control Messages

---

You can control the retransmission of unacknowledged L2TP control messages by configuring how many times the local peer retransmits the message and how long it waits for a response before retransmission.

L2TP peers maintain a queue of control messages that must be sent to the peer device. After the local peer (LAC or LNS) sends a message, it waits for a response from the remote peer. If a response is not received within the minimum retransmission interval, the local peer retransmits the message and waits for double the retransmission interval. Each time it retransmits the message, the peer doubles how long it waits, up to a maximum of 16 seconds.

If no response is received, the local peer continues to send the message until the number of retransmissions matches the retransmission count. In this case, retransmissions stop and the tunnel and all its sessions are cleared.



**BEST PRACTICE:** Before you downgrade to a Junos OS release that does not support these statements, we recommend that you explicitly unconfigure the feature by including the `no retransmission-count-established` statement and the `no retransmission-count-non-established` statement at the `[edit services l2tp tunnel]` hierarchy level.



**BEST PRACTICE:** During a unified in-service software upgrade (unified ISSU) on an MX Series router configured as the LAC, the LAC does not respond to control messages from the LNS. This can result in dropping LAC L2TP

sessions. You can avoid this situation by ensuring that the maximum retransmission count on the LNS is set to 16 or higher.

.....  
To set the maximum retransmission count for established tunnels:

To set the maximum retransmission count for established tunnels:

- Configure the count.

```
[edit services l2tp tunnel]
user@host# set retransmission-count-established count
```

To set the maximum retransmission count for non-established tunnels:

To set the maximum retransmission count for non-established tunnels:

- Configure the count.

```
[edit services l2tp tunnel]
user@host# set retransmission-count-not-established count
```

To set the minimum interval between retransmissions:

To set the minimum interval between retransmissions:

- Configure the interval.

```
[edit services l2tp tunnel]
user@host# set minimum-retransmission-timeout seconds
```

For example, the following configuration specifies that established tunnels have a maximum retransmission count of three and a minimum retransmission interval of two seconds:

```
[edit services l2tp tunnel]
user@host# set retransmission-count-established 3
user@host# set minimum-retransmission-timeout 2
```

With this sample configuration, the following sequence applies to each control message sent by the LAC or LNS:

With this sample configuration, the following sequence applies to each control message sent by the LAC or LNS:

1. The local peer sends the control message and waits for a response from the remote peer.
2. If the response is not received within the minimum interval of 2 seconds, the local peer retransmits the message. This is the first retransmission.
3. If the response is not received within 4 seconds, the local peer retransmits the message. This is the second retransmission.

4. If the response is not received within 8 seconds, the local peer retransmits the message. This is the third and final retransmission, because the maximum count has been reached.
5. If the response is not received within 16 seconds, the tunnel and all its sessions are cleared.

**Related  
Documentation**

- [Retransmission of L2TP Control Messages on page 8](#)
- [Configuring an L2TP LAC on page 35](#)
- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)

## Setting the L2TP Tunnel Idle Timeout

You can configure the LAC or the LNS to specify how long a tunnel without any sessions remains active. The idle timer starts when the last session on the tunnel is terminated. When the timer expires the tunnel is disconnected. This idle timeout frees up resources otherwise consumed by inactive tunnels.

If you set the idle timeout value to zero, the tunnel is forced to remain active indefinitely after the last session is terminated until one of the following occurs:

If you set the idle timeout value to zero, the tunnel is forced to remain active indefinitely after the last session is terminated until one of the following occurs:

- You issue the **clear services l2tp tunnel** command.
- The remote peer disconnects the tunnel.



**BEST PRACTICE:** Before you downgrade to a Junos OS Release that does not support this statement, we recommend that you explicitly unconfigure the feature by including the `no idle-timeout` statement at the `[edit services l2tp tunnel]` hierarchy level.

To set the tunnel idle timeout:

To set the tunnel idle timeout:

- Configure the timeout period.

```
[edit services l2tp tunnel]
user@host# set idle-timeout seconds
```

**Related  
Documentation**

- [Configuring an L2TP LAC on page 35](#)
- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)

## Setting the L2TP Receive Window Size

---

You can configure the L2TP receive window size for an L2TP tunnel. The receive window size specifies the number of packets a peer can send before waiting for an acknowledgment from the router.

By default, the receive window size is set to four packets. If the receive window size is set to its default value, the router does not send the Receive Window Size AVP, AVP 10, in its first packet sent during tunnel negotiation to its peer.

To configure the receive window size:

```
[edit services l2tp tunnel]
user@host# set rx-window-size packets
```

To configure the receive window size:

```
[edit services l2tp tunnel]
user@host# set rx-window-size packets
```

### Related Documentation

- [Configuring an L2TP LAC on page 35](#)
- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)

## Setting the L2TP Destruct Timeout

---

You can configure the LAC or the LNS to specify how long the router attempts to maintain dynamic destinations, tunnels, and sessions after they have been destroyed. This destruct timeout aids debugging and other analysis by saving underlying memory structures after the destination, tunnel, or session is terminated. Any specific dynamic destination, tunnel, or session may not be maintained for this entire time period if the resources must be reclaimed early to allow new tunnels to be established.



**BEST PRACTICE:** Before you downgrade to a Junos OS Release that does not support this statement, we recommend that you explicitly unconfigure the feature by including the `no destruct-timeout` statement at the `[edit services l2tp]` hierarchy level.

To set the L2TP destruct timeout:

To set the L2TP destruct timeout:

- Configure the timeout period.

```
[edit services l2tp]
user@host# set destruct-timeout seconds
```

### Related Documentation

- [Configuring an L2TP LAC on page 35](#)
- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)

## Enabling Tunnel and Global Counters for SNMP Statistics Collection

By default, SNMP polling is disabled for L2TP statistics. As a consequence, the L2TP tunnel and global counters listed in [Table 9 on page 77](#) have a default value of zero.

**Table 9: SNMP Counters for L2TP Statistics**

Counter Name	Type
jnxL2tpTunnelStatsDataTxPkts	Tunnel
jnxL2tpTunnelStatsDataRxPkts	Tunnel
jnxL2tpTunnelStatsDataTxBytes	tunnel
jnxL2tpTunnelStatsDataRxBytes	Tunnel
jnxL2tpStatsPayloadRxOctets	Global
jnxL2tpStatsPayloadRxPkts	Global
jnxL2tpStatsPayloadTxOctets	Global
jnxL2tpStatsPayloadTxPkts	Global

You can enable collection of these statistics by including the **enable-snmp-tunnel-statistics** statement at the **[edit services l2tp]** hierarchy level. When enabled, the L2TP process polls for these statistics every 30 seconds for 1000 sessions. The potential age of the statistics increases with the number of subscriber sessions; the data is refreshed more quickly as the number of sessions decreases. For example, with 60,000 sessions, none of these statistics can be more than 30 minutes old.



**BEST PRACTICE:** The system load can increase when you enable these counters and also use RADIUS interim accounting updates. We recommend you enable these counters when you are using only SNMP statistics.

To enable L2TP statistics collection for SNMP:

To enable L2TP statistics collection for SNMP:

- Enable statistics collection.

**[edit services l2tp]**

user@host1# **set enable-snmp-tunnel-statistics**

### Related Documentation

- [Configuring an L2TP LAC on page 35](#)
- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)





# Example

- [Example: Configuring an L2TP LNS on page 79](#)

## Example: Configuring an L2TP LNS

This example shows how you can configure an L2TP LNS on an MX Series router to provide tunnel endpoints for an L2TP LAC in your network. This configuration includes a dynamic profile for dual-stack subscribers.

- [Requirements on page 79](#)
- [Overview on page 80](#)
- [Configuration on page 82](#)

## Requirements

L2TP LNS requires the following hardware and software:

L2TP LNS requires the following hardware and software:

- MX Series 3D Universal Edge Router
- One or more MPCs
- Junos OS Release 11.4 or later

No special configuration beyond device initialization is required before you can configure this feature.

You must configure certain standard RADIUS attributes and Juniper Networks VSAs in the attribute return list on the AAA server associated with the LNS for this example to work. [Table 10 on page 79](#) lists the attributes with their required order setting and values. We recommend that you use the most current Juniper Networks RADIUS dictionary, available in the *Downloads* box on the *Junos OS Subscriber Management* page for the current release at [http://www.juniper.net/techpubs/en\\_US/junos/information-products/pathway-pages/subscriber-access/index.html](http://www.juniper.net/techpubs/en_US/junos/information-products/pathway-pages/subscriber-access/index.html).

Table 10: VSA and Standard RADIUS Attribute Names, Order, and Values Required for Example

VSA Name [Number]	Order	Value
CoS-Parameter-Type [26–108]	1	T01 Multiplay

Table 10: VSA and Standard RADIUS Attribute Names, Order, and Values Required for Example (*continued*)

VSA Name [Number]	Order	Value
CoS-Parameter-Type [26-108]	2	T02 10m
CoS-Parameter-Type [26-108]	3	T08 -36
CoS-Parameter-Type [26-108]	4	T07 cell-mode
Framed-IPv6-Pool [100]	0	jnpr_ipv6_pool
Framed-Pool [88]	0	jnpr_pool
Egress-Policy-Name [26-11]	0	classify
Ingress-Policy-Name [26-10]	0	classify
Virtual-Router [26-1]	0	default

## Overview

The LNS employs user group profiles to apply PPP attributes to the PPP subscribers that are tunneled from the LAC. LACs in the network are clients of the LNS. The clients are associated with user group profiles in the L2TP access profile configured on the LNS. In this example, the user group profile **ce-l2tp-group-profile** specifies the following PPP attributes:

The LNS employs user group profiles to apply PPP attributes to the PPP subscribers that are tunneled from the LAC. LACs in the network are clients of the LNS. The clients are associated with user group profiles in the L2TP access profile configured on the LNS. In this example, the user group profile **ce-l2tp-group-profile** specifies the following PPP attributes:

- A 30-second interval between PPP keepalive messages for L2TP tunnels from the client LAC terminating on the LNS.
- A 200-second interval that defines how long the PPP subscriber session can be idle before it is considered to have timed out.
- Both PAP and CHAP as the PPP authentication methods that apply to tunneled PPP subscribers at the LNS.

The L2TP access profile **ce-l2tp-profile** defines a set of L2TP parameters for each client LAC. In this example, the user group profile **ce-l2tp-group-profile** is associated with both clients, **lac1** and **lac2**. Both clients are configured to have the LNS renegotiate the link control protocol (LCP) with the PPP client rather than accepting the pre-negotiated LCP parameters that the LACs pass to the LNS. LCP renegotiation also causes authentication to be renegotiated by the LNS; the authentication method is specified in the user group profile. The maximum number of sessions allowed per tunnel is set to 1000 for **lac1** and to 4000 for **lac2**. A different password is configured for each LAC.

A local AAA access profile, **aaa-profile**, enables you to override the global AAA access profile, so that you can specify an authentication order, a RADIUS server that you want to use for L2TP, and a password for the server.

In this example, an address pool defines a range of IP addresses that the LNS allocates to the tunneled PPP sessions. This example defines ranges of IPv4 and IPv6 addresses.

Two inline service interfaces are enabled on the MPC located in slot 5 of the router. For each interface, 10 Gbps of bandwidth is reserved for tunnel traffic on the interface's associated PFE. These *anchor* interfaces serve as the underlying physical interface. To enable CoS queue support on the individual logical inline service interfaces, you must configure both services encapsulation (**generic-services**) and hierarchical scheduling support on the anchors. The IPv4 address family is configured for both anchor interfaces. Both anchor interfaces are specified in the **lns\_p1** service device pool. The LNS can balance traffic loads across the two anchor interfaces when the tunnel group includes the pool.

This example uses the dynamic profile **dyn-lns-profile2** to specify characteristics of the L2TP sessions that are created or assigned dynamically when a subscriber is tunneled to the LNS. For many of the characteristics, a predefined variable is set; the variables are dynamically replaced with the appropriate values when a subscriber is tunneled to the LNS.

The interface to which the tunneled PPP client connects (**\$junos-interface-name**) is dynamically created in the routing instance (**\$junos-routing-instance**) assigned to the subscriber. Routing options for access routes include the route's next hop address (**\$junos-framed-route-nexthop**), metric (**\$junos-framed-route-cost**), and preference (**\$junos-framed-route-distance**). For access-internal routes, a dynamic IP address variable (**\$junos-subscriber-ip-address**) is set.

The logical inline service interfaces are defined by the name of a configured anchor interface (**\$junos-interface-ifd-name**) and a logical unit number (**\$junos-interface-unit**). The profile assigns **l2tp-encapsulation** as the identifier for the logical interface and specifies that each interface can be used for only a single session at a time.

The IPv4 address is set to a value returned from the AAA server. For IPv4 traffic an input firewall filter **\$junos-input-filter** and an output firewall filter **\$junos-output-filter** are attached to the interface. The loopback variable (**\$junos-loopback-interface**) derives an IP address from a loopback interface (**lo**) configured in the routing instance and uses it in IPCP negotiation as the PPP server address. Because this is a dual-stack configuration, the IPv6 address family is also set, with the addresses provided by the **\$junos-ipv6-address** variable.

The **\$junos-ipv6-address** variable is used because Router Advertisement Protocol is also configured. This variable enables AAA to allocate the first address in the prefix to be reserved as the local address for the interface. The minimal configuration for the Router Advertisement Protocol in the dynamic profile specifies the **\$junos-interface-name** and **\$junos-ipv6-ndra-prefix** variables to dynamically assign a prefix value in IPv6 neighbor discovery router advertisements.

The dynamic profile also includes the class of service configuration that is applied to the tunnel traffic. The traffic-control profile (**tc-profile**) includes variables for the scheduler

map (`$junos-cos-scheduler-map`), shaping rate (`$junos-cos-shaping-rate`), overhead accounting (`$junos-cos-shaping-mode`), and byte adjustment `$junos-cos-byte-adjust`). The dynamic profile applies the CoS configuration—including the forwarding class, the output traffic-control profile, and the rewrite rules—to the dynamic service interfaces.

The **tg-dynamic** tunnel group configuration specifies the access profile **ce-l2tp-profile**, the local AAA profile **aaa-profile**, and the dynamic profile **dyn-lns-profile2** that are used to dynamically create LNS sessions and define the characteristics of the sessions. The **lns\_p1** service device pool associates a pool of service interfaces with the group to enable LNS to balance traffic across the interfaces. The local gateway address **10.1.1.2** corresponds to the remote gateway address that is configured on the LAC. The local gateway name **ce-lns** corresponds to the remote gateway name that is configured on the LAC.



**NOTE:** This example does not show all possible configuration choices.

## Configuration

### CLI Quick Configuration

To quickly configure an L2TP LNS, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
[edit]
edit access group-profile ce-l2tp-group-profile
set ppp idle-timeout 200
set ppp ppp-options pap
set ppp ppp-options chap
set ppp keepalive 30
top
edit access profile ce-l2tp-profile
set client lac1 l2tp maximum-sessions-per-tunnel 1000
set client lac1 l2tp interface-id l2tp-encapsulation-1
set client lac1 l2tp lcp-renegotiation
set client lac1 l2tp shared-secret "lac1-secret"
set client lac1 user-group-profile ce-l2tp-group-profile
set client lac2 l2tp maximum-sessions-per-tunnel 4000
set client lac2 l2tp interface-id l2tp-encap-2
set client lac2 l2tp lcp-renegotiation
set client lac2 l2tp shared-secret "lac2-secret"
set client lac2 user-group-profile ce-l2tp-group-profile
top
edit access profile aaa-profile
set authentication-order radius
set radius-server 172.21.146.93 secret "aaa-secret"
top
edit access address-assignment pool client-pool1 family inet
set network 192.168.1.1/16
set range lns-v4-pool-range low 192.168.1.1
set range lns-v4-pool-range high 192.168.255.255
top
edit access address-assignment pool client-ipv6-pool2 family inet6
set prefix 2001:DB8::/32
set range lns-v6-pool-range low 2001:DB8:1::/48
```

```

set range lns-v6-pool-range high 2001:DB8:ffff::/48
top
set interfaces ge-5/0/1 unit 11 vlan-id 11
set interfaces ge-5/0/1 unit 11 family inet address 10.1.1.2/24
set interfaces lo0 unit 0 family inet address 127.0.0.1/32
top
set chassis fpc 5 pic 0 inline-services bandwidth 10g
set chassis fpc 5 pic 2 inline-services bandwidth 10g
top
edit interfaces si-5/0/0
set hierarchical-scheduler maximum-hierarchy-levels 2
set encapsulation generic-services
set unit 0 family inet
top
edit interfaces si-5/2/0
set hierarchical-scheduler maximum-hierarchy-levels 2
set encapsulation generic-services
set unit 0 family inet
top
set services service-device-pools pool lns_p1 interface si-5/0/0
set services service-device-pools pool lns_p1 interface si-5/2/0
top
edit dynamic-profiles dyn-lns-profile2 routing-instances $junos-routing-instance
set interface $junos-interface-name
edit routing-options access route $junos-framed-route-ip-address-prefix
set next-hop $junos-framed-route-nexthop
set metric $junos-framed-route-cost
set preference $junos-framed-route-distance
up 2
edit access-internal route $junos-subscriber-ip-address
set qualified-next-hop $junos-interface-name
up 5
edit interfaces $junos-interface-ifd-name unit $junos-interface-unit
set dial-options l2tp-interface-id l2tp-encapsulation
set dial-options dedicated
set family inet filter input $junos-input-filter
set family inet filter output $junos-output-filter
set family inet unnumbered-address $junos-loopback-interface
set family inet6 address $junos-ipv6-address
set family inet6 filter input $junos-input-ipv6-filter
set family inet6 filter output $junos-output-ipv6-filter
up 3
edit protocols router-advertisement
set interface $junos-interface-name prefix $junos-ipv6-ndra-prefix
top
[edit class-of-service]
edit rewrite-rules dscp rewriteDSCP forwarding-class expedited-forwarding
set loss-priority high code-point af11
set loss-priority high code-point af12
top
edit dynamic-profiles dyn-lns-profile2 class-of-service traffic-control-profiles tc-profile
set scheduler-map $junos-cos-scheduler-map
set shaping-rate $junos-cos-shaping-rate
set overhead-accounting $junos-cos-shaping-mode
set overhead-accounting bytes $junos-cos-byte-adjust
up

```

```

edit interfaces $junos-interface-ifd-name unit $junos-interface-unit
set forwarding-class expedited-forwarding
set output-traffic-control-profile tc-profile
set rewrite-rules dscp rewriteDSCP
edit interfaces si-5/0/0
set output-control-profile-remaining tc-profile
top
set services l2tp tunnel-group tg-dynamic l2tp-access-profile ce-l2tp-profile
set services l2tp tunnel-group tg-dynamic aaa-access-profile aaa-profile
set services l2tp tunnel-group tg-dynamic local-gateway address 10.1.1.2
set services l2tp tunnel-group tg-dynamic local-gateway gateway-name ce-lns
set services l2tp tunnel-group tg-dynamic service-device-pool lns_p1
set services l2tp tunnel-group tg-dynamic dynamic-profile dyn-lns-profile2

```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure an L2TP LNS with inline service interfaces:

1. Configure a user group profile that defines the PPP configuration for tunnel subscribers.

```

[edit access]
user@host# edit group-profile ce-l2tp-group-profile
[edit access group-profile ce-l2tp-group-profile]
user@host# set ppp keepalive 30
user@host# set ppp idle-timeout 200
user@host# set ppp ppp-options chap
user@host# set ppp ppp-options pap

```

2. Configure an L2TP access profile that defines the L2TP parameters for each client LAC. This includes associating a user group profile with the client and specifying the identifier for the inline services logical interface that represents an L2TP session on the LNS.

```

[edit access profile ce-l2tp-profile client lac1]
user@host# set l2tp interface-id l2tp-encapsulation
user@host# set l2tp maximum-sessions-per-tunnel 1000
user@host# set l2tp shared-secret "lac1-secret"
user@host# set l2tp lcp-renegotiation
user@host# set user-group-profile ce-l2tp-group-profile
[edit access profile ce-l2tp-profile client lac2]
user@host# set l2tp interface-id interface-id
user@host# set l2tp maximum-sessions-per-tunnel 4000
user@host# set l2tp shared-secret "lac2-secret"
user@host# set l2tp lcp-renegotiation
user@host# set user-group-profile ce-l2tp-group-profile

```



**NOTE:** If <user-group-profile> is modified or deleted, the existing LNS subscribers, which were using this Layer 2 Tunneling Protocol client configuration, will go down.

3. Configure a AAA access profile to override the global access profile for the order of AAA authentication methods and server attributes.

```
[edit access profile aaa-profile]
user@host# set authentication-order radius
user@host# set radius-server 172.21.146.93 secret "aaa-secret"
```

4. Configure IPv4 and IPv6 address-assignment pools to allocate addresses for the clients (LACs).

```
[edit access address-assignment pool client-pool1 family inet]
user@host# set network 192.168.1.1/16
user@host# set range lns-v4-pool-range low 192.168.1.1 high 192.168.255.255
[edit access address-assignment pool client-ipv6-pool2 family inet6]
user@host# set prefix 2010:DB8::/32
user@host# set range lns-v6-pool-range low 2010:DB8:1::/48
user@host# set range lns-v6-pool-range high 2010:DB8:ffff::/48
```

5. Configure the peer interface to terminate the tunnel and the PPP server-side IPCP address (loopback address).

```
[edit interfaces ge-5/0/1]
user@host# set vlan-tagging
user@host# set unit 11
[edit interfaces ge-5/0/1.11]
user@host# set vlan-id 11
user@host# set family inet address 10.1.1.2/24
[edit interfaces lo0]
user@host# set unit 0 family inet address 127.0.0.1/32
```

6. Enable inline service interfaces on an MPC.

```
[edit chassis fpc 5]
user@host# set pic 0 inline-services bandwidth 10g
user@host# set pic 2 inline-services bandwidth 10g
```

7. Configure the anchor service interfaces with services encapsulation, hierarchical scheduling, and the address family.

```
[edit interfaces si-5/0/0]
user@host# set hierarchical-scheduler maximum hierarchy-levels 2
user@host# set encapsulation generic-services
user@host# set unit 0 family inet
[edit interfaces si-5/2/0]
user@host# set hierarchical-scheduler maximum hierarchy-levels 2
user@host# set encapsulation generic-services
user@host# set unit 0 family inet
```

8. Configure a pool of service interfaces for dynamic LNS sessions.

```
[edit services service-device-pools pool lns_p1]
user@host# set interface si-5/0/0
user@host# set interface si-5/2/0
```

9. Configure a dynamic profile that dynamically creates L2TP logical interfaces for dual-stack subscribers.

```
[edit dynamic-profiles dyn-lns-profile2]
user@host# edit routing-instances $junos-routing-instance
user@host# set interface $junos-interface-name
```

```
[edit dynamic-profiles dyn-lns-profile2 routing-instances "$junos-routing-instance"]
user@host# edit routing-options access route $junos-framed-route-ip-address-prefix
[edit dynamic-profiles dyn-lns-profile2 routing-instances "$junos-routing-instance"
  routing-options access route "$junos-framed-route-ip-address-prefix"]
user@host# set next-hop $junos-framed-route-nexthop
user@host# set metric $junos-framed-route-cost
user@host# set preference $junos-framed-route-distance
[edit dynamic-profiles dyn-lns-profile2 routing-instances "$junos-routing-instance"
  routing-options access-internal]
user@host# set route $junos-subscriber-ip-address qualified-next-hop
  $junos-interface-name
[edit dynamic-profiles dyn-lns-profile2 interfaces "$junos-interface-ifd-name" unit
  "$junos-interface-unit"]
user@host# set dial-options l2tp-interface-id l2tp-encapsulation
user@host# set dial-options dedicated
user@host# set family inet unnumbered-address $junos-loopback-interface
user@host# set family inet filter input $junos-input-filter
user@host# set family inet filter output $junos-output-filter
user@host# set family inet6 address $junos-ipv6-address
set family inet6 filter input $junos-input-ipv6-filter
set family inet6 filter output $junos-output-ipv6-filter
[edit dynamic-profiles dyn-lns-profile2 protocols router-advertisement]
user@host# set interface $junos-interface-name prefix $junos-ipv6-ndra-prefix
```

10. Configure shaping, scheduling, and rewrite rules, and apply in the dynamic profile to tunnel traffic.

```
[edit class-of-service]
user@host# edit rewrite-rules dscp rewriteDSCP forwarding-class
  expedited-forwarding
user@host# set loss-priority high code-point af11
user@host# set loss-priority high code-point af12
[edit dynamic-profiles dyn-lns-profile2 class-of-service traffic-control-profiles
  tc-profile]
user@host# set scheduler-map $junos-cos-scheduler-map
user@host# set shaping-rate $junos-cos-shaping-rate
user@host# set overhead-accounting $junos-cos-shaping-mode
user@host# set overhead-accounting bytes $junos-cos-byte-adjust
[edit dynamic-profiles dyn-lns-profile2 class-of-service interfaces
  "$junos-interface-ifd-name" unit "$junos-interface-unit"]
user@host# set forwarding-class expedited-forwarding
user@host# set output-traffic-control-profile tc-profile
user@host# set rewrite-rules dscp rewriteDSCP
[edit class-of-service interfaces si-5/0/0]
user@host# set output-traffic-control-profile-remaining tc-profile
```

11. Configure the L2TP tunnel group to bring up dynamic LNS sessions using the pool of inline service interfaces to enable load-balancing.

```
[edit services l2tp tunnel-group tg-dynamic]
user@host# set l2tp-access-profile ce-l2tp-profile
user@host# set local-gateway address 10.1.1.2
user@host# set local-gateway gateway-name ce-lns
user@host# set aaa-access-profile aaa-profile
user@host# set dynamic-profile dyn-lns-profile2
user@host# set service-device-pool lns_p1
```



**Results** From configuration mode, confirm the access profile, group profile, AAA profile, and address-assignment pools configuration by entering the **show access** command. Confirm the inline services configuration by entering the **show chassis** command. Confirm the interface configuration by entering the **show interfaces** command. Confirm the dynamic profile configuration by entering the **show dynamic-profiles** command. Confirm the tunnel group configuration by entering the **show services l2tp** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show access
group-profile ce-l2tp-group-profile {
  ppp {
    idle-timeout 200;
    ppp-options {
      pap;
      chap;
    }
    keepalive 30;
  }
}
profile ce-l2tp-profile {
  client lac1 {
    l2tp {
      maximum-sessions-per-tunnel 1000;
      interface-id l2tp-encapsulation-1;
      lcp-renegotiation;
      shared-secret "$9$ZJGi.Pfz6/tmPtulIleLxNbwgaZjmPQDi"; ## SECRET-DATA
    }
    user-group-profile ce-l2tp-group-profile;
  }
  client lac2 {
    l2tp {
      maximum-sessions-per-tunnel 4000;
      interface-id l2tp-encap-2;
      lcp-renegotiation;
      shared-secret ""$9$KCjvLNdVYoaUdVDi.m3ntuOREyevLdVY8X"; ## SECRET-DATA
    }
    user-group-profile ce-l2tp-group-profile;
  }
}
profile aaa-profile {
  authentication-order radius;
  radius-server {
    172.21.146.93 secret "$9$4lJZjk.5Qz6k."; ## SECRET-DATA
  }
}
address-assignment {
  pool client-pool1 {
    family inet {
      network 192.168.1.1/16;
      range lns-v4-pool-range {
        low 192.168.1.1;
        high 192.168.255.255;
      }
    }
  }
}
```

```
    }  
  }  
  pool client-ipv6-pool2 {  
    family inet6 {  
      prefix 2001:DB8::/32;  
      range lns-v6-pool-range {  
        low 2001:DB8:1::/48;  
        high 2001:DB8:ffff::/48;  
      }  
    }  
  }  
}
```

```
[edit]  
user@host# show chassis  
fpc 5 {  
  pic 0 {  
    inline-services {  
      bandwidth 10g;  
    }  
  }  
  pic 2 {  
    inline-services {  
      bandwidth 10g;  
    }  
  }  
}
```

```
[edit]  
user@host# show interfaces  
ge-5/0/1 {  
  vlan-tagging;  
  unit 11 {  
    vlan-id 11;  
    family inet {  
      address 10.1.1.2/24;  
    }  
  }  
}  
si-5/0/0 {  
  hierarchical-scheduler maximum-hierarchy-levels 2;  
  encapsulation generic-services;  
  unit 0 {  
    family inet;  
  }  
}  
si-5/2/0 {  
  hierarchical-scheduler maximum-hierarchy-levels 2;  
  encapsulation generic-services;  
  unit 0 {  
    family inet;  
  }  
}  
lo0 {  
  unit 0 {
```

```

        family inet {
            address 127.0.0.1/32;
        }
    }
}
[edit]
user@host# show dynamic-profiles
dyn-lns-profile2 {
    routing-instances {
        "$junos-routing-instance" {
            interface "$junos-interface-name";
            routing-options {
                access {
                    route $junos-framed-route-ip-address-prefix {
                        next-hop "$junos-framed-route-nexthop";
                        metric "$junos-framed-route-cost";
                        preference "$junos-framed-route-distance";
                    }
                }
                access-internal {
                    route $junos-subscriber-ip-address {
                        qualified-next-hop "$junos-interface-name";
                    }
                }
            }
        }
    }
}
interfaces {
    "$junos-interface-ifd-name" {
        unit "$junos-interface-unit" {
            dial-options {
                l2tp-interface-id l2tp-encapsulation;
                dedicated;
            }
            family inet {
                filter {
                    input "$junos-input-filter";
                    output "$junos-output-filter";
                }
                unnumbered-address "$junos-loopback-interface";
            }
            family inet6 {
                address $junos-ipv6-address;
                input $junos-input-ipv6-filter;
                output $junos-output-ipv6-filter;
            }
        }
    }
}
protocols {
    router-advertisement {
        interface "$junos-interface-name" {
            prefix $junos-ipv6-ndra-prefix;
        }
    }
}

```

```

class-of-service {
  rewrite-rules {
    dscp rewriteDSCP {
      forwarding-class expedited-forwarding {
        loss-priority high code-point af11
        loss-priority high code-point af12
      }
    }
  }
  traffic-control-profiles {
    tc-profile {
      scheduler-map "$junos-cos-scheduler-map";
      shaping-rate "$junos-cos-shaping-rate";
      overhead-accounting "$junos-cos-shaping-mode" bytes "$junos-cos-byte-adjust";
    }
  }
  interfaces {
    "$junos-interface-ifd-name" {
      unit "$junos-interface-unit" {
        forwarding-class expedited-forwarding;
        output-traffic-control-profile tc-profile;
        rewrite-rules {
          dscp rewriteDSCP;
        }
      }
    }
  }
}

[edit]
user@host# show services l2tp
tunnel-group tg-dynamic {
  l2tp-access-profile ce-l2tp-profile;
  aaa-access-profile aaa-profile;
  local-gateway {
    address 10.1.1.2;
    gateway-name ce-lns;
  }
  service-device-pool lns_p1;
  dynamic-profile dyn-lns-profile2;
}

```

When you are done configuring the device, enter **commit** from configuration mode.

#### Related Documentation

- [L2TP for Subscriber Access Overview on page 3](#)
- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)
- [Configuring an L2TP LAC on page 35](#)

## CHAPTER 8

# Configuration Statements

- [\[edit access tunnel-profile\] Hierarchy Level on page 93](#)
- [\[edit access tunnel-switch-profile\] Hierarchy Level on page 94](#)
- [\[edit services l2tp\] Hierarchy Level on page 94](#)
- [aaa-access-profile \(L2TP LNS\) on page 96](#)
- [access-line-information \(L2TP LAC\) on page 97](#)
- [address \(LNS Local Gateway\) on page 97](#)
- [address \(Tunnel Profile Remote Gateway\) on page 98](#)
- [address \(Tunnel Profile Source Gateway\) on page 98](#)
- [assignment-id-format \(L2TP LAC\) on page 99](#)
- [avp \(L2TP Tunnel Switching\) on page 100](#)
- [bandwidth \(Inline Services\) on page 100](#)
- [bearer-type \(L2TP Tunnel Switching\) on page 101](#)
- [calling-number \(L2TP Tunnel Switching\) on page 102](#)
- [chap on page 103](#)
- [chap \(Dynamic PPP\) on page 104](#)
- [chap \(L2TP\) on page 104](#)
- [cisco-nas-port-info \(L2TP Tunnel Switching\) on page 105](#)
- [client on page 106](#)
- [destination \(L2TP\) on page 107](#)
- [destruct-timeout \(L2TP\) on page 108](#)
- [dial-options on page 109](#)
- [dial-options \(Dynamic Profiles\) on page 110](#)
- [disable-calling-number-avp \(L2TP LAC\) on page 110](#)
- [disable-failover-protocol \(L2TP LAC\) on page 111](#)
- [dynamic-profile \(L2TP\) on page 111](#)
- [enable-snmp-tunnel-statistics \(L2TP\) on page 112](#)
- [failover-within-preference \(L2TP LAC\) on page 112](#)
- [fpc \(MX Series 3D Universal Edge Routers\) on page 113](#)

- [gateway-name \(LNS Local Gateway\) on page 114](#)
- [gateway-name \(Tunnel Profile Remote Gateway\) on page 114](#)
- [gateway-name \(Tunnel Profile Source Gateway\) on page 115](#)
- [group-profile \(Group Profile\) on page 116](#)
- [hello-interval on page 117](#)
- [identification \(Tunnel Profile\) on page 117](#)
- [idle-timeout \(Access\) on page 118](#)
- [idle-timeout \(L2TP\) on page 119](#)
- [inline-services \(FPC Level\) on page 120](#)
- [inline-services \(PIC level\) on page 120](#)
- [interface \(L2TP Service Interfaces\) on page 121](#)
- [interface-id on page 122](#)
- [ip-reassembly on page 123](#)
- [ip-reassembly-rules \(Service Set\) on page 124](#)
- [ip-reassembly \(L2TP\) on page 125](#)
- [keepalive on page 126](#)
- [keepalives on page 127](#)
- [keepalives \(Dynamic Profiles\) on page 128](#)
- [l2tp on page 129](#)
- [l2tp-access-profile on page 131](#)
- [lcp-renegotiation on page 131](#)
- [local-gateway \(L2TP LNS\) on page 132](#)
- [lockout-timeout \(L2TP Destination Lockout\) on page 133](#)
- [logical-system \(Tunnel Profile\) on page 134](#)
- [match-direction \(IP Reassembly Rule\) on page 134](#)
- [maximum-sessions-per-tunnel on page 135](#)
- [max-sessions \(Tunnel Profile\) on page 135](#)
- [medium \(Tunnel Profile\) on page 136](#)
- [minimum-retransmission-timeout \(L2TP Tunnel\) on page 136](#)
- [nas-port-method \(L2TP LAC\) on page 137](#)
- [nas-port-method \(Tunnel Profile\) on page 137](#)
- [next-hop-service on page 138](#)
- [pap on page 139](#)
- [pap \(Dynamic PPP\) on page 140](#)
- [pap \(L2TP\) on page 140](#)
- [pic \(M Series and T Series Routers\) on page 141](#)
- [pool \(L2TP Service Interfaces\) on page 142](#)

- [ppp \(Group Profile\) on page 143](#)
- [ppp-options on page 144](#)
- [ppp-options \(Dynamic PPP\) on page 145](#)
- [ppp-options \(L2TP\) on page 146](#)
- [preference \(Tunnel Profile\) on page 146](#)
- [remote-gateway \(Tunnel Profile\) on page 147](#)
- [request services l2tp destination unlock](#)
- [retransmission-count-established \(L2TP\) on page 149](#)
- [retransmission-count-not-established \(L2TP\) on page 150](#)
- [routing-instance \(Tunnel Profile\) on page 150](#)
- [rule \(IP Reassembly\) on page 151](#)
- [rx-connect-speed-when-equal \(L2TP LAC\) on page 152](#)
- [rx-window-size \(L2TP\) on page 152](#)
- [secret \(Tunnel Profile\) on page 153](#)
- [service-device-pool \(L2TP\) on page 153](#)
- [service-device-pools \(L2TP Service Interfaces\) on page 154](#)
- [service-interface on page 155](#)
- [shared-secret on page 155](#)
- [source-gateway \(Tunnel Profile\) on page 156](#)
- [tos-reflect \(L2TP\) on page 156](#)
- [traceoptions \(L2TP\) on page 157](#)
- [tunnel \(Tunnel Profile\) on page 162](#)
- [tunnel \(L2TP\) on page 163](#)
- [tunnel-group on page 164](#)
- [tunnel-profile \(L2TP Tunnel Switching\) on page 165](#)
- [tunnel-profile \(Tunnel Profile\) on page 166](#)
- [tunnel-switch-profile \(L2TP Tunnel Switching, Application\) on page 167](#)
- [tunnel-switch-profile \(L2TP Tunnel Switching, Definition\) on page 167](#)
- [tx-address-change \(L2TP LAC\) on page 168](#)
- [tx-connect-speed-method \(L2TP LAC\) on page 169](#)
- [type \(Tunnel Profile\) on page 170](#)
- [user-group-profile on page 170](#)
- [weighted-load-balancing \(L2TP LAC\) on page 171](#)

## [\[edit access tunnel-profile\] Hierarchy Level](#)

---

```
access {  
  tunnel-profile profile-name {  
    tunnel tunnel-id {
```

```

identification name;
logical-system logical-system-name;
max-sessions number;
medium type;
nas-port-method cisco-avp;
preference number;
remote-gateway {
    address server-ip-address;
    gateway-name server-name;
}
routing-instance routing-instance-name;
secret password;
source-gateway {
    address client-ip-address;
    gateway-name client-name;
}
type tunnel-type;
}
}
}

```

**Related Documentation**

- [Configuring a Tunnel Profile for Subscriber Access on page 37](#)

## [edit access tunnel-switch-profile] Hierarchy Level

```

access {
    tunnel-switch-profile profile-name {
        avp {
            bearer-type action;
            calling-number action;
            cisco-nas-port-info action;
        }
        tunnel-profile profile-name;
    }
}

```

**Related Documentation**

- [Configuring L2TP Tunnel Switching on page 70](#)

## [edit services l2tp] Hierarchy Level



**NOTE:** The `tunnel-group group-name` stanza is not supported for L2TP LAC. It applies only to L2TP LNS. Similarly, some of the options for the `traceoptions` statement apply only to L2TP LNS; for more information, see [traceoptions](#).

```

services {
    l2tp {
        destination [ip-address] {
            access-line-information <connection-speed-update>;
            lockout-timeout seconds;
        }
    }
}

```



```

destruct-timeout seconds;
disable-calling-number-avp;
disable-failover-protocol;
enable-snmp-tunnel-statistics;
failover-within-preference;
ip-reassembly;
rx-connect-speed-when-equal;
traceoptions {
  debug-level level;
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  filter {
    protocol name;
    user user@domain;
    user-name username;
  }
  flag flag;
  interfaces interface-name {
    debug-level severity;
    flag flag;
  }
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
tunnel {
  assignment-id-format (assignment-id | client-server-id);
  idle-timeout seconds;
  minimum-retransmission-timeout;
  nas-port-method;
  retransmission-count-established count;
  retransmission-count-not-established count;
  rx-window-size
  tx-address-change (accept | ignore | ignore-ip-address | ignore-udp-port);
}
tunnel-group group-name {
  aaa-access-profile profile-name;
  dynamic-profile;
  hello-interval seconds;
  hide-avps;
  l2tp-access-profile profile-name;
  local-gateway address;
  maximum-send-window packets;
  ppp-access-profile profile-name;
  receive-window packets;
  retransmit-interval seconds;
  service-device-pool;
  service-interface interface-name;
  syslog {
    host hostname {
      facility-override facility-name;
      log-prefix prefix-value;
      services severity-level;
    }
  }
  tos-reflect;
  tunnel-switch-profile profile-name;

```

```
        tunnel-timeout seconds;  
    }  
    tunnel-switch-profile profile-name;  
    tx-connect-speed-method method;  
    weighted-load-balancing;  
    }  
}
```

- Related Documentation**
- [L2TP for Subscriber Access Overview on page 3](#)
  - [Configuring an L2TP LAC on page 35](#)
  - [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)

---

## aaa-access-profile (L2TP LNS)

---

<b>Syntax</b>	<code>aaa-access-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	[edit services l2tp <code>tunnel-group <i>name</i></code> ], [edit access profile <i>profile-name</i> client <i>client-name</i> l2tp]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4. Support at the [edit access profile <i>profile-name</i> client <i>client-name</i> l2tp] hierarchy level introduced in Junos OS Release 12.1.
<b>Description</b>	Specify a AAA access profile that overrides the AAA access profile configured for the routing instance with the <b>access-profile</b> statement. You can configure a profile to specify the RADIUS server settings for a tunnel group or for a LAC client, or both. The AAA access profile configured for the client takes precedence over the AAA access profile configured for the tunnel group, which takes precedence over the access profile configured for the routing instance.
<b>Options</b>	<i>profile-name</i> —Name of the local access profile for the tunnel group or client.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring an L2TP LNS with Inline Service Interfaces on page 51</a></li><li>• <a href="#">Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64</a></li></ul>

## access-line-information (L2TP LAC)

<b>Syntax</b>	<code>access-line-information &lt;connection-speed-update&gt;;</code>
<b>Hierarchy Level</b>	[edit services l2tp tunnel <i>destination ip-address</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	Configure the LAC to forward subscriber line identification and other DSL attributes to the LNS by means of L2TP AVPs for tunnels with the specified endpoint address.
<b>Options</b>	<b>connection-speed-update</b> —(Optional) Include the Connect Speed Update Enable AVP (98) in ICRQ messages to alert the LNS that the LAC may send CSUN messages that report speed changes originating with the ANCP agent.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the LAC to Report Access Line Information to the LNS on page 48</a></li> </ul>

## address (LNS Local Gateway)

<b>Syntax</b>	<code>address <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit services l2tp tunnel-group <i>name local-gateway</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the local (LNS) IP address for L2TP tunnel.
<b>Options</b>	<b>address</b> —Local IP address; corresponds to the IP address that is used by LACs to identify the LNS. When the LAC is an MX Series router, this address matches the remote gateway address configured in the LAC tunnel profile.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Local Gateway Address and PIC.</a></li> <li>• <a href="#">Configuring L2TP Tunnel Groups</a></li> <li>• <a href="#">Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64</a></li> </ul>

## address (Tunnel Profile Remote Gateway)

---


<b>Syntax</b>	<code>address <i>server-ip-address</i>;</code>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i> <a href="#">remote-gateway</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the IP address of the remote gateway device at the L2TP tunnel endpoint, the LNS.
<b>Options</b>	<i>server-ip-address</i> —IP address of the remote gateway device. <b>Default:</b> 0.0.0.0.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li></ul>

## address (Tunnel Profile Source Gateway)

---

<b>Syntax</b>	<code>address <i>client-ip-address</i>;</code>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i> <a href="#">source-gateway</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the IP address of the source gateway device at the local L2TP tunnel endpoint, the LAC. This value overrides the default address for the logical system or routing instance.
<b>Options</b>	<i>client-ip-address</i> —IP address of the source gateway device. <b>Default:</b> 0.0.0.0.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li></ul>

## assignment-id-format (L2TP LAC)

<b>Syntax</b>	assignment-id-format (assignment-id   client-server-id);
<b>Hierarchy Level</b>	[edit services l2tp <a href="#">tunnel</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Set the format for the name used for a tunnel, the tunnel assignment ID.
<div>  <p><b>NOTE:</b> Before you downgrade to a Junos OS Release that does not support this statement, unconfigure the statement by issuing <code>no services l2tp tunnel assignment-id-format</code>.</p> </div>	
<b>Default</b>	assignment-Id
<b>Options</b>	<p><b>assignment-Id</b>—The tunnel name corresponds to RADIUS attribute Tunnel-Assignment-Id [82].</p> <p><b>client-server-id</b>—The tunnel name is a combination of RADIUS attributes Tunnel-Client-Auth-Id [90], Tunnel-Server-Auth-Id [91], and Tunnel-Assignment-Id [82].</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Setting the Format for the Tunnel Name on page 45</a></li> </ul>

## avp (L2TP Tunnel Switching)

---

<b>Syntax</b>	<pre>avp {     bearer-type;     calling-number;     cisco-nas-port-info; }</pre>
<b>Hierarchy Level</b>	[edit access <a href="#">tunnel-switch-profile</a> <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2.
<b>Description</b>	<p>Specify the action taken on L2TP AVPs that are negotiated when the first session is created; these AVPs are contained in the L2TP packets that are switched by the tunnel switch profile.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring L2TP Tunnel Switching on page 70</a></li></ul>

## bandwidth (Inline Services)

---

<b>Syntax</b>	<pre>bandwidth (1g   10g);</pre>
<b>Hierarchy Level</b>	[edit chassis <a href="#">fpc</a> <i>slot-number</i> <a href="#">pic</a> <i>number</i> <a href="#">inline-services</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Configure the amount of bandwidth reserved on each Packet Forwarding Engine for tunnel traffic using inline services.
<b>Options</b>	<p><b>1g</b>—Reserves 1 Gbps of bandwidth for tunnel traffic. Configuring a bandwidth of 1 Gbps creates a virtual tunnel interface that is represented as <code>vt-&lt;slot-number/pic-number/10&gt;</code>.</p> <p><b>10g</b>—Reserves 10 Gbps of bandwidth for tunnel traffic. Configuring a bandwidth of 10 Gbps creates a virtual tunnel interface that is represented as <code>vt-&lt;slot-number/pic-number/0&gt;</code>.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Enabling Inline Service Interfaces on page 61</a></li><li>• <a href="#">Configuring an L2TP LNS with Inline Service Interfaces on page 51</a></li></ul>

---

## bearer-type (L2TP Tunnel Switching)

---

<b>Syntax</b>	<code>bearer-type <i>action</i>;</code>
<b>Hierarchy Level</b>	[edit access tunnel-switch-profile <i>profile-name</i> <b>avp</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2.
<b>Description</b>	Specify the action taken on the Bearer Type AVP (18) in the L2TP packets during tunnel switching if the AVP is negotiated when the first session is created.
<b>Options</b>	<p><b><i>action</i></b>—One of the following actions:</p> <p><b><i>action</i></b>—One of the following actions:</p> <ul style="list-style-type: none"><li>• <b>drop</b>—Drop the AVP.</li><li>• <b>regenerate</b>—Regenerate the AVP based on the local policy at the LTS and send it in the switched packet. The local policy may or may not use the value for the AVP received during negotiation for the first session.</li><li>• <b>relay</b>—Forward the AVP transparently as is and send it in the switched packet.</li></ul> <p><b>Default:</b> <code>relay</code></p>
<b>Required Privilege Level</b>	<p><code>admin</code>—To view this statement in the configuration.</p> <p><code>admin-control</code>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring L2TP Tunnel Switching on page 70</a></li></ul>


## calling-number (L2TP Tunnel Switching)

---

<b>Syntax</b>	<code>calling-number <i>action</i>;</code>
<b>Hierarchy Level</b>	[edit access tunnel-switch-profile <i>profile-name</i> <b>avp</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2.
<b>Description</b>	Specify the action taken on the Calling Number AVP (22) in the L2TP packets during tunnel switching if the AVP is negotiated when the first session is created.
<b>Options</b>	<p><b><i>action</i></b>—One of the following actions:</p> <p><b><i>action</i></b>—One of the following actions:</p> <ul style="list-style-type: none"><li>• <b>drop</b>—Drop the AVP.</li><li>• <b>regenerate</b>—Regenerate the AVP based on the local policy at the LTS and send it in the switched packet. The local policy may or may not use the value for the AVP received during negotiation for the first session.</li><li>• <b>relay</b>—Forward the AVP transparently as is and send it in the switched packet.</li></ul> <p><b>Default:</b> <code>relay</code></p>
<b>Required Privilege Level</b>	<p><code>admin</code>—To view this statement in the configuration.</p> <p><code>admin-control</code>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring L2TP Tunnel Switching on page 70</a></li></ul>



## chap

<b>Syntax</b>	<pre> chap {   access-profile <i>name</i>;   challenge-length minimum <i>minimum-length</i> maximum <i>maximum-length</i>;   default-chap-secret <i>name</i>;   local-name <i>name</i>;   passive; } </pre>
<b>Hierarchy Level</b>	<p>[edit interfaces <i>interface-name</i> <a href="#">ppp-options</a>],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <a href="#">ppp-options</a>],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <a href="#">ppp-options</a>]</p>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Allow each side of a link to challenge its peer, using a “secret” known only to the authenticator and that peer. The secret is not sent over the link.</p> <p>By default, PPP CHAP is disabled. If CHAP is not explicitly enabled, the interface makes no CHAP challenges and denies all incoming CHAP challenges.</p> <p>For ATM2 IQ interfaces only, you can configure CHAP on the logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:</p> <ul style="list-style-type: none"> <li>• <b>atm-ppp-llc</b>—PPP over AAL5 LLC encapsulation.</li> <li>• <b>atm-ppp-vc-mux</b>—PPP over AAL5 multiplex encapsulation.</li> </ul>
	<p>.....</p> <div>  <p><b>BEST PRACTICE:</b> On inline service (si) interfaces for L2TP, only the <code>chap</code> statement itself is typically used for subscriber management. We recommend that you leave the subordinate statements at their default values.</p> </div> <p>.....</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the PPP Challenge Handshake Authentication Protocol</a></li> <li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile on page 53</a></li> <li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface on page 54</a></li> </ul>

## chap (Dynamic PPP)

---

<b>Syntax</b>	<pre>chap {     challenge-length minimum <i>minimum-length</i> maximum <i>maximum-length</i>; }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" <b>ppp-options</b> ], [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit" <b>ppp-options</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Support at the [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit" <b>ppp-options</b> ] hierarchy level introduced in Junos OS Release 12.2.
<b>Description</b>	Specify CHAP authentication in a PPP dynamic profile.  The remaining statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Dynamic Profiles Overview</a></li><li>• <a href="#">Configuring Dynamic Authentication for PPP Subscribers</a></li><li>• <a href="#">Attaching Dynamic Profiles to Static PPP Subscriber Interfaces</a></li><li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface on page 54</a></li></ul>

## chap (L2TP)

---

<b>Syntax</b>	<pre>chap;</pre>
<b>Hierarchy Level</b>	[edit access group-profile <i>profile-name</i> ppp <b>ppp-options</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	(MX Series routers only) Specify CHAP authentication for PPP subscribers in an L2TP LNS user group profile.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile on page 53</a></li><li>• <a href="#">Configuring an L2TP LNS with Inline Service Interfaces on page 51</a></li></ul>

## cisco-nas-port-info (L2TP Tunnel Switching)

<b>Syntax</b>	<code>cisco-nas-port-info <i>action</i>;</code>
<b>Hierarchy Level</b>	[edit access tunnel-switch-profile <i>profile-name</i> <b>avp</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2.
<b>Description</b>	<p>Define a tunnel profile for subscriber access.</p> <p>Specify the action taken on the Cisco NAS Port Info AVP (100) in the L2TP packets during tunnel switching if the AVP is negotiated when the first session is created.</p>
<b>Options</b>	<p><b><i>action</i></b>—One of the following actions:</p> <p><b><i>action</i></b>—One of the following actions:</p> <ul style="list-style-type: none"> <li>• <b>drop</b>—Drop the AVP.</li> <li>• <b>regenerate</b>—Regenerate the AVP based on the local policy at the LTS and send it in the switched packet. The local policy may or may not use the value for the AVP received during negotiation for the first session.</li> <li>• <b>relay</b>—Forward the AVP transparently as is and send it in the switched packet.</li> </ul> <p><b>Default:</b> relay</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring L2TP Tunnel Switching on page 70</a></li> </ul>

## client

**Syntax**    client *client-name* {  
              chap-secret *chap-secret*;  
              group-profile *profile-name*;  
              ike {  
                  allowed-proxy-pair {  
                      remote *remote-proxy-address* local *local-proxy-address*;  
                  }  
              pre-shared-key (ascii-text *character-string* | hexadecimal *hexadecimal-digits*);  
              ike-policy *policy-name*;  
              interface-id *string-value*;  
              }  
              l2tp {  
                  aaa-access-profile *profile-name*;  
                  interface-id *interface-id*;  
                  lcp-renegotiation;  
                  local-chap;  
                  maximum-sessions-per-tunnel *number*;  
                  multilink {  
                      drop-timeout *milliseconds*;  
                      fragment-threshold *bytes*;  
                  }  
                  ppp-authentication (chap | pap);  
                  ppp-profile *profile-name*;  
                  shared-secret *shared-secret*;  
                  }  
              pap-password *pap-password*;  
              ppp {  
                  cell-overhead;  
                  encapsulation-overhead *bytes*;  
                  framed-ip-address *ip-address*;  
                  framed-pool *framed-pool*;  
                  idle-timeout *seconds*;  
                  interface-id *interface-id*;  
                  keepalive *seconds*;  
                  primary-dns *primary-dns*;  
                  primary-wins *primary-wins*;  
                  secondary-dns *secondary-dns*;  
                  secondary-wins *secondary-wins*;  
              }  
              user-group-profile *profile-name*;  
              }

**Hierarchy Level**    [edit access profile *profile-name*]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Configure the peer identity.



**NOTE:** Subordinate statement support depends on the platform. See individual statement topics for more detailed support information.

**Options** *client-name*—A peer identity. For L2TP clients, you can use a special name to configure a default client. This client enables the LNS to accept any LAC to establish the session. On M Series routers, use \* for the default client configuration. On MX Series routers, use **default**.

The remaining statements are explained separately.

**Required Privilege Level** admin—To view this statement in the configuration.  
admin-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring the L2TP Client](#)
- [Configuring Access Profiles for L2TP or PPP Parameters](#)
- [Configuring an L2TP Access Profile on the LNS on page 56](#)

## destination (L2TP)

**Syntax** `destination [ip-address] {  
    access-line-information <connection-speed-update>;  
    lockout-timeout seconds;  
}`

**Hierarchy Level** [edit services [l2tp](#)]

**Release Information** Statement introduced in Junos OS Release 13.2.  
Option *ip-address* introduced in Junos OS Release 14.1

**Description** Configure attributes for all L2TP destinations or a specified L2TP destination.

The remaining statements are explained separately.

**Options** *ip-address*—(Optional) Endpoint address of an L2TP tunnel. This option applies only to the **access-line-information** statement.


**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring the L2TP Destination Lockout Timeout on page 69](#)
- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)
- [Configuring the LAC to Report Access Line Information to the LNS on page 48](#)

## destruct-timeout (L2TP)

---

<b>Syntax</b>	<code>destruct-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit services <a href="#">l2tp</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	Set how long the router attempts to maintain dynamic destinations, tunnels, and sessions after they have been destroyed.
<div> <b>BEST PRACTICE:</b> Before you downgrade to a Junos OS Release that does not support this statement, unconfigure the statement by issuing <code>no services l2tp destruct-timeout</code>.</div>	
<b>Options</b>	<p><i>seconds</i>—Length of the destruct timeout.</p> <p><b>Range:</b> 10 through 3600</p> <p><b>Default:</b> 300</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Setting the L2TP Destruct Timeout on page 76</a></li><li>• <a href="#">Configuring an L2TP LAC on page 35</a></li><li>• <a href="#">Configuring an L2TP LNS with Inline Service Interfaces on page 51</a></li></ul>

## dial-options

<b>Syntax</b>	<pre>dial-options {   ipsec-interface-id <i>name</i>;   l2tp-interface-id <i>name</i>;   (shared   dedicated); }</pre>
<b>Hierarchy Level</b>	<pre>[edit interfaces sp-<i>fpc/pic/port</i> unit <i>logical-unit-number</i>], [edit interfaces si-<i>fpc/pic/port</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces sp-<i>fpc/pic/port</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces si-<i>fpc/pic/port</i> unit <i>logical-unit-number</i>]</pre>
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>The <b>[edit ...si-...]</b> hierarchy levels introduced in Junos OS Release 11.4.</p>
<b>Description</b>	Specify the options for configuring logical interfaces for group and user sessions in L2TP or IPsec dynamic endpoint tunneling.
<b>Options</b>	<p><b>dedicated</b>—(LNS on M Series routers and MX Series routers only) Specify that a logical interface can host only one session at a time.</p> <p><b>ipsec-interface-id <i>name</i></b>—(M Series routers only) Interface identifier for group of dynamic peers. This identifier must be replicated at the <b>[edit access profile <i>name</i> client * ike]</b> hierarchy level.</p> <p><b>l2tp-interface-id <i>name</i></b>—Interface identifier that must be replicated at the <b>[edit access profile <i>name</i>]</b> hierarchy level.</p> <p><b>shared</b>—(LNS on M Series routers only) Specify that a logical interface can host multiple (shared) sessions at a time.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring the Identifier for Logical Interfaces that Provide L2TP Services</i></li> <li>• <i>Configuring Dynamic Endpoints for IPsec Tunnels</i></li> <li>• <a href="#">Configuring Options for the LNS Inline Services Logical Interface on page 64</a></li> </ul>

## dial-options (Dynamic Profiles)

---

<b>Syntax</b>	<pre>dial-options {     ipsec-interface-id <i>name</i>;     l2tp-interface-id <i>name</i>;     (shared   dedicated); }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Specify the options for configuring logical interfaces in dynamic profiles for group and user sessions in L2TP or IPsec dynamic endpoint tunneling.
<b>Options</b>	<p><b>dedicated</b>—(LNS on M Series routers and MX Series routers only) Specify that a logical interface can host only one session at a time.</p> <p><b>ipsec-interface-id <i>name</i></b>—Interface identifier for group of dynamic peers. This identifier must be replicated at the [edit access profile <i>name</i> client * <i>ike</i>] hierarchy level. This options is not currently supported.</p> <p><b>l2tp-interface-id <i>name</i></b>—(MX Series routers only) L2TP interface identifier that must be replicated at the [edit access profile <i>name</i>] hierarchy level.</p> <p><b>shared</b>—(LNS on M Series routers only) Specify that a logical interface can host multiple (shared) sessions at a time</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Dynamic Profile for Dynamic LNS Sessions on page 67</a></li></ul>

## disable-calling-number-avp (L2TP LAC)

---

<b>Syntax</b>	<pre>disable-calling-number-avp;</pre>
<b>Hierarchy Level</b>	[edit services <b>l2tp</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Prevent the LAC from sending L2TP Calling Number AVP 22 in incoming-call request (ICRQ) packets to the LNS. By default, the LAC in an L2TP network generates this AVP from the Calling-Station-Id and sends it to the LNS.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Preventing the LAC from Sending Calling Number AVP 22 to the LNS on page 42</a></li></ul>



## disable-failover-protocol (L2TP LAC)

---

<b>Syntax</b>	disable-failover-protocol;
<b>Hierarchy Level</b>	[edit services l2tp]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Configure the LAC to use only the silent failover method when resynchronizing with the peer LNS in the event of LAC failover. This command prevents the default behavior, wherein the LAC first attempts to use the failover protocol and then falls back on the silent failover method. This configuration can be useful when routers that act as the LNS are configured for silent failover or incorrectly negotiate use of the failover protocol even though they do not support it.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Preventing the LAC From Negotiating L2TP Failover Protocol on page 44</a></li> </ul>

## dynamic-profile (L2TP)

---

<b>Syntax</b>	dynamic-profile <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group</b> <i>name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Assign a dynamic profile to the tunnel group for dynamic LNS sessions.
<b>Options</b>	<i>profile-name</i> —Name of the dynamic profile for the tunnel group.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring a Dynamic Profile for Dynamic LNS Sessions on page 67</a></li> </ul>

## enable-snmp-tunnel-statistics (L2TP)

---

<b>Syntax</b>	enable-snmp-tunnel-statistics;
<b>Hierarchy Level</b>	[edit services <a href="#">l2tp</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1R4 and supported in later 12.1Rx releases. Statement supported in Junos OS Release 12.2R2 and later 12.2Rx releases. (Not supported in Junos OS Release 12.2R1.) Statement supported in Junos OS Release 12.3 and later releases.
<b>Description</b>	Enable collection of L2TP tunnel and global counters for SNMP statistics.



**NOTE:** The system load can increase when you enable these counters and also use RADIUS interim accounting updates. We recommend you enable these counters when you are using only SNMP statistics.

<b>Default</b>	Disabled.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Enabling Tunnel and Global Counters for SNMP Statistics Collection on page 77</a></li></ul>

## failover-within-preference (L2TP LAC)

---

<b>Syntax</b>	failover-within-preference;
<b>Hierarchy Level</b>	[edit services <a href="#">l2tp</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Enable L2TP LAC tunnel selection within a preference level. When the router is unable to connect to a destination at a given preference level, it attempts to connect to another destination at the same level. By default, when a connection attempt fails at one preference level, the next attempt is made at the next lower level.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring LAC Tunnel Selection Failover Within a Preference Level on page 40</a></li><li>• <a href="#">Configuring the L2TP LAC Tunnel Selection Parameters on page 40</a></li></ul>

## fpc (MX Series 3D Universal Edge Routers)

<b>Syntax</b>	<pre> fpc slot-number {     inline-services {         flow-table-size {             ipv4-flow-table-size units;             ipv4-flow-table-size units;         }     }     pic number {         inline-services {             bandwidth (1g   10g);         }         port-mirror-instance port-mirroring-instance-name-pic-level;         tunnel-services {             bandwidth (1g   10g)         }     }     port-mirror-instance port-mirroring-instance-name-fpc-level; } </pre>
<b>Hierarchy Level</b>	[edit chassis]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 8.2.</p> <p>Option <b>port-mirror-instance</b> introduced in Junos OS Release 9.3.</p>
<b>Description</b>	<p>Configure properties for the DPC or MPC and corresponding Packet Forwarding Engines to create tunnel interfaces.</p> <p>(MX Series Virtual Chassis only) To configure properties for MPCs in a member router in an MX Series Virtual Chassis configuration, you must specify the router's Virtual Chassis member number <i>before</i> the <b>fpc</b> statement. Specify the member number in the form <b>member member-id</b>, where <i>member-id</i> is 0 or 1. If you do not specify the member number before the <b>fpc</b> statement, the commit operation fails and the software displays an error message indicating that the <b>fpc</b> statement must include the member number for routers in Virtual Chassis mode.</p>
<b>Options</b>	<p><b>fpc slot-number</b>—Specify the slot number of the DPC.</p> <p><b>Range:</b> 0 through 11</p> <p><b>pic number</b>—Specify the number of the Packet Forwarding Engine. Each DPC includes four Packet Forwarding Engines.</p> <p><b>Range:</b> 0 through 4</p> <p><b>port-mirror-instance port-mirroring-instance-name-fpc-level</b>—Associate a port-mirroring instance with the DPC and its corresponding PICs. The port-mirroring instance is configured under the <b>[edit forwarding-options port-mirroring]</b> hierarchy level.</p> <p>The remaining statements are explained separately.</p>

<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Port-Mirroring Instances on MX Series 3D Universal Edge Routers</a></li><li>• <a href="#">Enabling Inline Service Interfaces on page 61</a></li></ul>

---

## gateway-name (LNS Local Gateway)

---

<b>Syntax</b>	<code>gateway-name gateway-name;</code>
<b>Hierarchy Level</b>	[edit services l2tp tunnel-group <i>group-name</i> <b>local-gateway</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.2.
<b>Description</b>	Specify the gateway name for the LNS, which the LNS returns to the LAC in response to the LAC's SCCRQ message. This name must match the remote gateway name configured on the LAC, or the tunnel cannot be established.
<b>Options</b>	<b>gateway-name</b> —Name of the LNS.
<b>Required Privilege</b>	admin—To view this statement in the configuration.
<b>Level</b>	admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64</a></li></ul>

---

## gateway-name (Tunnel Profile Remote Gateway)

---

<b>Syntax</b>	<code>gateway-name server-name;</code>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i> <b>remote-gateway</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the hostname expected by the remote gateway—the LNS—from the source gateway—the LAC—when you set up a tunnel.
<b>Options</b>	<b>server-name</b> —Name of the LNS.
<b>Required Privilege</b>	admin—To view this statement in the configuration.
<b>Level</b>	admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li></ul>

## gateway-name (Tunnel Profile Source Gateway)

---

<b>Syntax</b>	<code>gateway-name <i>client-name</i>;</code>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i> <a href="#">source-gateway</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the hostname provided by the source gateway—the LAC—to the remote gateway—the LNS—when you set up a tunnel.
<b>Options</b>	<i>client-name</i> —Name of the LAC.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li></ul>

## group-profile (Group Profile)

**Syntax**

```
group-profile profile-name {
  l2tp {
    interface-id interface-id;
    lcp-renegotiation;
    local-chap;
    maximum-sessions-per-tunnel number;
  }
  ppp {
    cell-overhead;
    encapsulation-overhead bytes;
    framed-pool pool-id;
    idle-timeout seconds;
    interface-id interface-id;
    keepalive seconds;
    ppp-options {
      chap;
      pap;
    }
    primary-dns primary-dns;
    primary-wins primary-wins;
    secondary-dns secondary-dns;
    secondary-wins secondary-wins;
  }
}
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Configure the group profile.



**NOTE:** Subordinate statement support depends on the platform. See individual statement topics for more detailed support information.

**Options** *profile-name*—Name assigned to the group profile.

The remaining statements are explained separately.


**Required Privilege Level**

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring the Group Profile for Defining L2TP Attributes](#)
- [Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile on page 53](#)

## hello-interval


<b>Syntax</b>	<code>hello-interval <i>seconds</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services l2tp <i>tunnel-group name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the keepalive timer for L2TP tunnels.
<div>  <b>NOTE:</b> Subordinate statement support depends on the platform. See individual statement topics for more detailed support information.         </div>	
<b>Options</b>	<p><b><i>seconds</i></b>—Interval, in seconds, after which the server sends a hello message if no messages are received. A value of <b>0</b> means that no hello messages are sent.</p> <p><b>Default:</b> 60 seconds</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Timers for L2TP Tunnels</a></li> <li>• <a href="#">Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64</a></li> </ul>

## identification (Tunnel Profile)

<b>Syntax</b>	<code>identification <i>name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access tunnel-profile <i>profile-name</i> <i>tunnel</i> <i>tunnel-id</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the assignment ID of an L2TP tunnel. L2TP sessions with the same tunnel assignment identification and destination are grouped into the same tunnel.
<b>Options</b>	<b><i>name</i></b> —Tunnel assignment ID; string of up to 32 alphanumeric characters.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li> </ul>


## idle-timeout (Access)

---

<b>Syntax</b>	<code>idle-timeout seconds;</code>
<b>Hierarchy Level</b>	<code>[edit access group-profile <i>profile-name</i> ppp],</code> <code>[edit access profile <i>profile-name</i> client <i>client-name</i> ppp]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	<p>Configure the idle timeout for a user. The router might consider a PPP session to be idle because of the following reasons:</p> <ul style="list-style-type: none"><li>• There is no ingress traffic on the PPP session.</li><li>• There is no egress traffic.</li><li>• There is neither ingress or egress traffic on the PPP session.</li><li>• There is no ingress or egress PPP control traffic. This is applicable only if keepalives are enabled.</li></ul>
<b>Options</b>	<p><b>seconds</b>—Number of seconds a user can remain idle before the session is terminated.</p> <p><b>Range:</b> 0 through 4,294,967,295 seconds</p> <p><b>Default:</b> 0</p>
<hr/> <div> <b>NOTE:</b> The <code>[edit access]</code> hierarchy is not available on QFabric systems.</div> <hr/>	
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Group Profile for Defining L2TP Attributes</a></li><li>• <a href="#">Configuring PPP Properties for a Client-Specific Profile</a></li><li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile on page 53</a></li></ul>



## idle-timeout (L2TP)

<b>Syntax</b>	<code>idle-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit services l2tp <a href="#">tunnel</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	Specify how long a tunnel is active after its last session is terminated. The timer starts when the session is terminated and the tunnel is disconnected when the timer expires.
<div>  <p><b>BEST PRACTICE:</b> Before you downgrade to a Junos OS Release that does not support this statement, unconfigure the statement by issuing <code>no services l2tp tunnel idle-timeout</code>.</p> </div>	
<b>Options</b>	<p><i>seconds</i>—Length of the idle timeout. A value of <b>0</b> creates a persistent tunnel; that is, the tunnel remains active indefinitely until the remote peer disconnects it or you issue the <code>clear services l2tp tunnel</code> command.</p> <p><b>Range:</b> 0 through 86,400</p> <p><b>Default:</b> 60</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Setting the L2TP Tunnel Idle Timeout on page 75</a></li> <li>• <a href="#">Configuring an L2TP LAC on page 35</a></li> <li>• <a href="#">Configuring an L2TP LNS with Inline Service Interfaces on page 51</a></li> </ul>

## inline-services (FPC Level)

---

<b>Syntax</b>	<pre>inline-services {     flow-table-size {         ipv4-flow-table-size <i>units</i>;         ipv6-flow-table-size <i>units</i>;     } }</pre>
<b>Hierarchy Level</b>	[edit chassis <b>fpc</b> <i>slot-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	Enable inline services on MPCs, configured at the FPC level. To enable inline services that are specified at the PIC level, see configuration statement <a href="#">inline-services (PIC level)</a> .
<b>Options</b>	The remaining statements are defined separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Enabling Inline Service Interfaces on page 61</a></li><li>• <a href="#">Configuring an L2TP LNS with Inline Service Interfaces on page 51</a></li><li>• <a href="#">Configuring Inline Sampling</a></li></ul>

## inline-services (PIC level)

---

<b>Syntax</b>	<pre>inline-services {     <b>bandwidth</b> (1g   10g); }</pre>
<b>Hierarchy Level</b>	[edit chassis <b>fpc</b> <i>slot-number</i> <b>pic</b> <i>number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Enable inline services on PICs residing on MPCs. To enable inline services that are specified at the fpc level, see configuration statement <a href="#">inline-services (FPC Level)</a> .  The remaining statement is explained separately.
<b>Options</b>	The option is described separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Enabling Inline Service Interfaces on page 61</a></li><li>• <a href="#">Configuring an L2TP LNS with Inline Service Interfaces on page 51</a></li></ul>

---

## interface (L2TP Service Interfaces)

---

<b>Syntax</b>	<code>interface <i>service-interface-name</i>;</code>
<b>Hierarchy Level</b>	[edit services service-device-pools <b>pool</b> <i>pool-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Specify a service interface assigned to a service interface pool. You specify more than one interface for each pool; the interfaces are used by an L2TP tunnel group to balance traffic loads.
<b>Options</b>	<i>service-interface-name</i> —Name of the service interface.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Pool of Inline Services Interfaces for Dynamic LNS Sessions on page 66</a></li><li>• <a href="#">Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64</a></li></ul>

## interface-id

---

<b>Syntax</b>	<code>interface-id <i>interface-id</i>;</code>
<b>Hierarchy Level</b>	[edit access group-profile <i>profile-name</i> l2tp], [edit access group-profile <i>profile-name</i> <b>ppp</b> ], [edit access profile <i>profile-name</i> client <i>client-name</i> ike], [edit access profile <i>profile-name</i> client <i>client-name</i> l2tp], [edit access profile <i>profile-name</i> client <i>client-name</i> ppp]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the interface identifier.
<b>Options</b>	<b><i>interface-id</i></b> —Identifier for the interface representing a Layer 2 Tunneling Protocol (L2TP) session configured at the [edit interfaces <b><i>interface-name</i></b> unit <b><i>local-unit-number</i></b> <b>dial-options</b> ] hierarchy level. For more information about the interface ID, see <i>Services Interface Naming Overview</i> .
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Group Profile for Defining L2TP Attributes</i></li><li>• <i>Configuring the Group Profile for Defining L2TP Attributes</i></li><li>• <i>Configuring L2TP Properties for a Client-Specific Profile</i></li><li>• <i>Configuring PPP Properties for a Client-Specific Profile</i></li><li>• <i>Configuring an IKE Access Profile</i></li><li>• <a href="#">Configuring an L2TP Access Profile on the LNS on page 56</a></li></ul>

## ip-reassembly

**Syntax**

```
ip-reassembly {
  profile profile-name
  rule rule-name {
    match-direction direction
  };
}
```

**Hierarchy Level** [edit services]

**Release Information** Statement introduced in Junos OS Release 13.1.

**Description** Configure the IP reassembly parameters to be applied to the L2TP server.



**NOTE:** Inline IP reassembly configuration does not require you to configure the **profile** statement. The **profile** configuration is used when IP reassembly is configured on services PICs.

**Options** **profile *profile-name***—Name of the IP reassembly profile.

The remaining statements are explained separately.

**Required Privilege Level**

interface	—To view this statement in the configuration.
interface-control	—To add this statement to the configuration.

**Related Documentation**

- [Configuring IP Inline Reassembly for L2TP on page 61](#)
- [IP Packet Fragment Reassembly for L2TP Overview on page 26](#)

## ip-reassembly-rules (Service Set)

---

<b>Syntax</b>	<code>ip-reassembly-rules <i>rule-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services service-set<i>service-set-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 13.1.
<b>Description</b>	Specify one or more previously configured IP reassembly rules to associate with the service set.




**NOTE:** The IP reassembly rule must be defined at the `[edit services ip-reassembly rule]` hierarchy level.

---

<b>Options</b>	<i>rule-name</i> —Name of an IP reassembly rule.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring IP Inline Reassembly for L2TP on page 61</a></li><li>• <a href="#">IP Packet Fragment Reassembly for L2TP Overview on page 26</a></li></ul>

## ip-reassembly (L2TP)

---

<b>Syntax</b>	ip-reassembly { service-set <i>service-set-name</i> ; }
<b>Hierarchy Level</b>	[edit services <a href="#">l2tp</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.1.
<b>Description</b>	Associate the reassembly service-set with the L2TP service.
<div>  <b>NOTE:</b> The service set must be defined at the [edit services] hierarchy level. </div>	
<b>Options</b>	<b>service-set <i>service-set-name</i></b> —Identifies the service set to be associated with the L2TP service.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">IP Packet Fragment Reassembly for L2TP Overview on page 26</a></li> <li>• <a href="#">Configuring IP Inline Reassembly for L2TP on page 61</a></li> </ul>

## keepalive

---

<b>Syntax</b>	<code>keepalive seconds;</code>
<b>Hierarchy Level</b>	[edit access group-profile <i>profile-name</i> <b>ppp</b> ], [edit access profile <i>profile-name</i> client <i>client-name</i> ppp]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the keepalive interval for an L2TP tunnel.
<b>Options</b>	<p><b>seconds</b>—Time period that must elapse before the Junos OS checks the status of the Point-to-Point Protocol (PPP) session by sending an echo request to the peer.</p> <p>For L2TP on MX Series routers, the minimum recommended interval is 30 seconds. A value of 0 disables generation of keepalive messages from the LNS.</p> <p><b>Range:</b> 0 through 32,767 seconds</p> <p><b>Default:</b> 30 seconds</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Group Profile for Defining L2TP Attributes</a></li><li>• <a href="#">Configuring PPP Properties for a Client-Specific Profile</a></li><li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile on page 53</a></li></ul>



## keepalives

<b>Syntax</b>	<code>keepalives &lt;interval seconds&gt; &lt;down-count number&gt; &lt;up-count number&gt;;</code>
<b>Hierarchy Level</b>	<code>[edit interfaces <i>interface-name</i>],</code> <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Enable the sending of keepalives on a physical interface configured with PPP, Frame Relay, or Cisco HDLC encapsulation.</p> <p>For ATM2 IQ interfaces only, you can enable keepalives on a logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:</p> <ul style="list-style-type: none"> <li>• <b>atm-ppp-llc</b>—PPP over AAL5 LLC encapsulation.</li> <li>• <b>atm-ppp-vc-mux</b>—PPP over AAL5 multiplex encapsulation.</li> </ul>
<b>Default</b>	Sending of keepalives is enabled by default. The default keepalive interval is 10 seconds for PPP, Frame Relay, or Cisco HDLC. The default down-count is 3 and the default up-count is 1 for PPP or Cisco HDLC.
<b>Options</b>	<p><b>down-count <i>number</i></b>—The number of keepalive packets a destination must fail to receive before the network takes down a link.</p> <p><b>Range:</b> 1 through 255</p> <p><b>Default:</b> 3</p> <p><b>interval <i>seconds</i></b>—The time in seconds between successive keepalive requests.</p> <p><b>Range:</b> 1 through 32767 seconds</p> <p><b>Default:</b> 10 seconds</p> <p><b>up-count <i>number</i></b>—The number of keepalive packets a destination must receive to change a link's status from down to up.</p> <p><b>Range:</b> 1 through 255</p> <p><b>Default:</b> 1</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Keepalives</a></li> <li>• <a href="#">Configuring Frame Relay Keepalives</a></li> <li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface on page 54</a></li> </ul>

## keepalives (Dynamic Profiles)

---

<b>Syntax</b>	<pre>keepalives {     interval <i>seconds</i>; }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit <i>logical-unit-number</i> ] [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit"] [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit"]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Support at the [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit"] hierarchy level introduced in Junos OS Release 10.1. Support at the [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit"] hierarchy level introduced in Junos OS Release 12.2.
<b>Description</b>	Specify the keepalive interval in a PPP dynamic profile.
<b>Default</b>	Sending of keepalives is enabled by default.
<b>Options</b>	<b>interval <i>seconds</i></b> —The time in seconds between successive keepalive requests. <b>Range:</b> 1 through 32767 seconds <b>Default:</b> 30 seconds for LNS-based PPP sessions. 10 seconds for all other PPP sessions.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Dynamic Profiles Overview</i></li><li>• <i>Configuring Dynamic Authentication for PPP Subscribers</i></li><li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface on page 54</a></li></ul>

## l2tp

```

Syntax  l2tp {
    destination [ip-address] {
        access-line-information <connection-speed-update>;
        lockout-timeout seconds;
    }
    destruct-timeout seconds;
    disable-calling-number-avp;
    disable-failover-protocol;
    enable-snmp-tunnel-statistics;
    failover-within-preference;
    ip-reassembly;
    rx-connect-speed-when-equal;
    traceoptions {
        debug-level level;
        file filename <files number> <match regular-expression > <size maximum-file-size>
            <world-readable | no-world-readable>;
        filter {
            protocol name;
            user user@domain;
            user-name username;
        }
        flag flag;
        interfaces interface-name {
            debug-level severity;
            flag flag;
        }
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
    tunnel {
        assignment-id-format (assignment-id | client-server-id);
        idle-timeout seconds;
        minimum-retransmission-timeout;
        nas-port-method;
        retransmission-count-established count;
        retransmission-count-not-established count;
        rx-window-size packets;
        tx-address-change (accept | ignore | ignore-ip-address | ignore-udp-port);
    }
    tunnel-group group-name {
        aaa-access-profile profile-name;
        dynamic-profile profile-name;
        hello-interval seconds;
        hide-avps;
        l2tp-access-profile profile-name;
        local-gateway address {
            address address;
            gateway-name gateway-name;
        }
        maximum-send-window packets;
        ppp-access-profile profile-name;
        receive-window packets;
    }
}

```

```

retransmit-interval seconds;
service-device-pool pool-name;
service-interface interface-name;
syslog {
    host hostname {
        facility-override facility-name;
        log-prefix prefix-value;
        services severity-level;
    }
}
tos-reflect;
tunnel-switch-profile profile-name;
tunnel-timeout seconds;
}
tunnel-switch-profile profile-name;
tx-connect-speed-method method;
weighted-load-balancing;
}

```

**Hierarchy Level** [edit services]

**Release Information** Statement introduced before Junos OS Release 7.4.  
 Support for LAC on MX Series routers introduced in Junos OS Release 10.4.  
 Support for LNS on MX Series routers introduced in Junos OS Release 11.4.

**Description** Configure L2TP services to establish PPP tunnels across a network.  
 The remaining statements are explained separately.



**NOTE:** Subordinate statement support depends on the platform. See individual statement topics for more detailed support information.

**Required Privilege Level** interface—To view this statement in the configuration.  
 interface-control—To add this statement to the configuration.


**Related Documentation**

- [Layer 2 Tunneling Protocol Overview](#)
- [L2TP for Subscriber Access Overview on page 3](#)

## l2tp-access-profile

<b>Syntax</b>	<code>l2tp-access-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services l2tp <a href="#">tunnel-group name</a>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the profile used to validate all L2TP connection requests to the local gateway address.
<b>Options</b>	<i>profile-name</i> —Identifier for the L2TP connection profile.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Access Profiles for L2TP Tunnel Groups</a></li> <li>• <a href="#">Configuring an L2TP Access Profile on the LNS on page 56</a></li> </ul>

## lcp-renegotiation


<b>Syntax</b>	<code>lcp-renegotiation;</code>
<b>Hierarchy Level</b>	<code>[edit access group-profile <i>profile-name</i> l2tp],</code> <code>[edit access profile <i>profile-name</i> client <i>client-name</i> l2tp]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the L2TP network server (LNS) so it renegotiates the link control protocol (LCP) with the PPP client. When LCP renegotiation is disabled, LNS uses the pre-negotiated LCP parameters between the L2TP access concentrator (LAC) and PPP client to set up the session. When LCP renegotiation is enabled, authentication is also renegotiated.
<div style="display: flex; align-items: center;">  <div> <p><b>NOTE:</b> This statement is not supported at the <code>[edit access group-profile l2tp]</code> hierarchy level for L2TP LNS on MX Series routers.</p> </div> </div>	
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Group Profile for Defining L2TP Attributes</a></li> <li>• <a href="#">Configuring L2TP Properties for a Client-Specific Profile</a></li> <li>• <a href="#">Configuring an L2TP Access Profile on the LNS on page 56</a></li> </ul>

## local-gateway (L2TP LNS)

---

<b>Syntax</b>	<pre>local-gateway {     address address;     gateway-name gateway-name; }</pre>
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group name</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Specify the IP address or name for the local (LNS) gateway for L2TP tunnel.</p> <p>The remaining statements are explained separately.</p>
<b>Options</b>	<b>address</b> —Local IP address; corresponds to the IP address that is used by LACs to identify the LNS. When the LAC is an MX Series router, this address matches the remote gateway address configured in the LAC tunnel profile.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Local Gateway Address and PIC.</i></li><li>• <i>Configuring L2TP Tunnel Groups</i></li><li>• <a href="#">Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64</a></li></ul>

## lockout-timeout (L2TP Destination Lockout)

<b>Syntax</b>	<code>lockout-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit services l2tp <a href="#">destination</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2.
<b>Description</b>	Set the duration of the timeout period for which all future destinations are locked out, meaning that they are not considered for selection when a new tunnel is created. Destinations are locked out when L2TP cannot connect to the destination during the tunnel selection process. This statement does not affect destinations that are currently locked out.
<div>  <b>NOTE:</b> The <i>ip-address</i> option for the <i>destination</i> statement does not apply to the <i>lockout-timeout</i> statement. </div>	
<b>Options</b>	<p><b><i>seconds</i></b>—Length of the period during which the destination is locked out.</p> <p><b>Range:</b> 60 through 3600 seconds</p> <p><b>Default:</b> 300 seconds</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the L2TP Destination Lockout Timeout on page 69</a></li> <li>• <a href="#">Configuring an L2TP LNS with Inline Service Interfaces on page 51</a></li> </ul>

## logical-system (Tunnel Profile)

---

<b>Syntax</b>	<code>logical-system <i>logical-system-name</i>;</code>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> <b>tunnel</b> <i>tunnel-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify a logical system for a tunnel. When you specify a logical system, you must also specify a routing instance.
<b>Options</b>	<b><i>logical-system-name</i></b> — Name of the logical system. <b>Default:</b> Logical system <i>default</i>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li></ul>

## match-direction (IP Reassembly Rule)

---

<b>Syntax</b>	<code>match-direction <i>direction</i></code>
<b>Hierarchy Level</b>	[edit services <b>ip-reassembly</b> <i>rule</i> <i>rule-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.1.
<b>Description</b>	Configure the direction in which the IP reassembly rule matching is applied. The match direction is used with respect to the traffic flow through the inline services interface. You must configure a match direction for an IP reassembly rule.
<b>Options</b>	<b><i>direction</i></b> —Match direction. For inline IP reassembly, <b>input</b> is the only match direction supported.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring IP Inline Reassembly for L2TP on page 61</a></li><li>• <a href="#">IP Packet Fragment Reassembly for L2TP Overview on page 26</a></li></ul>



## maximum-sessions-per-tunnel

<b>Syntax</b>	<code>maximum-sessions-per-tunnel <i>number</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access group-profile l2tp],</code> <code>[edit access profile <i>profile-name</i> client <i>client-name</i> l2tp]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the maximum sessions for a Layer 2 tunnel.



**NOTE:** This statement is not supported at the `[edit access group-profile l2tp]` hierarchy level for L2TP LNS on MX Series routers.

<b>Options</b>	<i>number</i> —Maximum number of sessions for a Layer 2 tunnel.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Group Profile for Defining L2TP Attributes</a></li> <li>• <a href="#">Configuring L2TP Properties for a Client-Specific Profile</a></li> <li>• <a href="#">Configuring an L2TP Access Profile on the LNS on page 56</a></li> </ul>

## max-sessions (Tunnel Profile)

<b>Syntax</b>	<code>max-sessions <i>number</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access tunnel-profile <i>profile-name</i> <b>tunnel</b> <i>tunnel-id</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the maximum number of sessions allowed in the tunnel.
<b>Options</b>	<i>number</i> —Maximum number of sessions allowed in the tunnel. <b>Range:</b> 0 through 60,000 <b>Default:</b> 0
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li> </ul>

## medium (Tunnel Profile)

---

<b>Syntax</b>	<code>medium type;</code>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> <b>tunnel</b> <i>tunnel-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the medium type for the tunnel.
<b>Default</b>	<code>ipv4</code>
<b>Options</b>	<b>type</b> —Medium type for the tunnel. The only value currently available is <code>ipv4</code> .
<b>Required Privilege Level</b>	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li></ul>

## minimum-retransmission-timeout (L2TP Tunnel)

---

<b>Syntax</b>	<code>minimum-retransmission-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	Configure the minimum (initial) interval that the LAC or the LNS waits for a response after transmitting an L2TP control message to a peer. If no response has been received by the time the period expires, the message is retransmitted. The timeout period is doubled for each retransmission until the maximum of 16 seconds is reached.
<b>Options</b>	<b>seconds</b> —Minimum interval before initial retransmission. <b>Range:</b> 1, 2, 4, 8, or 16 seconds <b>Default:</b> 1
<b>Required Privilege Level</b>	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Retransmission Attributes for L2TP Control Messages on page 73</a></li><li>• <a href="#">Configuring an L2TP LAC on page 35</a></li><li>• <a href="#">Configuring an L2TP LNS with Inline Service Interfaces on page 51</a></li></ul>

## nas-port-method (L2TP LAC)

<b>Syntax</b>	nas-port-method cisco-avp;
<b>Hierarchy Level</b>	[edit services l2tp <a href="#">tunnel</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	Globally configure the LAC to interoperate with Cisco LNS devices by including the Cisco NAS Port Info AVP (100) in the ICRQ to the LNS. This AVP conveys the physical NAS port number identifier and the type of the physical port, such as Ethernet or ATM.




**NOTE:** This global configuration can be overridden by the configuration in a tunnel profile or by the RADIUS configuration.

<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Globally Configuring the LAC to Interoperate with Cisco LNS Devices on page 47</a></li> <li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li> <li>• <a href="#">LAC Interoperation with Third-Party LNS Devices on page 17</a></li> </ul>

## nas-port-method (Tunnel Profile)

<b>Syntax</b>	nas-port-method cisco-avp;
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> <a href="#">tunnel</a> <i>tunnel-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2.
<b>Description</b>	Configure the LAC to interoperate with Cisco LNS devices by including the Cisco NAS Port Info AVP (100) in the ICRQ to the LNS. This AVP conveys the physical NAS port number identifier and the type of the physical port, such as Ethernet or ATM.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li> </ul>

## next-hop-service

<b>Syntax</b>	<pre> next-hop-service {   inside-service-interface <i>interface-name.unit-number</i>;   outside-service-interface <i>interface-name.unit-number</i>;   outside-service-interface-type local;   service-interface-pool <i>name</i>; } </pre>
<b>Hierarchy Level</b>	[edit services service-set <i>service-set-name</i> ]
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p><b>service-interface-pool</b> option added in Junos OS Release 9.3.</p>
<b>Description</b>	Specify interface names or a service interface pool for the forwarding next-hop service set. You cannot specify both a service interface pool and an inside or outside interface.
<b>Options</b>	<p><b>inside-service-interface <i>interface-name.unit-number</i></b>—Name and logical unit number of the service interface associated with the service set applied inside the network.</p> <p><b>outside-service-interface <i>interface-name.unit-number</i></b>—Name and logical unit number of the service interface associated with the service set applied outside the network.</p> <p><b>outside-service-interface-type <i>interface-type</i></b>—Identifies the interface type of the service interface associated with the service set applied outside the network. For inline IP reassembly, set the interface type to local.</p> <p><b>service-interface-pool <i>name</i></b>—Name of the pool of logical interfaces configured at the [edit services service-interface-pools pool <i>pool-name</i>] hierarchy level. You can configure a service interface pool only if the service set has a PGCP rule configured. The service set cannot contain any other type of rule.</p>
<div>  <p><b>NOTE:</b> <b>service-interface-pool</b> is not applicable for IP reassembly configuration on L2TP.</p> </div>	
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring Service Sets to be Applied to Services Interfaces</i></li> </ul>

## pap

<b>Syntax</b>	<pre>pap {   access-profile <i>name</i>;   default-pap-password <i>password</i>;   local-name <i>name</i>;   local-password <i>password</i>;   passive; }</pre>
<b>Hierarchy Level</b>	<pre>[edit interfaces <i>interface-name</i> <b>ppp-options</b>], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <b>ppp-options</b>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <b>ppp-options</b>]</pre>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	<p>Configure the Password Authentication Protocol (PAP). Use PAP authentication as a means to provide a simple method for the peer to establish its identity using a two-way handshake. This is done only upon initial link establishment.</p> <p>After the link is established, an ID and password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.</p>



**BEST PRACTICE:** On inline service (si) interfaces for L2TP, only the **pap** statement itself is typically used for subscriber management. We recommend that you leave the subordinate statements at their default values.

The remaining statements are explained separately.

<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring the PPP Challenge Handshake Authentication Protocol</i></li> <li>• <i>Configuring PPP PAP Authentication</i></li> <li>• <i>Tracing Operations of the pppd Process</i></li> <li>• <i>traceoptions (PPP Process)</i></li> <li>• <i>Example: Configuring PAP for an L2TP Profile</i></li> <li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface on page 54</a></li> </ul>

## pap (Dynamic PPP)

---

<b>Syntax</b>	<code>pap;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" <a href="#">ppp-options</a> ], [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit" <a href="#">ppp-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Support at the [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit" <a href="#">ppp-options</a> ] hierarchy level introduced in Junos OS Release 12.2.
<b>Description</b>	Specify PAP authentication in a PPP dynamic profile.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Dynamic Profiles Overview</i></li><li>• <i>Configuring Dynamic Authentication for PPP Subscribers</i></li><li>• <i>Attaching Dynamic Profiles to Static PPP Subscriber Interfaces</i></li><li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface on page 54</a></li></ul>

## pap (L2TP)

---

<b>Syntax</b>	<code>pap;</code>
<b>Hierarchy Level</b>	[edit access group-profile <i>profile-name</i> ppp <a href="#">ppp-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	(MX Series routers only) Specify PAP authentication for PPP subscribers in an L2TP LNS user group profile.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile on page 53</a></li></ul>

## pic (M Series and T Series Routers)

```
Syntax  pic pic-number {
        cel {
            ei port-number {
                channel-group group-number timeslots slot-number;
            }
        }
        ct3 {
            port port-number {
                t1 link-number {
                    channel-group group-number timeslots slot-number;
                }
            }
        }
        framing (sdh | sonet);
        idle-cell format {
            itu-t;
            payload-pattern payload-pattern-byte;
        }
        inline-services {
            bandwidth (1g | 10g);
        }
        max-queues-per-interface (8 | 4);
        no-concatenate;
    }
```

**Hierarchy Level** [edit chassis fpc *slot-number*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Configure properties for an individual PIC.

**Options** *pic-number*—Slot number in which the PIC is installed.  
**Range:** 0 through 3

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
 interface-control—To add this statement to the configuration.

**Related Documentation**

- *Configuring the Junos OS to Enable SONET/SDH Framing for SONET/SDH PICs*
- *Configuring the Junos OS to Enable a SONET PIC to Operate in Channelized (Multiplexed) Mode*
- *Configuring the Junos OS to Support Channelized DS3-to-DS0 Naming for Channel Groups and Time Slots*
- *Configuring the Junos OS to Support Channel Groups and Time Slots for Channelized E1 PICs*
- [Enabling Inline Service Interfaces on page 61](#)

## pool (L2TP Service Interfaces)

---

<b>Syntax</b>	<code>pool <i>pool-name</i> {     interface <i>service-interface-name</i>; }</code>
<b>Hierarchy Level</b>	[edit services <a href="#">service-device-pools</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Define a pool of service interfaces that can be assigned to an L2TP tunnel group for traffic load-balancing. The service device pool is required for dynamic LNS sessions.
<b>Options</b>	<p><i>pool-name</i>—Name of the service interface pool.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Pool of Inline Services Interfaces for Dynamic LNS Sessions on page 66</a></li></ul>



## ppp (Group Profile)

**Syntax**

```
ppp {
  cell-overhead;
  encapsulation-overhead bytes;
  framed-pool framed-pool;
  idle-timeout seconds;
  interface-id interface-id;
  keepalive seconds;
  ppp-options {
    chap;
    pap;
  }
  primary-dns primary-dns;
  primary-wins primary-wins;
  secondary-dns secondary-dns;
  secondary-wins secondary-wins;
}
```

**Hierarchy Level** [edit access [group-profile](#) *profile-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Configure PPP properties for a group profile.

The remaining statements are explained separately.



**NOTE:** Subordinate statement support depends on the platform. See individual statement topics for more detailed support information.

**Required Privilege Level**

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring the Group Profile for Defining L2TP Attributes](#)
- [Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile on page 53](#)

## ppp-options

<b>Syntax</b>	<pre> ppp-options {   authentication [ <i>authentication-protocols</i> ];   chap {     access-profile <i>name</i>;     challenge-length minimum <i>minimum-length</i> maximum <i>maximum-length</i>;     default-chap-secret <i>name</i>;     local-name <i>name</i>;     passive;   }   compression {     acfc;     pfc;   }   dynamic-profile <i>profile-name</i>;   initiate-ncp (ip   ipv6   dual-stack-passive)   lcp-max-conf-req <i>number</i>   lcp-restart-timer <i>milliseconds</i>;   loopback-clear-timer <i>seconds</i>;   ncp-max-conf-req <i>number</i>   ncp-restart-timer <i>milliseconds</i>;   on-demand-ip-address   pap {     access-profile <i>name</i>;     default-pap-password <i>password</i>;     local-name <i>name</i>;     local-password <i>password</i>;     passive;   } } </pre>
<b>Hierarchy Level</b>	<pre> [edit interfaces <i>interface-name</i>], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>] </pre>

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** On interfaces with PPP encapsulation, configure PPP-specific interface properties.

For ATM2 IQ interfaces only, you can configure CHAP on the logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:

- **atm-ppp-llc**—PPP over AAL5 LLC encapsulation.
- **atm-ppp-vc-mux**—PPP over AAL5 multiplex encapsulation.



**BEST PRACTICE:** On inline service (si) interfaces for L2TP, only the **chap** and **pap** statements are typically used for subscriber management. We recommend that you leave the other statements subordinate to

ppp-options—including those subordinate to chap and pap—at their default values.

The remaining statements are explained separately.

<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the PPP Challenge Handshake Authentication Protocol</a></li> <li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface on page 54</a></li> </ul>

## ppp-options (Dynamic PPP)

<b>Syntax</b>	<pre>ppp-options {   authentication [ authentication-protocols ];   chap {     challenge-length minimum <i>minimum-length</i> maximum <i>maximum-length</i>;   }   initiate-ncp (ip   ipv6   dual-stack-passive)   on-demand-ip-address;   pap; }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit"], [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit"]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Support at the [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit"] hierarchy level introduced in Junos OS Release 12.2.
<b>Description</b>	Configure PPP-specific interface properties in a dynamic profile.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Dynamic Profiles Overview</a></li> <li>• <a href="#">Configuring Dynamic Authentication for PPP Subscribers</a></li> <li>• <a href="#">Attaching Dynamic Profiles to Static PPP Subscriber Interfaces</a></li> <li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface on page 54</a></li> </ul>

## ppp-options (L2TP)

---

<b>Syntax</b>	<pre>ppp-options {     chap;     initiate-ncp (ip   ipv6   dual-stack-passive)     pap; }</pre>
<b>Hierarchy Level</b>	[edit access group-profile <i>profile-name</i> <b>ppp</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	<p>Configure PPP-specific properties in a group profile that applies to tunneled PPP subscribers at the LNS.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Group Profile for Defining L2TP Attributes</a></li><li>• <a href="#">Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile on page 53</a></li></ul>

## preference (Tunnel Profile)

---

<b>Syntax</b>	<pre>preference <i>number</i>;</pre>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> <b>tunnel</b> <i>tunnel-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	<p>Specify the preference for a tunnel. You can specify up to 8 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.</p> <p>This value can be overridden by RADIUS attribute Tunnel-Preference [83].</p>
<b>Options</b>	<p><b>number</b>—Number that indicates the order in which the router attempts to connect to the destination. Zero is the highest level of preference.</p> <p><b>Range:</b> 0 through 2000</p> <p><b>Default:</b> 2000</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li></ul>

---

## remote-gateway (Tunnel Profile)

---

<b>Syntax</b>	<pre>remote-gateway {     address <i>server-ip-address</i>;     gateway-name <i>server-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> <b>tunnel</b> <i>tunnel-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	<p>Specify the IP address and hostname of the remote gateway at the L2TP tunnel endpoint, the LNS.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li></ul>

## request services l2tp destination unlock

---

<b>Syntax</b>	<b>request services l2tp destination unlock</b> <i>destination-name</i>
<b>Release Information</b>	Command introduced in Junos OS Release 13.2.
<b>Description</b>	Remove the specified destination from the destination lockout list immediately, before its lockout period expires. As a result, the L2TP process can again consider the destination during the selection of new tunnels.
<b>Options</b>	<i>destination-name</i> —Name of the destination to be unlocked.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Removing an L2TP Destination from the Destination Lockout List on page 69</a></li><li>• <a href="#">Configuring the L2TP Destination Lockout Timeout on page 69</a></li><li>• <a href="#">show services l2tp destination lockout on page 219</a></li></ul>
<b>List of Sample Output</b>	<a href="#">request services l2tp destination unlock on page 148</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

### Sample Output

#### request services l2tp destination unlock

```
user@host> request services l2tp destination unlock dest-a
Destination dest-a unlocked
```

## retransmission-count-established (L2TP)

<b>Syntax</b>	<code>retransmission-count-established <i>count</i>;</code>
<b>Hierarchy Level</b>	[edit services l2tp <a href="#">tunnel</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	Set the maximum number of times control messages are retransmitted for established tunnels.




**BEST PRACTICE:** Before you downgrade to a Junos OS Release that does not support this statement, unconfigure the statement by issuing `no services l2tp tunnel retransmission-count-established`.

<b>Options</b>	<i>count</i> —Number of retransmissions. <b>Range:</b> 2 through 30 <b>Default:</b> 7
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Retransmission Attributes for L2TP Control Messages on page 73</a></li> <li>• <a href="#">Configuring an L2TP LAC on page 35</a></li> <li>• <a href="#">Configuring an L2TP LNS with Inline Service Interfaces on page 51</a></li> </ul>

## retransmission-count-not-established (L2TP)

---

<b>Syntax</b>	<code>retransmission-count-not-established</code> <i>count</i> ;
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	Set the maximum number of times control messages are retransmitted for tunnels that are not established.
<div> <b>BEST PRACTICE:</b> Before you downgrade to a Junos OS Release that does not support this statement, unconfigure the statement by issuing <code>no services l2tp tunnel retransmission-count-not-established</code>.</div>	
<b>Options</b>	<i>count</i> —Number of retransmissions. <b>Range:</b> 2 through 30 <b>Default:</b> 5
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Retransmission Attributes for L2TP Control Messages on page 73</a></li><li>• <a href="#">Configuring an L2TP LAC on page 35</a></li><li>• <a href="#">Configuring an L2TP LNS with Inline Service Interfaces on page 51</a></li></ul>



## routing-instance (Tunnel Profile)

---

<b>Syntax</b>	<code>routing-instance</code> <i>routing-instance-name</i> ;
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> <b>tunnel</b> <i>tunnel-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify a routing instance for a tunnel.
<b>Options</b>	<i>routing-instance-name</i> —Name of the routing instance. <b>Default:</b> Routing instance <i>default</i>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li></ul>



## rule (IP Reassembly)

<b>Syntax</b>	<code>rule <i>rule-name</i> {     <code>match-direction</code> <i>direction</i>; }</code>
<b>Hierarchy Level</b>	[edit services <code>ip-reassembly</code> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.1.
<b>Description</b>	Configure an IP reassembly rule, which is used for inline IP reassembly on the inline services interface. The IP reassembly rule can be attached to a service set to indicate that the service set is of type IP reassembly. For inline IP reassembly, each rule must include the <code>match-direction</code> statement, which specifies the direction in which the match is applied.
<div>  <p><b>NOTE:</b> If you configure an IP reassembly rule, then you must configure the <code>match-direction</code> statement.</p> </div>	
<b>Options</b>	<p><b><i>rule-name</i></b>—Name of the IP reassembly rule.</p> <p><b>Range:</b> Up to 63 characters</p> <p>The remaining statement is explained separately.</p>
<div>  <p><b>NOTE:</b> To create more than one IP reassembly rule, include the rule statement multiple times.</p> </div>	
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring IP Inline Reassembly for L2TP on page 61</a></li> <li>• <a href="#">IP Packet Fragment Reassembly for L2TP Overview on page 26</a></li> </ul>

## rx-connect-speed-when-equal (L2TP LAC)

---

<b>Syntax</b>	rx-connect-speed-when-equal
<b>Hierarchy Level</b>	[edit services l2tp]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.1.
<b>Description</b>	Enable sending the receive connect speed, which is represented by AVP 38, even when its value is equal to that of the transmit connect speed, which is represented by AVP 24. By default, AVP 38 is sent from the LAC to the LNS during the establishment of an L2TP tunnel session, only when its value is different from AVP 24. You can override the default setting with this configuration statement.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Method to Set the LAC Connection Speeds to the LNS on page 42</a></li><li>• <a href="#">Transmission of the Receive Connect Speed AVP When Transmit and Receive Connect Speeds are Equal on page 44</a></li></ul>

## rx-window-size (L2TP)

---

<b>Syntax</b>	rx-window-size <i>packets</i> ;
<b>Hierarchy Level</b>	[edit services l2tp <a href="#">tunnel</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3.
<b>Description</b>	Configure the L2TP receive window size for an L2TP tunnel.
<b>Options</b>	<p><i>packets</i>—Number of packets that a peer can transmit without receiving an acknowledgment from the router. By default, this value is set to 4 packets. If the receive window size is configured to its default value, the router does not send the Receive Window Size AVP (AVP 10) in the first tunnel negotiation packet that is sent to its peer.</p> <p><b>Range:</b> 4 through 128</p> <p><b>Default:</b> 4</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Setting the L2TP Receive Window Size on page 76</a></li><li>• <a href="#">Configuring an L2TP LAC on page 35</a></li><li>• <a href="#">Configuring an L2TP LNS with Inline Service Interfaces on page 51</a></li></ul>

## secret (Tunnel Profile)

<b>Syntax</b>	<code>secret <i>password</i>;</code>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> <b>tunnel</b> <i>tunnel-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the tunnel password sent to the LNS for authentication.
<b>Options</b>	<i>password</i> —Cleartext password.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li> </ul>

## service-device-pool (L2TP)

<b>Syntax</b>	<code>service-device-pool <i>pool-name</i>;</code>
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group</b> <i>name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Assign a pool of service interfaces to the tunnel group to balance traffic across.



**NOTE:** The service interface configuration is required for static LNS sessions. Either the service interface configuration or the service device pool configuration can be used for dynamic LNS sessions.


<b>Options</b>	<i>pool-name</i> —Name of the service device pool.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64</a></li> </ul>

## service-device-pools (L2TP Service Interfaces)

---

<b>Syntax</b>	<pre>service-device-pools {     pool <i>pool-name</i> {         interface <i>service-interface-name</i>;     } }</pre>
<b>Hierarchy Level</b>	[edit services]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Configure one or more pools of service interfaces that can be assigned to an L2TP tunnel group for traffic load-balancing. The service device pool is required for dynamic LNS sessions.
<b>Options</b>	<p><i>pool-name</i>—Name of the service interface pool.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Pool of Inline Services Interfaces for Dynamic LNS Sessions on page 66</a></li></ul>

## service-interface

<b>Syntax</b>	<code>service-interface <i>interface-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services l2tp <b>tunnel-group</b> <i>name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Option <b>si-fpc/pic/port</b> introduced in Junos OS Release 11.4.
<b>Description</b>	Specify the service interface responsible for handling L2TP processing.
<div>  <p><b>NOTE:</b> On MX Series routers, the service interface configuration is required for static LNS sessions. Either the service interface configuration or the service device pool configuration can be used for dynamic LNS sessions.</p> </div>	
<b>Options</b>	<p><b>interface-name</b>—Name of the service interface. The interface type depends on the line card as follows:</p> <ul style="list-style-type: none"> <li>• <b>sp-fpc/pic/port</b>—On AS or Multiservices PICs on M7i, M10i, and M120 routers.</li> <li>• <b>si-fpc/pic/port</b>—On MPCs on MX Series routers.</li> </ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Local Gateway Address and PIC</a></li> <li>• <a href="#">Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64</a></li> </ul>

## shared-secret

<b>Syntax</b>	<code>shared-secret <i>shared-secret</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access profile <i>profile-name</i> client <i>client-name</i> l2tp]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Configure the shared secret.
<b>Options</b>	<b>shared-secret</b> —Shared secret key for authenticating the peer.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring L2TP Properties for a Client-Specific Profile</a></li> <li>• <a href="#">Configuring an L2TP Access Profile on the LNS on page 56</a></li> </ul>

## source-gateway (Tunnel Profile)

---

<b>Syntax</b>	<pre>source-gateway {     address <i>client-ip-address</i>;     gateway-name <i>client-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> <b>tunnel</b> <i>tunnel-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	<p>Specify the IP address and hostname of the source gateway at the local L2TP tunnel endpoint, the LAC.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li></ul>

## tos-reflect (L2TP)

---

<b>Syntax</b>	<pre>tos-reflect;</pre>
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group</b> <i>name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	<p>Configure the LNS to reflect the IP ToS value in the inner IP header to the outer IP header. When CoS rewrite rules are also configured ([edit class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> rewrite-rules]), the rewrite is performed only on the inner IP ToS; the outer IP TOS value is not affected.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Access Profiles for L2TP Tunnel Groups</a></li><li>• <a href="#">Configuring Dynamic CoS for an L2TP LNS Inline Service</a></li></ul>

## traceoptions (L2TP)

<b>Syntax</b>	<pre> traceoptions {   debug-level <i>level</i>;   file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;   filter {     protocol <i>name</i>;     user <i>user@domain</i>;     user-name <i>username</i>;   }   flag <i>flag</i>;   interfaces <i>interface-name</i> {     debug-level <i>level</i>;     flag <i>flag</i>;   }   level (all   error   info   notice   verbose   warning);   no-remote-trace; } </pre>
<b>Hierarchy Level</b>	[edit services <a href="#">l2tp</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define tracing operations for L2TP processes.
<b>Options</b>	<p><b>debug-level <i>level</i></b>—Trace level for PPP, L2TP, RADIUS, and UDP; this option does not apply to L2TP on MX Series routers:</p> <p><b>debug-level <i>level</i></b>—Trace level for PPP, L2TP, RADIUS, and UDP; this option does not apply to L2TP on MX Series routers:</p> <ul style="list-style-type: none"> <li><b>detail</b>—Trace detailed debug information.</li> <li><b>error</b>—Trace error information.</li> <li><b>packet-dump</b>—Trace packet decoding information.</li> </ul> <p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory <code>/var/log</code>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>filter</b>—Additional filter to refine the output to display particular subscribers. Filtering based on the following subscriber identifiers simplifies troubleshooting in a scaled environment.</p>

**filter**—Additional filter to refine the output to display particular subscribers. Filtering based on the following subscriber identifiers simplifies troubleshooting in a scaled environment.

- **protocol *name***—One of the following protocols; this option does not apply to L2TP on MX Series routers:

**protocol *name***—One of the following protocols; this option does not apply to L2TP on MX Series routers:

- **l2tp**
- **ppp**
- **radius**
- **udp**
- **user *user@domain***—Username of a subscriber; this option does not apply to L2TP on M Series routers. Optionally use an asterisk (\*) as a wildcard to substitute for characters at the beginning or end of either term or both terms.
- **user-name *username***—Username of a subscriber; this option does not apply to L2TP on MX Series routers.



**flag flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

**flag flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **configuration**—Trace configuration events.
- **events**—Trace interface events.
- **general**—Trace general events.
- **gres**—Trace GRES events.
- **init**—Trace daemon initialization.
- **ipc-rx**—Trace IPC receive events.
- **ipc-tx**—Trace IPC transmit events.
- **memory**—Trace memory management code.
- **message**—Trace message processing code.
- **packet-error**—Trace packet error events.
- **parse**—Trace parsing events.
- **protocol**—Trace L2TP events.
- **receive-packets**—Trace received L2TP packets.
- **routing-process**—Trace routing process interactions.
- **routing-socket**—Trace routing socket events.
- **session-db**—Trace session database interactions.
- **states**—Trace state machine events.
- **timer**—Trace timer events.
- **transmit-packets**—Trace transmitted L2TP packets.
- **tunnel**—Trace tunnel events.

**interfaces *interface-name***—Apply L2TP traceoptions to a specific services interface. This option does not apply to L2TP on MX Series routers.

**interfaces *interface-name***—Apply L2TP traceoptions to a specific services interface. This option does not apply to L2TP on MX Series routers.

- **debug-level *level***—Trace level for the interface; this option does not apply to L2TP on MX Series routers:
  - **detail**—Trace detailed debug information.
  - **error**—Trace error information.
  - **extensive**—Trace all PIC debug information.
- **flag *flag***—Tracing operation to perform for the interface. This option does not apply to L2TP on MX Series routers. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:
  - **all**—Trace everything.
  - **ipc**—Trace L2TP Inter-Process Communication (IPC) messages between the PIC and the Routing Engine.
  - **packet-dump**—Dump each packet content based on debug level.
  - **protocol**—Trace L2TP, PPP, and multilink handling.
  - **system**—Trace packet processing on the PIC.

**level**—Specify level of tracing to perform. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

**level**—Specify level of tracing to perform. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

- **all**—Match messages of all levels.
- **error**—Match error messages.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure **verbose**, messages at all higher levels are traced. Therefore, the result is the same as when you configure **all**.
- **warning**—Match warning messages.

**Default:** error

**match *regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

**no-remote-trace**—Disable remote tracing.

**no-world-readable**—(Optional) Disable unrestricted file access.

**size** *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**Syntax:** *size***k** to specify KB, *size***m** to specify MB, or *size***g** to specify GB

**Range:** 10240 through 1073741824

**world-readable**—(Optional) Enable unrestricted file access.

<b>Required Privilege Level</b>	trace—To view this statement in the configuration.
	trace-control—To add this statement to the configuration.

<b>Related Documentation</b>	• <i>Tracing L2TP Operations</i>
	• <a href="#">Tracing L2TP Operations for Subscriber Access on page 283</a>

## tunnel (Tunnel Profile)

---

<b>Syntax</b>	<pre>tunnel <i>tunnel-id</i> {     <i>identification name</i>;     <i>logical-system logical-system-name</i>;     <i>max-sessions number</i>;     <i>medium type</i>;     <i>nas-port-method</i> cisco-avp;     <i>preference number</i>;     <i>remote-gateway</i> {         <i>address server-ip-address</i>;         <i>gateway-name server-name</i>;     }     <i>routing-instance routing-instance-name</i>;     <i>secret password</i>;     <i>source-gateway</i> {         <i>address client-ip-address</i>;         <i>gateway-name client-name</i>;     }     <i>type tunnel-type</i>; }</pre>
<b>Hierarchy Level</b>	[edit access <i>tunnel-profile profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Define the attributes of a tunnel for the tunnel profile. You can define up to 31 tunnels for each tunnel profile.
<b>Options</b>	<p><i>tunnel-id</i>—Unique integer that identifies a tunnel defined within a profile. For a subscriber, RADIUS attributes and VSAs can supply or override the attributes defined here for the tunnel.</p> <p><b>Range:</b> 1 through 31</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li></ul>

## tunnel (L2TP)

---

<b>Syntax</b>	<pre> tunnel {   assignment-id-format (assignment-id   client-server-id);   idle-timeout <i>seconds</i>;   minimum-retransmission-timeout;   nas-port-method;   retransmission-count-established <i>count</i>;   retransmission-count-not-established <i>count</i>;   rx-window-size   tx-address-change (accept   ignore   ignore-ip-address   ignore-udp-port); } </pre>
<b>Hierarchy Level</b>	[edit services <a href="#">l2tp</a> ]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 11.4.</p> <p>Option <b>rx-window-size</b> introduced in Junos OS Release 13.2.</p>
<b>Description</b>	<p>Configure L2TP tunnel characteristics.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring an L2TP LAC on page 35</a></li> <li>• <a href="#">Configuring an L2TP LNS with Inline Service Interfaces on page 51</a></li> </ul>

## tunnel-group

**Syntax** `tunnel-group group-name {`  
     `aaa-access-profile profile-name;`  
     `dynamic-profile profile-name;`  
     `hello-interval seconds;`  
     `hide-avps;`  
     `l2tp-access-profile profile-name;`  
     `local-gateway address {`  
         `address address;`  
         `gateway-name gateway-name;`  
     `}`  
     `maximum-send-window packets;`  
     `ppp-access-profile profile-name;`  
     `receive-window packets;`  
     `retransmit-interval seconds;`  
     `service-device-pool pool-name;`  
     `service-interface interface-name;`  
     `syslog {`  
         `host hostname {`  
             `services severity-level;`  
             `facility-override facility-name;`  
             `log-prefix prefix-value;`  
         `}`  
     `}`  
     `tos-reflect;`  
     `tunnel-switch-profile profile-name;`  
     `tunnel-timeout seconds;`  
     `}`

**Hierarchy Level** [edit services [l2tp](#)]

**Release Information** Statement introduced before Junos OS Release 7.4.  
 Support for MX Series routers introduced in Junos OS Release 11.4.

**Description** Specify the L2TP tunnel properties.



**NOTE:** Subordinate statement support depends on the platform. See individual statement topics for more detailed support information.

**Options** *group-name*—Identifier for the tunnel group.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
 interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring L2TP Tunnel Groups](#)

- [Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces on page 64](#)

## **tunnel-profile (L2TP Tunnel Switching)**

---

<b>Syntax</b>	<code>tunnel-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	[edit access <a href="#">tunnel-switch-profile</a> <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2.
<b>Description</b>	Specify the name of an L2TP tunnel profile that defines the tunnel to which PPP subscriber traffic is switched.
<b>Options</b>	<i>profile-name</i> —Unique name that identifies the tunnel profile; configured with the <b>tunnel-profile</b> statement at the [edit access] hierarchy level.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring L2TP Tunnel Switching on page 70</a></li></ul>

## tunnel-profile (Tunnel Profile)

---

Syntax	<pre>tunnel-profile <i>profile-name</i> {     tunnel <i>tunnel-id</i> {         identification <i>name</i>;         logical-system <i>logical-system-name</i>;         max-sessions <i>number</i>;         medium <i>type</i>;         nas-port-method cisco-avp;         preference <i>number</i>;         remote-gateway {             address <i>server-ip-address</i>;             gateway-name <i>server-name</i>;         }         routing-instance <i>routing-instance-name</i>;         secret <i>password</i>;         source-gateway {             address <i>client-ip-address</i>;             gateway-name <i>client-name</i>;         }         type <i>tunnel-type</i>;     } }</pre>
Hierarchy Level	[edit access]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Define a tunnel profile for subscriber access.
Options	<p><b><i>profile-name</i></b>—Unique name that identifies the tunnel profile. The profile can be referenced from within a domain map or by the RADIUS Tunnel-Group VSA [26-64].</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a></li></ul>



## tunnel-switch-profile (L2TP Tunnel Switching, Application)

<b>Syntax</b>	<code>tunnel-switch-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	[edit access domain map <i>domain-map-name</i> ], [edit services l2tp], [edit services l2tp <i>tunnel-group</i> <i>group-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2.
<b>Description</b>	Specify a tunnel switch profile that determines whether packets in an L2TP session from a LAC are switched to another session that has a different destination LNS.
<b>Options</b>	<i>profile-name</i> —Unique name that identifies the tunnel switch profile.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring L2TP Tunnel Switching on page 70</a></li> </ul>

## tunnel-switch-profile (L2TP Tunnel Switching, Definition)


<b>Syntax</b>	<pre>tunnel-switch-profile <i>profile-name</i> {   avp {     bearer-type <i>action</i>;     calling-number <i>action</i>;     cisco-nas-port-info <i>action</i>;   }   tunnel-profile <i>profile-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit access]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2.
<b>Description</b>	<p>Define a tunnel switch profile for subscriber access; specify actions to take for L2TP AVPs in the switched packets and the profile for the tunnel to which the PPP traffic is switched.</p> <p>The remaining statements are explained separately.</p>
<b>Options</b>	<i>profile-name</i> —Unique name that identifies the tunnel switch profile. The profile can be applied as a default or referenced from within a domain map, a tunnel group, or by the RADIUS Tunnel-Group VSA [26-64].
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring L2TP Tunnel Switching on page 70</a></li> </ul>

## tx-address-change (L2TP LAC)

---

<b>Syntax</b>	tx-address-change (accept   ignore   ignore-ip-address   ignore-udp-port);
<b>Hierarchy Level</b>	[edit services l2tp <a href="#">tunnel</a> ]
<b>Description</b>	Configure whether the LAC accepts or ignores requests from a peer to change the destination IP address, UDP port, or both.
<b>Default</b>	The LAC accepts the IP address change from its peer.
<b>Options</b>	<b>accept</b> —Accept a change in IP address , UDP port, or both. <b>ignore</b> —Ignore a change request for IP address or UDP port. <b>ignore-ip-address</b> —Ignore a change request for IP address. <b>ignore-udp-port</b> —Ignore a change request for UDP port.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the LAC to Ignore Address and Port Changes Requested by the LNS on page 46</a></li></ul>

## tx-connect-speed-method (L2TP LAC)

<b>Syntax</b>	<code>tx-connect-speed-method <i>method</i>;</code>
<b>Hierarchy Level</b>	[edit services <b>l2tp</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4. Options <b>ancp</b> , <b>pppoe-ia-tag</b> , and <b>static</b> introduced in Junos OS Release 13.1.
<b>Description</b>	Specify the method that determines the connection speed values sent from the LAC to the LNS in Incoming-Call-Connected (ICCN) messages. The transmit speed is conveyed in AVP 24 (Tx Connect Speed ) and the receive speed is conveyed in AVP 38 (Rx Connect Speed). Both values are in bits per seconds (BPS).
<b>Default</b>	<b>static</b>
<b>Options</b>	<p><b><i>method</i></b>—Method used to derive the connection speed values.</p> <ul style="list-style-type: none"> <li>• <b>ancp</b>—The speed is derived from the configured ANCP value for the underlying interface. You can change this rate after a subscriber has logged in, but those changes do not affect the actual rate used by the LNS. The <b>ancp</b> method gets the highest preference among the methods configured.</li> <li>• <b>pppoe-ia-tags</b>—PPPoE IA tags sent from the DSLAM to the LAC. This speed value transmitted when a subscriber logs in and it cannot be subsequently changed. This value is used when the <b>ancp</b> value is not available. This speed does not apply to the subscribers that are already logged in; it is effective only for subscribers that log in after this setting has been saved. AVP 24 is the value of Actual-Data-Rate-Downstream (VSA 26-129). AVP 38 is the value of Actual-Data-Rate-Upstream (VSA 26-130), and is sent only when the VSA values differ.</li> </ul>
	<p> <b>NOTE:</b> This rate does not affect the subscribers already logged in; however, new subscribers inherit the new rate.</p>
	<ul style="list-style-type: none"> <li>• <b>static</b>—The speed is derived from the recommended (advisory) shaping rate configured on the PPPoE logical interface underlying the subscriber interface. If the advisory speed is not configured on the underlying interface, then the actual port speed is used. The default method, when no other methods yield a value, is the <b>static</b> method or the advisory speed method. If the advisory speed is not configured, then the actual port speed is used. For ge and xe interfaces, the speed value is set to 10,000,000 and for ae interfaces, the speed value is set to 0 and sent in both AVP 24 and AVP 38.</li> </ul>
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.

- Related Documentation**
- [Configuring the Method to Set the LAC Connection Speeds to the LNS on page 42](#)


## type (Tunnel Profile)

---

<b>Syntax</b>	<code>type tunnel-type;</code>
<b>Hierarchy Level</b>	<code>[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the tunnel type (protocol).
<b>Default</b>	l2tp
<b>Options</b>	<i>tunnel-type</i> —Tunnel protocol type. The only value currently available is <b>l2tp</b> .
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	• <a href="#">Configuring a Tunnel Profile for Subscriber Access on page 37</a>

## user-group-profile

---

<b>Syntax</b>	<code>user-group-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access profile <i>profile-name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Apply a configured PPP group profile to PPP users.
<div> <b>NOTE:</b> If <i>&lt;user-group-profile&gt;</i> is modified or deleted, the existing LNS subscribers, which were using this Layer 2 Tunneling Protocol client configuration, will go down.</div>	
<b>Options</b>	<i>profile-name</i> —Name of a PPP group profile configured at the <code>[edit access group-profile <i>profile-name</i>]</code> hierarchy level.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	• <a href="#">Applying a Configured PPP Group Profile to a Tunnel</a> • <a href="#">Configuring an L2TP Access Profile on the LNS on page 56</a>

## weighted-load-balancing (L2TP LAC)

---

<b>Syntax</b>	weighted-load-balancing;
<b>Hierarchy Level</b>	[edit services <a href="#">l2tp</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify that the router chooses among multiple tunnels that share the same preference level by considering the maximum sessions configured per tunnel. The tunnel configured with the highest maximum number of sessions in the preference level has the highest weight. This tunnel is selected until the maximum number of sessions for the tunnel is reached. Then the router selects the tunnel with the next higher weight to establish connections until that tunnel's maximum session limit is reached, and so on.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Weighted Load Balancing for LAC Tunnel Sessions on page 41</a></li><li>• <a href="#">Configuring the L2TP LAC Tunnel Selection Parameters on page 40</a></li></ul>



## PART 3

# Administration

- [Verifying and Monitoring Configurations on page 175](#)
- [Monitoring Commands on page 179](#)





## CHAPTER 9

# Verifying and Monitoring Configurations

- [Verifying and Managing L2TP for Subscriber Access on page 175](#)
- [Testing L2TP Tunnel Configurations from the LAC on page 176](#)

### Verifying and Managing L2TP for Subscriber Access

---

**Purpose** View or clear information about L2TP tunnels and sessions.

**Action** • To display a summary of L2TP tunnels, sessions, errors, and control and data packets:

```
user@host> show services l2tp summary
```

- To display the L2TP destinations:

```
user@host> show services l2tp destination
```

- To clear all L2TP destinations:

```
user@host> clear services l2tp destination all
```

- To clear statistics for all L2TP tunnels belonging to a destination, tunnels belonging to a specified local-gateway address, and tunnels belonging to a specified peer-gateway address:

```
user@host> clear services l2tp destination statistics all
```

```
user@host> clear services l2tp destination local-gateway 10.1.1.2
```

- To display the L2TP sessions:

```
user@host> show services l2tp session
```

- To clear all L2TP sessions, the session with a specified local session ID, or sessions associated with the local gateway specified by an IP address or name:

```
user@host> clear services l2tp session all
```

```
user@host> clear services l2tp session local-session-id 40553
```

```
user@host> clear services l2tp session local-gateway 10.1.1.2
```

```
user@host> clear services l2tp session local-gateway-name lns-mx960
```

- To clear statistics for all L2TP sessions, the session with a specified local session ID, or sessions associated with the local gateway specified by an IP address or name:

```
user@host> clear services l2tp session statistics all
```

```
user@host> clear services l2tp session statistics local-session-id 17967
```

```
user@host> clear services l2tp session statistics local-gateway 10.1.1.2
```

```
user@host> clear services l2tp session statistics local-gateway-name lns-mx960
```

- To display the L2TP tunnels:

```
user@host> show services l2tp tunnel
```

- To clear all L2TP tunnels, the tunnel with a specified local tunnel ID, or tunnels associated with the local gateway specified by an IP address or name:

```
user@host> clear services l2tp tunnel all
user@host> clear services l2tp tunnel local-tunnel-id 40553
user@host> clear services l2tp tunnel local-gateway 10.1.1.2
user@host> clear services l2tp tunnel local-gateway-name lns-mx960
```

- To clear statistics for all L2TP tunnels, the tunnel with a specified local tunnel ID, or tunnels associated with the local gateway specified by an IP address or name:

```
user@host> clear services l2tp tunnel statistics all
user@host> clear services l2tp tunnel statistics local-tunnel-id 40553
user@host> clear services l2tp tunnel statistics local-gateway 10.1.1.2
user@host> clear services l2tp tunnel statistics local-gateway-name lns-mx960
```

#### Related Documentation

- [Configuring an L2TP LAC on page 35](#)
- [Configuring an L2TP LNS with Inline Service Interfaces on page 51](#)
- [CLI Explorer](#).

---

## Testing L2TP Tunnel Configurations from the LAC

You can test L2TP tunnel configurations on the LAC and successful subscriber authentication and tunneling without bringing up a PPP user and an associated tunnel.

Issue the **test services l2tp tunnel** command from CLI operational mode to map a subscriber to an L2TP tunnel, verify the L2TP tunnel configuration (both locally on the LAC and on a back-end server such as a RADIUS server), and verify that L2TP tunnels from the LAC can be established with the remote LNS.

The Junos OS LAC implementation enables you to configure multiple tunnels from which one tunnel is chosen for tunneling a PPP subscriber. You can use the **test services l2tp tunnel** command to test all possible tunnel configurations to verify that each can be established. Alternatively, you can test only a specific tunnel for the subscriber.

You must specify a configured subscriber username when you issue the command. The test generates a dummy password—*testpass*—for the subscriber, or you can optionally specify the password. The test verifies whether the subscriber identified by that username can be tunneled according to the tunnel configuration. If the subscriber can be tunneled, then the test verifies whether the L2TP tunnel can be established with the LNS according to the L2TP configuration.

You can optionally specify a tunnel ID, in which case only that tunnel is tested; the tunnel must be already configured for that username. If you omit this option, the test is applied to the full set of tunnel configurations that are returned for the username. The tunnel ID you specify is the same as that used by Tunnel-Assignment-Id (RADIUS attribute 82) and specified by the **identification** statement in the tunnel profile.

To test subscriber authentication and tunnel configuration:

To test subscriber authentication and tunnel configuration:

- Specify only the username.

Example 1:

```
user@host> test services l2tp tunnel user test-user1@example.com
Subscriber: test-user1@example.com, authentication failed
```

The user failed authentication with the generated password and consequently was not tunneled.

Example 2:

```
user@host> test services l2tp tunnel user user23@example.com
Subscriber: user23@example.com, authentication success, l2tp tunneled
Tunnel-name  Tunnel-peer  Logical-System  Routing-Instance  Status
test1tunnel  192.168.2.3   default         default           Up
test2tunnel  192.168.30.3  default         default           Peer unresponsive
test3tunnel  192.168.50.1  default         test              Up
```

This user was authenticated with the generated password and successfully tunneled. A set of tunnels was found to be associated with that username and the entire set was tested.

- Specify the username and the user's configured password.

```
user@host> test services l2tp tunnel user test-user1@example.com password grZ98#jW
Subscriber: test-user1@example.com, authentication success, locally terminated
```

The subscriber was authenticated. However, the user was terminated locally rather than tunneled; this means that no tunnel was found to be associated with the user.

- Specify the username and a particular tunnel for the subscriber.

```
user@host> test services l2tp tunnel user rx37w@example.com tunnel-name ce-lac
Subscriber: rx37w@example.com, authentication success, l2tp tunneled
Tunnel-name  Tunnel-peer  Logical-System  Routing-Instance  Status
ce-lac       192.168.5.10  default         default           Up
```

The subscriber was authenticated and tunneled. The specified tunnel was found for the subscriber and the tunnel was established, confirming the tunnel configuration.

- Specify the username, the user's configured password, and a tunnel.

```
user@host> test services l2tp tunnel user fanta4-mfg-fan@example.com password dieda499
tunnel-name tunnel5
Subscriber: fanta4-mfg-fan@example.com, authentication success, l2tp tunneled
```

The subscriber was authenticated and tunneled. The absence of tunnel information in the output indicates that the specified tunnel configuration does not exist.

**Related Documentation** • [L2TP for Subscriber Access Overview on page 3](#)



## CHAPTER 10

# Monitoring Commands

- clear services l2tp destination
- clear services l2tp session
- clear services l2tp session statistics
- clear services l2tp tunnel
- clear services l2tp tunnel statistics
- restart
- show ppp interface
- show services inline ip-reassembly statistics
- show services l2tp destination
- show services l2tp destination lockout
- show services l2tp session
- show services l2tp tunnel-switch destination
- show services l2tp tunnel-switch session
- show services l2tp tunnel-switch tunnel
- show services l2tp tunnel-switch summary
- show services l2tp summary
- show services l2tp tunnel
- show subscribers
- show subscribers summary
- test services l2tp tunnel

## clear services l2tp destination

---

<b>Syntax</b>	<code>clear services l2tp destination</code> <code>&lt;all   local-gateway <i>gateway-address</i>   peer-gateway <i>gateway-address</i>&gt;</code>
<b>Release Information</b>	Command introduced in Junos OS Release 10.4. <b>Statistics</b> option introduced in Junos OS Release 13.1
<b>Description</b>	Clear all Layer 2 Tunneling Protocol (L2TP) destinations and all tunnels and sessions that belong to the destinations. This command is available only for LAC on MX Series routers.
<b>Options</b>	<b>all</b> —Close all L2TP destinations.  <b>local-gateway <i>gateway-address</i></b> —Clear only the L2TP destinations and all tunnels and sessions associated with the specified local gateway address.  <b>peer-gateway <i>gateway-address</i></b> —Clear only the L2TP destinations and all tunnels and sessions associated with the peer gateway with the specified address.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show services l2tp destination on page 215</a></li></ul>
<b>List of Sample Output</b>	<a href="#">clear services l2tp destination all on page 180</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

### Sample Output

#### clear services l2tp destination all

```
user@host> clear services l2tp destination all

Destination 2 closed
```

## clear services l2tp session

<b>Syntax</b>	clear services l2tp session (all   interface <i>interface-name</i>   local-gateway <i>gateway-address</i>   local-gateway-name <i>gateway-name</i>   local-session-id <i>session-id</i>   local-tunnel-id <i>tunnel-id</i>   peer-gateway <i>gateway-address</i>   peer-gateway-name <i>gateway-name</i>   tunnel-group <i>group-name</i>   user <i>username</i> )
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	(M10i and M7i routers only) Clear Layer 2 Tunneling Protocol (L2TP) sessions on LNS.  (MX Series routers only) Clear L2TP sessions on LAC and LNS.
<b>Options</b>	<p><b>all</b>—Close all L2TP sessions.</p> <p><b>interface <i>interface-name</i></b>—Clear only the L2TP sessions using the specified adaptive services or inline services interface. The interface type depends on the line card as follows:</p> <ul style="list-style-type: none"> <li>• <b>si-<i>fpc/pic/port</i></b>—MPCs on MX Series routers only. This option is not available for L2TP on M Series routers.</li> <li>• <b>sp-<i>fpc/pic/port</i></b>—AS or Multiservices PICs on M7i, M10i, and M120 routers only. This option is not available for L2TP on MX Series routers.</li> </ul> <p><b>local-gateway <i>gateway-address</i></b>—Clear only the L2TP sessions associated with the specified local gateway address.</p> <p><b>local-gateway-name <i>gateway-name</i></b>—Clear only the L2TP sessions associated with the specified local gateway name.</p> <p><b>local-session-id <i>session-id</i></b>—Clear only the L2TP sessions with this identifier for the local endpoint of the L2TP session.</p> <p><b>local-tunnel-id <i>tunnel-id</i></b>—Clear only the L2TP sessions associated with the specified local tunnel identifier.</p> <p><b>peer-gateway <i>gateway-address</i></b>—Clear only the L2TP sessions associated with the peer gateway with the specified address.</p> <p><b>peer-gateway-name <i>gateway-name</i></b>—Clear only the L2TP sessions associated with the peer gateway with the specified name.</p> <p><b>tunnel-group <i>group-name</i></b>—Clear only the L2TP sessions associated with the specified tunnel group. This option is not available for L2TP LAC on MX Series routers.</p> <p><b>user <i>username</i></b>—(M Series routers only) Clear only the L2TP sessions for the specified username.</p>
<b>Required Privilege Level</b>	clear

- Related Documentation**
- [L2TP Services Configuration Overview](#)
  - [L2TP Minimum Configuration](#)
  - [clear services l2tp session statistics on page 183](#)
  - [show services l2tp session on page 220](#)

**List of Sample Output**    [clear services l2tp session on page 182](#)  
                                  [clear services l2tp session interface on page 182](#)

**Output Fields**    When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### [clear services l2tp session](#)

```
user@host> clear services l2tp session 31694

Session 31694 closed
```

## Sample Output

### [clear services l2tp session interface](#)

```
user@host> show services l2tp session Tunnel local ID: 17185
Local Remote State Interface Interface
ID ID unit Name
5117 1 Established 1073741828 si-2/0/0
34915 2 Established 1073741829 si-2/1/0
6454 3 Established 1073741830 si-2/0/0
46142 4 Established 1073741831 si-2/1/0

user@host> clear services l2tp session interface si-2/0/0
Session 5117 closed
Session 6454 closed

user@host> show services l2tp session Tunnel local ID: 17185
Local Remote State Interface Interface
ID ID unit Name
34915 2 Established 1073741829 si-2/1/0
46142 4 Established 1073741831 si-2/1/0
```



## clear services l2tp session statistics

<b>Syntax</b>	clear services l2tp session statistics (all   interface <i>interface-name</i>   local-gateway <i>gateway-address</i>   local-gateway-name <i>gateway-name</i>   local-session-id <i>session-id</i>   local-tunnel-id <i>tunnel-id</i>   peer-gateway <i>gateway-address</i>   peer-gateway-name <i>gateway-name</i>   tunnel-group <i>group-name</i>   user <i>username</i> )
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Support for MX Series routers added in Junos OS Release 10.4.
<b>Description</b>	(M10i and M7i routers: LNS only. MX Series routers: LAC and LNS.) Clear statistics for Layer 2 Tunneling Protocol (L2TP) sessions.
<b>Options</b>	<p><b>all</b>—Clear statistics for all L2TP sessions.</p> <p><b>interface <i>interface-name</i></b>—Clear only the L2TP sessions using the specified adaptive services or inline services interface. The interface type depends on the line card as follows:</p> <ul style="list-style-type: none"> <li><b>si-<i>fpc/pic/port</i></b>—MPCs on MX Series routers only. This option is not available for L2TP on M Series routers.</li> <li><b>sp-<i>fpc/pic/port</i></b>—AS or Multiservices PICs on M7i, M10i, and M120 routers only. This option is not available for L2TP on MX Series routers.</li> </ul> <p><b>local-gateway <i>gateway-address</i></b>—Clear statistics for only the L2TP sessions associated with the local gateway with the specified address.</p> <p><b>local-gateway-name <i>gateway-name</i></b>—Clear statistics for only the L2TP sessions associated with the local gateway with the specified name.</p> <p><b>local-session-id <i>session-id</i></b>—Clear statistics for only the L2TP sessions with this identifier for the local endpoint of the L2TP session.</p> <p><b>local-tunnel-id <i>tunnel-id</i></b>—Clear statistics for only the L2TP sessions associated with the specified local tunnel identifier.</p> <p><b>peer-gateway <i>gateway-address</i></b>—Clear statistics for only the L2TP sessions associated with the peer gateway with the specified address.</p> <p><b>peer-gateway-name <i>gateway-name</i></b>—Clear statistics for only the L2TP sessions associated with the peer gateway with the specified name.</p> <p><b>tunnel-group <i>group-name</i></b>—Clear statistics for only the L2TP sessions associated with the specified tunnel group. This option is not available for L2TP LAC on MX Series routers.</p> <p><b>user <i>username</i> &lt;statistics&gt;</b>—Clear statistics for only the L2TP sessions for the specified username. This option is not available for L2TP LAC on MX Series routers.</p>
<b>Required Privilege Level</b>	view

- Related Documentation**
- *L2TP Services Configuration Overview*
  - *L2TP Minimum Configuration*
  - [clear services l2tp session on page 181](#)
  - [show services l2tp session on page 220](#)

**List of Sample Output**    [clear services l2tp session statistics all on page 184](#)

**Output Fields**    When you enter this command, you are provided feedback on the status of your request.

## Sample Output

[clear services l2tp session statistics all](#)

```
user@host> clear services l2tp session statistics all
Session 26497 statistics cleared
```

## clear services l2tp tunnel

<b>Syntax</b>	clear services l2tp tunnel (all   interface <i>sp-fpc/pic/port</i>   local-gateway <i>gateway-address</i>   local-gateway-name <i>gateway-name</i>   local-tunnel-id <i>tunnel-id</i>   peer-gateway <i>gateway-address</i>   peer-gateway-name <i>gateway-name</i>   tunnel-group <i>group-name</i> )
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Support for LAC on MX Series routers introduced in Junos OS Release 10.4. Support for LNS on MX Series routers introduced in Junos OS Release 11.4.
<b>Description</b>	(M10i and M7i routers: LNS only. MX Series routers: LAC and LNS.) Clear Layer 2 Tunneling Protocol (L2TP) tunnels.
<b>Options</b>	<p><b>all</b>—Clear all L2TP tunnels.</p> <p><b>sp-fpc/pic/port</b>—(Optional) Clear only the L2TP tunnels using the specified adaptive services interface. This option is not available for L2TP on MX Series routers.</p> <p><b>local-gateway gateway-address</b>—Clear only the L2TP tunnels associated with the local gateway with the specified address.</p> <p><b>local-gateway-name gateway-name</b>—Clear only the L2TP tunnels associated with the local gateway with the specified name.</p> <p><b>local-tunnel-id tunnel-id</b>—Clear only the L2TP tunnels that have the specified local tunnel identifier.</p> <p><b>peer-gateway gateway-address</b>—Clear only the L2TP tunnels associated with the peer gateway with the specified address.</p> <p><b>peer-gateway-name gateway-name</b>—Clear only the L2TP tunnels associated with the peer gateway with the specified name.</p> <p><b>tunnel-group group-name</b>—Clear only the L2TP tunnels in the specified tunnel group. This option is not available for L2TP LAC on MX Series routers.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">L2TP Services Configuration Overview</a></li> <li>• <a href="#">L2TP Minimum Configuration</a></li> <li>• <a href="#">clear services l2tp tunnel statistics on page 187</a></li> <li>• <a href="#">show services l2tp tunnel on page 249</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">clear services l2tp tunnel on page 186</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

## Sample Output

clear services l2tp tunnel

```
user@host> clear services l2tp tunnel 17185
```

```
Tunnel 17185 closed
```

## clear services l2tp tunnel statistics

<b>Syntax</b>	clear services l2tp tunnel statistics (all   interface <i>sp-fpc/pic/port</i>   local-gateway <i>gateway-address</i>   local-gateway-name <i>gateway-name</i>   local-tunnel-id <i>tunnel-id</i>   peer-gateway <i>gateway-address</i>   peer-gateway-name <i>gateway-name</i>   tunnel-group <i>group-name</i> )
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Support for MX Series routers added in Junos OS Release 10.4.
<b>Description</b>	(M10i and M7i routers: LNS only. MX Series routers: LAC only.) Clear statistics for Layer 2 Tunneling Protocol (L2TP) tunnels.
<b>Options</b>	<p><b>all</b>—Clear statistics for all L2TP tunnels.</p> <p><b>interface <i>sp-fpc/pic/port</i></b>—Clear statistics for only the L2TP tunnels using the specified adaptive services interface. This option is not available for L2TP LAC on MX Series routers.</p> <p><b>local-gateway <i>gateway-address</i></b>—Clear statistics for only the L2TP tunnels associated with the local gateway with the specified address.</p> <p><b>local-gateway-name <i>gateway-name</i></b>—Clear statistics for only the L2TP tunnels associated with the local gateway with the specified name.</p> <p><b>local-tunnel-id <i>tunnel-id</i></b>—Clear statistics for only the L2TP tunnels that have the specified local tunnel identifier.</p> <p><b>peer-gateway <i>gateway-address</i></b>—Clear statistics for only the L2TP tunnels associated with the peer gateway with the specified address.</p> <p><b>peer-gateway-name <i>gateway-name</i></b>—Clear statistics for only the L2TP tunnels associated with the peer gateway with the specified name.</p> <p><b>tunnel-group <i>group-name</i></b>—Clear statistics for only the L2TP tunnels in the specified tunnel group. This option is not available for L2TP LAC on MX Series routers.</p>
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">L2TP Services Configuration Overview</a></li> <li>• <a href="#">L2TP Minimum Configuration</a></li> <li>• <a href="#">clear services l2tp tunnel on page 185</a></li> <li>• <a href="#">show services l2tp tunnel on page 249</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">clear services l2tp tunnel statistics all on page 188</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

## Sample Output

`clear services l2tp tunnel statistics all`

```
user@host> clear services l2tp tunnel statistics all
Tunnel 9933 statistics cleared
```

## restart

### List of Syntax [Syntax on page 189](#)

[Syntax \(ACX Series Routers\) on page 189](#)  
[Syntax \(EX Series Switches\) on page 189](#)  
[Syntax \(Routing Matrix\) on page 190](#)  
[Syntax \(J Series Routing Platform\) on page 190](#)  
[Syntax \(TX Matrix Routers\) on page 190](#)  
[Syntax \(TX Matrix Plus Routers\) on page 190](#)  
[Syntax \(MX Series Routers\) on page 190](#)  
[Syntax \(J Series Routers\) on page 191](#)  
[Syntax \(QFX Series\) on page 191](#)

### Syntax restart

```

<adaptive-services | ancpd-service | application-identification | audit-process |
  auto-configuration | captive-portal-content-delivery | ce-l2tp-service | chassis-control |
  class-of-service | clksyncd-service | database-replication | datapath-trace-service
  | dhcp-service | diameter-service | disk-monitoring | dynamic-flow-capture |
  ecc-error-logging | ethernet-connectivity-fault-management
  | ethernet-link-fault-management | event-processing | firewall
  | general-authentication-service | gracefully | iccp-service | idp-policy | immediately
  | interface-control | ipsec-key-management | kernel-replication | l2-learning | l2cpd-service
  | l2tp-service | l2tp-universal-edge | lacp | license-service | link-management
  | local-policy-decision-function | mac-validation | mib-process | mobile-ip | mounstd-service
  | mpls-traceroute | mspd | multicast-snooping | named-service | nfsd-service |
  packet-triggered-subscribers | peer-selection-service | pgcp-service | pgm |
  pic-services-logging | pki-service | ppp | ppp-service | pppoe |
  protected-system-domain-service | redundancy-interface-process | remote-operations |
  root-system-domain-service | routing <logical-system logical-system-name> | sampling
  | sbc-configuration-process | sdk-service | service-deployment | services | services pgcp
  gateway gateway-name | snmp | soft | static-subscribers | statistics-service |
  subscriber-management | subscriber-management-helper | tunnel-oamd | usb-control |
  vrrp | web-management>
<gracefully | immediately | soft>

```

### Syntax (ACX Series Routers)

```

restart
<adaptive-services | audit-process | auto-configuration | autoinstallation | chassis-control |
  class-of-service | clksyncd-service | database-replication | dhcp-service | diameter-service
  | disk-monitoring | dynamic-flow-capture | ethernet-connectivity-fault-management
  | ethernet-link-fault-management | event-processing | firewall
  | general-authentication-service | gracefully | immediately | interface-control |
  ipsec-key-management | l2-learning | lacp | link-management | mib-process | mobile-ip |
  mounstd-service | mpls-traceroute | mspd | named-service | nfsd-service | pgm | pki-service
  | ppp | pppoe | redundancy-interface-process | remote-operations | routing | sampling |
  sdk-service | secure-neighbor-discovery | service-deployment | services | snmp | soft
  | statistics-service | subscriber-management | subscriber-management-helper | tunnel-oamd
  | vrrp>

```

### Syntax (EX Series Switches)

```

restart
<autoinstallation | chassis-control | class-of-service | database-replication | dhcp |
  dhcp-service | diameter-service | dot1x-protocol | ethernet-link-fault-management |
  ethernet-switching | event-processing | firewall | general-authentication-service |
  interface-control | kernel-replication | l2-learning | lacp | license-service | link-management

```

	lldpd-service   mib-process   mounstd-service   multicast-snooping   pgm   redundancy-interface-process   remote-operations   routing   secure-neighbor-discovery   service-deployment   sflow-service   snmp   vrrp   web-management>
<b>Syntax (Routing Matrix)</b>	restart <adaptive-services   audit-process   chassis-control   class-of-service   disk-monitoring   dynamic-flow-capture   ecc-error-logging   event-processing   firewall   interface-control   ipsec-key-management   kernel-replication   l2-learning   l2tp-service   lacp   link-management   mib-process   pgm   pic-services-logging   ppp   pppoe   redundancy-interface-process   remote-operations   routing <logical-system <i>logical-system-name</i> >   sampling   service-deployment   snmp> <all   all-lcc   lcc <i>number</i> > <gracefully   immediately   soft>
<b>Syntax (J Series Routing Platform)</b>	restart <adaptive-services   audit-process   chassis-control   class-of-service   dhcp   dialer-services   dls   event-processing   firewall   interface-control   ipsec-key-management   isdn-signaling   l2-learning   l2tp-service   mib-process   network-access-service   pgm   ppp   pppoe   remote-operations   routing <logical-system <i>logical-system-name</i> >   sampling   service-deployment   snmp   usb-control   web-management> <gracefully   immediately   soft>
<b>Syntax (TX Matrix Routers)</b>	restart <adaptive-services   audit-process   chassis-control   class-of-service   dhcp-service   diameter-service   disk-monitoring   dynamic-flow-capture   ecc-error-logging   event-processing   firewall   interface-control   ipsec-key-management   kernel-replication   l2-learning   l2tp-service   lacp   link-management   mib-process   pgm   pic-services-logging   ppp   pppoe   redundancy-interface-process   remote-operations   routing <logical-system <i>logical-system-name</i> >   sampling   service-deployment   snmp   statistics-service> <all-chassis   all-lcc   lcc <i>number</i>   scc> <gracefully   immediately   soft>
<b>Syntax (TX Matrix Plus Routers)</b>	restart <adaptive-services   audit-process   chassis-control   class-of-service   dhcp-service   diameter-service   disk-monitoring   dynamic-flow-capture   ecc-error-logging   event-processing   firewall   interface-control   ipsec-key-management   kernel-replication   l2-learning   l2tp-service   lacp   link-management   mib-process   pgm   pic-services-logging   ppp   pppoe   redundancy-interface-process   remote-operations   routing <logical-system <i>logical-system-name</i> >   sampling   service-deployment   snmp   statistics-service> <all-chassis   all-lcc   all-sfc   lcc <i>number</i>   sfc <i>number</i> > <gracefully   immediately   soft>
<b>Syntax (MX Series Routers)</b>	restart <adaptive-services   ancpd-service   application-identification   audit-process   auto-configuration   captive-portal-content-delivery   ce-l2tp-service   chassis-control   class-of-service   clksyncd-service   database-replication   datapath-trace-service   dhcp-service   diameter-service   disk-monitoring   dynamic-flow-capture   ecc-error-logging   ethernet-connectivity-fault-management   ethernet-link-fault-management   event-processing   firewall   general-authentication-service   gracefully   iccp-service   idp-policy   immediately   interface-control   ipsec-key-management   kernel-replication   l2-learning   l2cpd-service   l2tp-service   l2tp-universal-edge   lacp   license-service   link-management   local-policy-decision-function   mac-validation   mib-process   mobile-ip   mounstd-service   mpls-traceroute   msp   multicast-snooping   named-service   nfsd-service



```

packet-triggered-subscribers |peer-selection-service | pgcp-service | pgm |
pic-services-logging | pki-service | ppp | ppp-service | pppoe |
protected-system-domain-service | redundancy-interface-process | remote-operations
|root-system-domain-service | routing |routing <logical-system logical-system-name> |
sampling | sbc-configuration-process | sdk-service |service-deployment |services | services
pgcp gateway gateway-name |snmp |soft |static-subscribers |statistics-service|
subscriber-management | subscriber-management-helper | tunnel-oamd | usb-control|
vrrp |web-management>
<all-members>
<gracefully | immediately | soft>
<local>
<member member-id>

```

**Syntax (J Series  
Routers)**

```

restart
<adaptive-services | audit-process | chassis-control | class-of-service | dhcp | dhcp-service
| dialer-services | diameter-service | dlsr | event-processing | firewall | interface-control |
ipsec-key-management | isdn-signaling | l2ald | l2-learning | l2tp-service | mib-process |
network-access-service | pgm | ppp | pppoe | remote-operations | routing <logical-system
logical-system-name> | sampling | service-deployment | snmp | usb-control |
web-management>
<gracefully | immediately | soft>

```

**Syntax (QFX Series)**

```

restart
<adaptive-services | audit-process | chassis-control | class-of-service | dialer-services |
diameter-service | dlsr | ethernet-connectivity | event-processing | fibre-channel | firewall
| general-authentication-service | igmp-host-services | interface-control |
ipsec-key-management | isdn-signaling | l2ald | l2-learning | l2tp-service | mib-process |
named-service | network-access-service | nstrace-process | pgm | ppp | pppoe |
redundancy-interface-process | remote-operations |logical-system-name> | routing |
sampling |secure-neighbor-discovery | service-deployment | snmp | usb-control |
web-management>
<gracefully | immediately | soft>

```

**Release Information**

Command introduced before Junos OS Release 7.4.  
 Command introduced in Junos OS Release 9.0 for EX Series switches.  
 Command introduced in Junos OS Release 11.1 for the QFX Series.  
 Command introduced in Junos OS Release 12.2 for ACX Series routers.  
 Options added:

- **dynamic-flow-capture** in Junos OS Release 7.4.
- **dlsr** in Junos OS Release 7.5.
- **event-processing** in Junos OS Release 7.5.
- **ppp** in Junos OS Release 7.5.
- **l2ald** in Junos OS Release 8.0.
- **link-management** in Release 8.0.
- **pgcp-service** in Junos OS Release 8.4.
- **sbc-configuration-process** in Junos OS Release 9.5.
- **services pgcp gateway** in Junos OS Release 9.6.
- **sfc** and **all-sfc** for the TX Matrix Router in Junos OS Release 9.6.

**Description** Restart a Junos OS process.



**CAUTION:** Never restart a software process unless instructed to do so by a customer support engineer. A restart might cause the router or switch to drop calls and interrupt transmission, resulting in possible loss of data.

**Options** **none**—Same as **gracefully**.

**adaptive-services**—(Optional) Restart the configuration management process that manages the configuration for stateful firewall, Network Address Translation (NAT), intrusion detection services (IDS), and IP Security (IPsec) services on the Adaptive Services PIC.

**all-chassis**—(TX Matrix and TX Matrix Plus routers only) (Optional) Restart the software process on all chassis.

**all-lcc**—(TX Matrix and TX Matrix Plus routers only) (Optional) For a TX Matrix router, restart the software process on all T640 routers connected to the TX Matrix router. For a TX Matrix Plus router, restart the software process on all T1600 routers connected to the TX Matrix Plus router.

**all-members**—(MX Series routers only) (Optional) Restart the software process for all members of the Virtual Chassis configuration.

**all-sfc**—(TX Matrix Plus routers only) (Optional) For a TX Matrix Plus router, restart the software processes for the TX Matrix Plus router (or switch-fabric chassis).

**ancpd-service**—(Optional) Restart the Access Node Control Protocol (ANCP) process, which works with a special Internet Group Management Protocol (IGMP) session to collect outgoing interface mapping events in a scalable manner.

**application-identification**—(Optional) Restart the process that identifies an application using intrusion detection and prevention (IDP) to allow or deny traffic based on applications running on standard or nonstandard ports.

**audit-process**—(Optional) Restart the RADIUS accounting process that gathers statistical data that can be used for general network monitoring, analyzing, and tracking usage patterns, for billing a user based on the amount of time or type of services accessed.

**auto-configuration**—(Optional) Restart the Interface Auto-Configuration process.

**autoinstallation**—(EX Series switches only) (Optional) Restart the autoinstallation process.

**captive-portal-content-delivery**—(Optional) Restart the HTTP redirect service by specifying the location to which a subscriber's initial Web browser session is redirected, enabling initial provisioning and service selection for the subscriber.

**ce-l2tp-service**—(M10, M10i, M7i, and MX Series routers only) (Optional) Restart the Universal Edge Layer 2 Tunneling Protocol (L2TP) process, which establishes L2TP tunnels and Point-to-Point Protocol (PPP) sessions through L2TP tunnels.

**chassis-control**—(Optional) Restart the chassis management process.

**class-of-service**—(Optional) Restart the class-of-service (CoS) process, which controls the router's or switch's CoS configuration.

**clksyncd-service**—(Optional) Restart the external clock synchronization process, which uses synchronous Ethernet (SyncE).

**database-replication**—(EX Series switches and MX Series routers only) (Optional) Restart the database replication process.

**d datapath-trace-service**—(Optional) Restart the packet path tracing process.

**dhcp**—(J Series routers and EX Series switches only) (Optional) Restart the software process for a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server allocates network IP addresses and delivers configuration settings to client hosts without user intervention.

**dhcp-service**—(Optional) Restart the Dynamic Host Configuration Protocol process.

**dialer-services**—(J Series routers and EX Series switches only) (Optional) Restart the ISDN dial-out process.

**diameter-service**—(Optional) Restart the diameter process.

**disk-monitoring**—(Optional) Restart disk monitoring, which checks the health of the hard disk drive on the Routing Engine.

**dlsw**—(J Series routers and QFX Series only) (Optional) Restart the data link switching (DLSw) service.

**dot1x-protocol**—(EX Series switches only) (Optional) Restart the port-based network access control process.

**dynamic-flow-capture**—(Optional) Restart the dynamic flow capture (DFC) process, which controls DFC configurations on Monitoring Services III PICs.

**ecc-error-logging**—(Optional) Restart the error checking and correction (ECC) process, which logs ECC parity errors in memory on the Routing Engine.

**ethernet-connectivity-fault-management**—(Optional) Restart the process that provides IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management (CFM) database information for CFM maintenance association end points (MEPs) in a CFM session.

**ethernet-link-fault-management**—(EX Series switches and MX Series routers only) (Optional) Restart the process that provides the OAM link fault management (LFM) information for Ethernet interfaces.

**ethernet-switching**—(EX Series switches only) (Optional) Restart the Ethernet switching process.

**event-processing**—(Optional) Restart the event process (eventd).

**fibre-channel**—(QFX Series only) (Optional) Restart the Fibre Channel process.

**firewall**—(Optional) Restart the firewall management process, which manages the firewall configuration and enables accepting or rejecting packets that are transiting an interface on a router or switch.

**general-authentication-service**—(EX Series switches and MX Series routers only) (Optional) Restart the general authentication process.

**gracefully**—(Optional) Restart the software process.

**iccp-service**—(Optional) Restart the Inter-Chassis Communication Protocol (ICCP) process.

**idp-policy**—(Optional) Restart the intrusion detection and prevention (IDP) protocol process.

**immediately**—(Optional) Immediately restart the software process.

**interface-control**—(Optional) Restart the interface process, which controls the router's or switch's physical interface devices and logical interfaces.

**ipsec-key-management**—(Optional) Restart the IPsec key management process.

**isdn-signaling**—(J Series routers and QFX Series only) (Optional) Restart the ISDN signaling process, which initiates ISDN connections.

**kernel-replication**—(Optional) Restart the kernel replication process, which replicates the state of the backup Routing Engine when graceful Routing Engine switchover (GRES) is configured.

**l2-learning**—(Optional) Restart the Layer 2 address flooding and learning process.

**l2cpd-service**—(Optional) Restart the Layer 2 Control Protocol process, which enables features such as Layer 2 protocol tunneling and nonstop bridging.

**l2tp-service**—(M10, M10i, M7i, and MX Series routers only) (Optional) Restart the Layer 2 Tunneling Protocol (L2TP) process, which sets up client services for establishing Point-to-Point Protocol (PPP) tunnels across a network and negotiating Multilink PPP if it is implemented.

**l2tp-universal-edge**—(MX Series routers only) (Optional) Restart the L2TP process, which establishes L2TP tunnels and PPP sessions through L2TP tunnels.

**lACP**—(Optional) Restart the Link Aggregation Control Protocol (LACP) process. LACP provides a standardized means for exchanging information between partner systems on a link to allow their link aggregation control instances to reach agreement on the identity of the LAG to which the link belongs, and then to move the link to that LAG,

and to enable the transmission and reception processes for the link to function in an orderly manner.

**lcc *number***—(TX Matrix and TX Matrix Plus routers only) (Optional) For a TX Matrix router, restart the software process for a specific T640 router that is connected to the TX Matrix router. For a TX Matrix Plus router, restart the software process for a specific router that is connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**license-service**—(EX Series switches only) (Optional) Restart the feature license management process.

**link-management**—(TX Matrix and TX Matrix Plus routers and EX Series switches only) (Optional) Restart the Link Management Protocol (LMP) process, which establishes and maintains LMP control channels.

**lldpd-service**—(EX Series switches only) (Optional) Restart the Link Layer Discovery Protocol (LLDP) process.

**local**—(MX Series routers only) (Optional) Restart the software process for the local Virtual Chassis member.

**local-policy-decision-function**—(Optional) Restart the process for the Local Policy Decision Function, which regulates collection of statistics related to applications and application groups and tracking of information about dynamic subscribers and static interfaces.

**mac-validation**—(Optional) Restart the Media Access Control (MAC) validation process, which configures MAC address validation for subscriber interfaces created on demux interfaces in dynamic profiles on MX Series routers.

**member *member-id***—(MX Series routers only) (Optional) Restart the software process for a specific member of the Virtual Chassis configuration. Replace *member-id* with a value of 0 or 1.

**mib-process**—(Optional) Restart the Management Information Base (MIB) version II process, which provides the router's MIB II agent.

**mobile-ip**—(Optional) Restart the Mobile IP process, which configures Junos OS Mobile IP features.

**mountd-service**—(EX Series switches and MX Series routers only) (Optional) Restart the service for NFS mount requests.

**mpls-traceroute**—(Optional) Restart the MPLS Periodic Traceroute process.

**mspd**—(Optional) Restart the Multiservice process.

**multicast-snooping**—(EX Series switches and MX Series routers only) (Optional) Restart the multicast snooping process, which makes Layer 2 devices, such as VLAN switches, aware of Layer 3 information, such as the media access control (MAC) addresses of members of a multicast group.

**named-service**—(Optional) Restart the DNS Server process, which is used by a router or a switch to resolve hostnames into addresses.

**network-access-service**—(J Series routers and QFX Series only) (Optional) Restart the network access process, which provides the router's Challenge Handshake Authentication Protocol (CHAP) authentication service.

**nfsd-service**—(Optional) Restart the Remote NFS Server process, which provides remote file access for applications that need NFS-based transport.

**packet-triggered-subscribers**—(Optional) Restart the packet-triggered subscribers and policy control (PTSP) process, which allows the application of policies to dynamic subscribers that are controlled by a subscriber termination device.

**peer-selection-service**—(Optional) Restart the Peer Selection Service process.

**pgcp-service**—(Optional) Restart the pgcpd service process running on the Routing Engine. This option does not restart pgcpd processes running on mobile station PICs. To restart pgcpd processes running on mobile station PICs, use the **services pgcp gateway** option.

**pgm**—(Optional) Restart the process that implements the Pragmatic General Multicast (PGM) protocol for assisting in the reliable delivery of multicast packets.

**pic-services-logging**—(Optional) Restart the logging process for some PICs. With this process, also known as fsad (the file system access daemon), PICs send special logging information to the Routing Engine for archiving on the hard disk.

**pki-service**—(Optional) Restart the PKI Service process.

**ppp**—(Optional) Restart the Point-to-Point Protocol (PPP) process, which is the encapsulation protocol process for transporting IP traffic across point-to-point links.

**ppp-service**—(Optional) Restart the Universal Edge PPP process, which is the encapsulation protocol process for transporting IP traffic across Universal Edge routers.

**pppoe**—(Optional) Restart the Point-to-Point Protocol over Ethernet (PPPoE) process, which combines PPP that typically runs over broadband connections with the Ethernet link-layer protocol that allows users to connect to a network of hosts over a bridge or access concentrator.

**protected-system-domain-service**—(Optional) Restart the Protected System Domain (PSD) process.

**redundancy-interface-process**—(Optional) Restart the ASP redundancy process.

**remote-operations**—(Optional) Restart the remote operations process, which provides the ping and traceroute MIBs.

**root-system-domain-service**—(Optional) Restart the Root System Domain (RSD) service.

**routing**—(ACX Series routers, QFX Series, EX Series switches, and MX Series routers only) (Optional) Restart the routing protocol process.

**routing <logical-system *logical-system-name*>**—(Optional) Restart the routing protocol process, which controls the routing protocols that run on the router or switch and maintains the routing tables. Optionally, restart the routing protocol process for the specified logical system only.

**sampling**—(Optional) Restart the sampling process, which performs packet sampling based on particular input interfaces and various fields in the packet header.

**sbc-configuration-process**—(Optional) Restart the session border controller (SBC) process of the border signaling gateway (BSG).

**scc**—(TX Matrix routers only) (Optional) Restart the software process on the TX Matrix router (or switch-card chassis).

**sdk-service**—(Optional) Restart the SDK Service process, which runs on the Routing Engine and is responsible for communications between the SDK application and Junos OS. Although the SDK Service process is present on the router, it is turned off by default.

**secure-neighbor-discovery**—(QFX Series, EX Series switches, and MX Series routers only) (Optional) Restart the secure Neighbor Discovery Protocol (NDP) process, which provides support for protecting NDP messages.

**sfc *number***—(TX Matrix Plus routers only) (Optional) Restart the software process on the TX Matrix Plus router (or switch-fabric chassis). Replace ***number*** with **0**.

**service-deployment**—(Optional) Restart the service deployment process, which enables Junos OS to work with the Session and Resource Control (SRC) software.

**services**—(Optional) Restart a service.

**services pgcp gateway *gateway-name***—(Optional) Restart the pgcpd process for a specific border gateway function (BGF) running on an MS-PIC. This option does not restart the pgcpd process running on the Routing Engine. To restart the pgcpd process on the Routing Engine, use the **pgcp-service** option.

**sflow-service**—(EX Series switches only) (Optional) Restart the flow sampling (sFlow technology) process.

**snmp**—(Optional) Restart the SNMP process, which enables the monitoring of network devices from a central location and provides the router's or switch's SNMP master agent.

**soft**—(Optional) Reread and reactivate the configuration without completely restarting the software processes. For example, BGP peers stay up and the routing table stays constant. Omitting this option results in a graceful restart of the software process.

**static-subscribers**—(Optional) Restart the static subscribers process, which associates subscribers with statically configured interfaces and provides dynamic service activation and activation for these subscribers.

**statistics-service**—(Optional) Restart the process that manages the Packet Forwarding Engine statistics.

**subscriber-management**—(Optional) Restart the Subscriber Management process.

**subscriber-management-helper**—(Optional) Restart the Subscriber Management Helper process.

**tunnel-oamd**—(Optional) Restart the Tunnel OAM process, which enables the Operations, Administration, and Maintenance of Layer 2 tunneled networks. Layer 2 protocol tunneling (L2PT) allows service providers to send Layer 2 PDUs across the provider's cloud and deliver them to Juniper Networks EX Series Ethernet Switches that are not part of the local broadcast domain.

**usb-control**—(J Series routers and MX Series routers only) (Optional) Restart the USB control process.

**vrrp**—(ACX Series routers, EX Series switches, and MX Series routers only) (Optional) Restart the Virtual Router Redundancy Protocol (VRRP) process, which enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts.

**web-management**—(J Series routers, QFX Series, EX Series switches, and MX Series routers only) (Optional) Restart the Web management process.

**Required Privilege Level**    reset

**Related Documentation**

- *Overview of Junos OS CLI Operational Mode Commands*

**List of Sample Output**    [restart interfaces on page 199](#)

**Output Fields**    When you enter this command, you are provided feedback on the status of your request.



## Sample Output

restart interfaces

```
user@host> restart interfaces
interfaces process terminated
interfaces process restarted
```

## show ppp interface

<b>Syntax</b>	<code>show ppp interface <i>interface-name</i></code> <code>&lt;extensive  terse&gt;</code>
<b>Release Information</b>	Command introduced in Junos OS Release 7.5.
<b>Description</b>	Display information about PPP interfaces.
<b>Options</b>	<i>interface-name</i> —Name of a logical interface.  <b>extensive   terse</b> —(Optional) Display the specified level of output.
<b>Required Privilege Level</b>	view
<b>List of Sample Output</b>	<a href="#">show ppp interface on page 208</a> <a href="#">show ppp interface extensive on page 208</a> <a href="#">show ppp interface terse on page 208</a>
<b>Output Fields</b>	<a href="#">Table 11 on page 200</a> lists the output fields for the <b>show ppp interface</b> command. Output fields are listed in the approximate order in which they appear.

Table 11: show ppp interface Output Fields

Field Name	Field Description	Level of Output
<b>Session</b>	Name of the logical interface on which the session is running.	All levels
<b>Type</b>	Session type: PPP.	All levels
<b>Phase</b>	PPP process phase: <b>Authenticate</b> , <b>Pending</b> , <b>Establish</b> , <b>LCP</b> , <b>Network</b> , <b>Disabled</b> , and <b>Tunneled</b> .	All levels
<b>Session flags</b>	Special conditions present in the session: <b>Bundled</b> , <b>TCC</b> , <b>No-keepalives</b> , <b>Looped</b> , <b>Monitored</b> , and <b>NCP-only</b> .	All levels
<b><i>protocol</i> State</b>	Protocol state information. See specific protocol state fields for information.	None specified
<b>AUTHENTICATION</b>	Challenge-Handshake Authentication Protocol (CHAP) authentication state information or Password Authentication Protocol (PAP) state information. See the <b>Authentication</b> field description for further information.	None specified

Table 11: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Keepalive settings</b>	<p>Keepalive settings for the PPP sessions on the L2TP network server (LNS). LNS based PPP sessions are supported only on service interfaces (si).</p> <ul style="list-style-type: none"> <li>• <b>Interval</b>—Time in seconds between successive keepalive requests. Keepalive aging timeout is calculated as a product of the <b>interval</b> and <b>Down-count</b> values. If the keepalive aging timeout is greater than 180 seconds, the keepalive packets are handled by the Routing Engine. If the aging timeout is less than or equal to 180 seconds, the packets are handled by the Packet Forwarding Engine.</li> <li>• <b>Up-count</b>—The number of keepalive packets a destination must receive to change a link's status from down to up.</li> <li>• <b>Down-count</b>—The number of keepalive packets a destination must fail to receive before the network takes down a link.</li> </ul>	<b>extensive</b>
<b>RE Keepalive statistics</b>	<p>Keepalive statistics for the packets handled by the Routing Engine.</p> <ul style="list-style-type: none"> <li>• <b>LCP echo req Tx</b>—LCP echo requests sent from the Routing Engine.</li> <li>• <b>LCP echo req Rx</b>—LCP echo requests received at the Routing Engine.</li> <li>• <b>LCP echo rep Tx</b>—LCP echo responses sent from the Routing Engine.</li> <li>• <b>LCP echo rep Rx</b>—LCP echo responses received at the Routing Engine.</li> <li>• <b>LCP echo req timeout</b>—Number of keepalive packets where the keepalive aging timer has expired.</li> <li>• <b>LCP Rx echo req Magic Num Failures</b>—LCP echo requests where the magic numbers shared between the PPP peers during LCP negotiation did not match.</li> <li>• <b>LCP Rx echo rep Magic Num Failures</b>—LCP echo responses where the magic numbers shared between the PPP peers during LCP negotiation did not match.</li> </ul>	<b>extensive</b>

Table 11: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
LCP	<p><b>LCP information:</b></p> <ul style="list-style-type: none"> <li>• <b>State</b>—LCP protocol state (all platforms except M120 and M320 routers): <ul style="list-style-type: none"> <li>• <b>Ack-rcvd</b>—A Configure-Request has been sent and a Configure-Ack has been received.</li> <li>• <b>Ack-sent</b>—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.</li> <li>• <b>Closed</b>—Link is not available for traffic.</li> <li>• <b>Opened</b>—Link is administratively available for traffic.</li> <li>• <b>Req-sent</b>—An attempt has been made to configure the connection.</li> </ul> </li> <li>• <b>State</b>—LCP protocol state (M120 and M320 routers): <ul style="list-style-type: none"> <li>• <b>Ack-rcvd</b>—A Configure-Request has been sent and a Configure-Ack has been received.</li> <li>• <b>Ack-sent</b>—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.</li> <li>• <b>Closed</b>—Link is available (up), but no Open has occurred.</li> <li>• <b>Closing</b>—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.</li> <li>• <b>Opened</b>—Link is administratively available for traffic. A Configure-Ack has been both sent and received.</li> <li>• <b>Req-sent</b>—An attempt has been made to configure the connection. A Configure-Request has been sent but a Configure-Ack has not yet been received.</li> <li>• <b>Starting</b>—An administrative Open has been initiated, but the lower layer is still unavailable (Down).</li> <li>• <b>Stopped</b>—The system is waiting for a Down event after the This-Layer-Finished action, or after sending a Terminate-Ack.</li> <li>• <b>Stopping</b>—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.</li> </ul> </li> <li>• <b>Last started</b>—LCP state start time.</li> <li>• <b>Last completed</b>—LCP state completion time.</li> </ul>	extensive

Table 11: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
	<ul style="list-style-type: none"> <li>• <b>Negotiated options:</b> <ul style="list-style-type: none"> <li>• <b>ACFC</b>—Address and-Control Field Compression. A configuration option that provides a method to negotiate the compression of the Data Link Layer Address and Control fields.</li> <li>• <b>Asynchronous map</b>—Asynchronous control character map. A configuration option used on asynchronous links such as telephone lines to identify control characters that must be replaced by a two-character sequence to prevent them from being interpreted by equipment used to establish the link.</li> <li>• <b>Authentication protocol</b>—Protocol used for authentication. This option provides a method to negotiate the use of a specific protocol for authentication. It requires a peer to authenticate itself before allowing network-layer protocol packets to be exchanged. By default, authentication is not required.</li> <li>• <b>Authentication algorithm</b>—Type of authentication algorithm. The Message Digest algorithm (MD5) is the only algorithm supported.</li> <li>• <b>Endpoint discriminator class</b>—For multilink PPP (MLPPP), a configuration option that identifies the system transmitting the packet. This option advises a system that the peer on this link could be the same as the peer on another existing link.</li> <li>• <b>Magic number</b>—A configuration option that provides a method to detect looped-back links and other data-link layer anomalies. By default, the magic number is not negotiated.</li> <li>• <b>MRU</b>—Maximum receive unit. A configuration option that may be sent to inform the peer that the implementation can receive larger packets, or to request that the peer send smaller packets. The default value is 1500 octets.</li> <li>• <b>MRRU</b>—For multilink PPP, the maximum receive reconstructed unit. A configuration option that specifies the maximum number of octets in the Information fields of reassembled packets.</li> <li>• <b>Multilink header suspendable classes</b>—For MLPPP, an LCP option that advises the peer that the implementation wishes to receive fragments with a format given by the code number, with the maximum number of suspendable classes given.</li> <li>• <b>Multilink header format classes</b>—For MLPPP, an LCP option that advises the peer that the implementation wishes to receive fragments with a format given by the code number.</li> <li>• <b>PFC</b>—Protocol-Field-Compression. A configuration option that provides a method to negotiate the compression of the PPP Protocol field.</li> <li>• <b>short sequence</b>—For MLPPP, an option that advises the peer that the implementation wishes to receive fragments with short, 12-bit sequence numbers.</li> </ul> </li> </ul>	

Table 11: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Authentication</b>	<p>CHAP or PAP authentication state information. For CHAP authentication:</p> <ul style="list-style-type: none"> <li>• <b>Chap-ans-rcvd</b>—Packet was sent from the peer, indicating that the peer received the <b>Chap-resp-sent</b> packet.</li> <li>• <b>Chap-ans-sent</b>—Packet was sent from the authenticator, indicating that the authenticator received the peer's <b>Chap-resp-rcvd</b> packet.</li> <li>• <b>Chap-chal-rcvd</b>—Challenge packet has been received by the peer.</li> <li>• <b>Chap-chal-sent</b>—Challenge packet has been sent by the authenticator to begin the CHAP protocol or has been transmitted at any time during the Network-Layer Protocol (NCP) phase to ensure that the connection has not been altered.</li> <li>• <b>Chap-resp-rcvd</b>—CHAP response packet has been received by the authenticator.</li> <li>• <b>Chap-resp-sent</b>—CHAP response packet has been sent to the authenticator.</li> <li>• <b>Closed</b>—Link is not available for authentication.</li> <li>• <b>Failure</b>—Authenticator compares the response value in the response packet from the peer with its own response value, but the value does not match. Authentication fails.</li> <li>• <b>Success</b>—Authenticator compares the response value in the response packet from the peer with its own response value, and the value matches. Authentication is successful.</li> </ul> <p>For PAP authentication:</p> <ul style="list-style-type: none"> <li>• <b>Pap-resp-sent</b>—PAP response sent to peer (ACK/NACK).</li> <li>• <b>Pap-req-rcvd</b>—PAP request packet received from peer.</li> <li>• <b>Pap-resp-rcvd</b>—PAP response received from the peer (ACK/NACK).</li> <li>• <b>Pap-req-sent</b>—PAP request packet sent to the peer.</li> <li>• <b>Closed</b>—Link is not available for authentication.</li> <li>• <b>Failure</b>—Authenticator compares the response value in the response packet from the peer with its own response value, but the value does not match. Authentication fails.</li> <li>• <b>Success</b>—Authenticator compares the response value in the response packet from the peer with its own response value, and the value matches. Authentication is successful.</li> </ul>	None specified

Table 11: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
IPCP	<p>Internet Protocol Control Protocol (IPCP) information.</p> <ul style="list-style-type: none"> <li>• <b>State</b>—(All platforms except M120 and M320 routers) One of the following values: <ul style="list-style-type: none"> <li>• <b>Ack-rcvcd</b>—A Configure-Request has been sent and a Configure-Ack has been received.</li> <li>• <b>Ack-sent</b>—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.</li> <li>• <b>Closed</b>—Link is not available for traffic.</li> <li>• <b>Opened</b>—Link is administratively available for traffic.</li> <li>• <b>Req-sent</b>—An attempt has been made to configure the connection.</li> </ul> </li> <li>• <b>State</b>—(M120 and M320 routers) One of the following values: <ul style="list-style-type: none"> <li>• <b>Ack-rcvcd</b>—A Configure-Request has been sent and a Configure-Ack has been received.</li> <li>• <b>Ack-sent</b>—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.</li> <li>• <b>Closed</b>—Link is available (up), but no Open has occurred.</li> <li>• <b>Closing</b>—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.</li> <li>• <b>Opened</b>—Link is administratively available for traffic. A Configure-Ack has been both sent and received.</li> <li>• <b>Req-sent</b>—An attempt has been made to configure the connection. A Configure-Request has been sent but a Configure-Ack has not yet been received.</li> <li>• <b>Starting</b>—An administrative Open has been initiated, but the lower layer is still unavailable (Down).</li> <li>• <b>Stopped</b>—The system is waiting for a Down event after the This-Layer-Finished action, or after sending a Terminate-Ack.</li> <li>• <b>Stopping</b>—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.</li> </ul> </li> <li>• <b>Last started</b>—IPCP state start time.</li> <li>• <b>Last completed</b>—IPCP state authentication completion time.</li> <li>• <b>Negotiated options</b>: <ul style="list-style-type: none"> <li>• <b>compression protocol</b>—Negotiate the use of a specific compression protocol. By default, compression is not enabled.</li> <li>• <b>local address</b>—Desired local address of the sender of a Configure-Request. If all four octets are set to zero, the peer provides the IP address.</li> <li>• <b>primary DNS server</b>—Negotiate with the remote peer to select the address of the primary DNS server to be used on the local end of the link.</li> <li>• <b>primary WINS server</b>—Negotiate with the remote peer to select the address of the primary WINS server to be used on the local end of the link.</li> <li>• <b>remote address</b>—IP address of the remote end of the link in dotted quad notation.</li> <li>• <b>secondary DNS server</b>—Negotiate with the remote peer to select the address of the secondary DNS server to be used on the local end of the link.</li> <li>• <b>secondary WINS server</b>—Negotiate with the remote peer to select the address of the secondary WINS server to be used on the local end of the link.</li> </ul> </li> <li>• <b>Negotiation mode</b>—PPP Network Control Protocol (NCP) negotiation mode configured for IPCP: <b>Active</b> or <b>Passive</b></li> </ul>	extensive

Table 11: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
IPV6CP	<p>Internet Protocol version 6 Control Protocol (IPv6CP) information.</p> <ul style="list-style-type: none"> <li>• <b>State</b>—(All platforms except M120 and M320 routers) One of the following values: <ul style="list-style-type: none"> <li>• <b>Ack-rcvd</b>—A Configure-Request has been sent and a Configure-Ack has been received.</li> <li>• <b>Ack-sent</b>—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.</li> <li>• <b>Closed</b>—Link is not available for traffic.</li> <li>• <b>Opened</b>—Link is administratively available for traffic.</li> <li>• <b>Req-sent</b>—An attempt has been made to configure the connection.</li> </ul> </li> <li>• <b>State</b>—(M120 and M320 routers) One of the following values: <ul style="list-style-type: none"> <li>• <b>Ack-rcvd</b>—A Configure-Request has been sent and a Configure-Ack has been received.</li> <li>• <b>Ack-sent</b>—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.</li> <li>• <b>Closed</b>—Link is available (up), but no Open has occurred.</li> <li>• <b>Closing</b>—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.</li> <li>• <b>Opened</b>—Link is administratively available for traffic. A Configure-Ack has been both sent and received.</li> <li>• <b>Req-sent</b>—An attempt has been made to configure the connection. A Configure-Request has been sent but a Configure-Ack has not yet been received.</li> <li>• <b>Starting</b>—An administrative Open has been initiated, but the lower layer is still unavailable (Down).</li> <li>• <b>Stopped</b>—The system is waiting for a Down event after the This-Layer-Finished action, or after sending a Terminate-Ack.</li> <li>• <b>Stopping</b>—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.</li> </ul> </li> <li>• <b>Last started</b>—IPv6CP state start time.</li> <li>• <b>Last completed</b>—IPv6CP state authentication completion time.</li> <li>• <b>Negotiated options</b>: <ul style="list-style-type: none"> <li>• <b>local interface identifier</b>—Desired local address of the sender of a Configure-Request. If all four octets are set to zero, the peer provides the IP address.</li> <li>• <b>remote interface identifier</b>—IP address of the remote end of the link in dotted quad notation.</li> </ul> </li> <li>• <b>Negotiation mode</b>—PPP Network Control Protocol (NCP) negotiation mode configured for IPv6CP: <b>Active</b> or <b>Passive</b></li> </ul>	extensive



Table 11: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
OSINLCP State	<p>OSI Network Layer Control Protocol (OSINLCP) protocol state information (all platforms except M120 and M320 routers):</p> <ul style="list-style-type: none"> <li>• <b>State:</b> <ul style="list-style-type: none"> <li>• <b>Ack-rcvd</b>—Configure-Request has been sent and Configure-Ack has been received.</li> <li>• <b>Ack-sent</b>—Configure-Request and Configure-Ack have both been sent, but Configure-Ack has not yet been received.</li> <li>• <b>Closed</b>—Link is not available for traffic.</li> <li>• <b>Opened</b>—Link is administratively available for traffic.</li> <li>• <b>Req-sent</b>—Attempt has been made to configure the connection.</li> </ul> </li> <li>• <b>Last started</b>—OSINLCP state start time.</li> <li>• <b>Last completed</b>—OSINLCP state completion time.</li> </ul>	extensive
TAGCP	<p>TAGCP information.</p> <ul style="list-style-type: none"> <li>• <b>State</b>—(All platforms except M120 and M320 routers) One of the following values: <ul style="list-style-type: none"> <li>• <b>Ack-rcvd</b>—A Configure-Request has been sent and a Configure-Ack has been received.</li> <li>• <b>Ack-sent</b>—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.</li> <li>• <b>Closed</b>—Link is not available for traffic.</li> <li>• <b>Opened</b>—Link is administratively available for traffic.</li> <li>• <b>Req-sent</b>—An attempt has been made to configure the connection.</li> </ul> </li> <li>• <b>State</b>—(M120 and M320 routers) One of the following values: <ul style="list-style-type: none"> <li>• <b>Ack-rcvd</b>—A Configure-Request has been sent and a Configure-Ack has been received.</li> <li>• <b>Ack-sent</b>—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.</li> <li>• <b>Closed</b>—Link is available (up), but no Open has occurred.</li> <li>• <b>Closing</b>—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.</li> <li>• <b>Opened</b>—Link is administratively available for traffic. A Configure-Ack has been both sent and received.</li> <li>• <b>Req-sent</b>—An attempt has been made to configure the connection. A Configure-Request has been sent but a Configure-Ack has not yet been received.</li> <li>• <b>Starting</b>—An administrative Open has been initiated, but the lower layer is still unavailable (Down).</li> <li>• <b>Stopped</b>—The system is waiting for a Down event after the This-Layer-Finished action, or after sending a Terminate-Ack.</li> <li>• <b>Stopping</b>—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.</li> </ul> </li> <li>• <b>Last started</b>—TAGCP state start time.</li> <li>• <b>Last completed</b>—TAGCP state authentication completion time.</li> </ul>	extensive none

## Sample Output

### show ppp interface

```
user@host> show ppp interface si-1/3/0.0
Session si-1/3/0.0, Type: PPP, Phase: Authenticate
Session flags: Monitored
LCP State: Opened
AUTHENTICATION: CHAP State: Chap-resp-sent, Chap-ans-sent
IPCP State: Closed, OSINLCP State: Closed
```

### show ppp interface extensive

```
user@host> show ppp interface si-0/0/3.0 extensive

Session si-0/0/3.0, Type: PPP, Phase: Network
Keepalive settings: Interval 30 seconds, Up-count 1, Down-count 3
RE Keepalive statistics:
LCP echo req Tx      : 657 (last sent 00:50:10 ago)
LCP echo req Rx      : 0 (last seen: never)
LCP echo rep Tx      : 0
LCP echo rep Rx      : 657
LCP echo req timeout : 0
LCP Rx echo req Magic Num Failures : 0
LCP Rx echo rep Magic Num Failures : 0
LCP
State: Opened
Last started: 2007-01-29 10:43:50 PST
Last completed: 2007-01-29 10:43:50 PST
Negotiated options:
Authentication protocol: PAP, Magic number: 2341124815, MRU: 4470
Authentication: PAP
State: Success
Last started: 2007-01-29 10:43:50 PST
Last completed: 2007-01-29 10:43:50 PST
IPCP
State: Opened
Last started: 2007-01-29 10:43:50 PST
Last completed: 2007-01-29 10:43:50 PST
Negotiated options:
Local address: 10.10.10.1, Remote address: 10.10.10.2
Negotiation mode: Active
IPV6CP
State: Opened
Last started: 2007-01-29 10:43:50 PST
Last completed: 2007-01-29 10:43:50 PST
Negotiated options:
Local interface identifier: 2a0:a522:64:d319, Remote interface identifier: 0:0:0:c
Negotiation mode: Passive
```

### show ppp interface terse

```
user@host> show ppp interface si-1/3/0 terse
Session name  Session type  Session phase  Session flags
si-1/3/0.0    PPP           Authenticate   Monitored
```

## show services inline ip-reassembly statistics

**Syntax** `show services inline ip-reassembly statistics`  
`<fpc fpc-slot>`  
`<pfe pfe-slot>`

**Release Information** Statement introduced in Junos OS Release 12.2X49.

**Description** Display the inline IP reassembly statistics for the Packet Forwarding Engines on one or more MPCs. Inline IP reassembly statistics are collected at the Packet Forwarding Engine level.



**NOTE:** For more information on MPCs that support inline IP reassembly, refer to *Protocols and Applications Supported by MX240, MX480, MX960, MX2010, and MX2020 Enhanced MPCs (MPCEs)*.

**Options** `none`—Displays standard inline IP reassembly statistics for all MPCs.

`fpc fpc`—(Optional) Displays inline IP reassembly statistics for the specified MPC.

`pfe pfe`—(Optional) Displays inline IP reassembly for the specified Packet Forwarding Engine slot. You must specify an FPC slot number before specifying a Packet Forwarding Engine slot.

**Required Privilege Level** view

**Related Documentation** • [ip-reassembly on page 123](#)

**List of Sample Output** [show services inline ip-reassembly statistics fpc on page 213](#)

**Output Fields** [Table 12 on page 209](#) lists the output fields for the `show services inline ip-reassembly statistics` command. Output fields are listed in the approximate order in which they appear.

**Table 12: show services inline ip-reassembly statistics Output Fields**

Field Name	Field Description
FPC	MPC slot number for which the statistics are displayed.
PFE	Packet Forwarding Engine on the MPC for which the statistics are displayed.

Table 12: show services inline ip-reassembly statistics Output Fields (*continued*)

Field Name	Field Description
<p><b>NOTE:</b> The output fields displayed (per Packet Forwarding Engine) are arranged in a logical sequence from top to bottom to enable users to understand how the inline IP reassembly statistics are gathered.</p> <p>The information about total number of fragments received is displayed first, and then the information about the reassembled packets and those pending reassembly are displayed. Then, the reasons why the fragments were dropped or not reassembled are displayed. Finally, the information about the fragments reassembled, fragments dropped, and fragments sent to the backup user plane PIC (services PIC) are displayed.</p>	
<b>Total Fragments Received</b>	<p>Total number of fragments received and the current rate of fragments received for inline IP reassembly. The following information is also displayed:</p> <ul style="list-style-type: none"> <li>• <b>First Fragments</b>—Number of first fragments received and current rate of first fragments processed.</li> <li>• <b>Intermediate Fragments</b>—Number of intermediate fragments received and current rate of intermediate fragments processed.</li> <li>• <b>Last Fragments</b>—Number and rate of last fragments received.</li> </ul> <p><b>NOTE:</b> Current rate refers to the current number of fragments processed per second in the instant preceding the command's execution.</p>
<b>Total Packets Reassembled</b>	Total number of packets reassembled and current rate, in the instant preceding the command's execution, at which the packets are reassembled.
<b>Approximate Packets Pending Reassembly</b>	Approximate number of packets pending reassembly.

Table 12: show services inline ip-reassembly statistics Output Fields (*continued*)

Field Name	Field Description
<b>Fragments Dropped Reasons</b>	<p>Total number of fragments dropped reasons and the current rate of total fragment dropped reasons. The number of dropped reasons and rate corresponding to each of the following reasons are also displayed:</p> <ul style="list-style-type: none"> <li>• Buffers not available</li> <li>• Fragments per packet exceeded</li> <li>• Packet length exceeded</li> <li>• Record insert error</li> <li>• Record in use error</li> <li>• Duplicate first fragments</li> <li>• Duplicate last fragments</li> <li>• Missing first fragment</li> </ul> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• These fields indicate <i>why</i> a fragment was dropped. When a fragment is dropped, the corresponding reason field is incremented by 1. For example, when a fragment is dropped because the memory runs out, the <b>Buffers not available</b> field increases by 1.</li> <li>• The maximum number of fragments allowed for reassembly is 16. If the interface encounters a 17th fragment, it drops the entire packet and increments the <b>Fragment per packet exceeded</b> field by 17.</li> <li>• Current rate refers to the current number of fragment dropped reasons per second in the instant preceding the command's execution.</li> </ul>
<b>Reassembly Errors Reasons</b>	<p>Number of errors during reassembly and the current rate of reassembly errors. The number of errors and the rate for each of the following types of errors are also displayed:</p> <ul style="list-style-type: none"> <li>• Fragment not found</li> <li>• Fragment not in sequence</li> <li>• ASIC errors</li> </ul> <p><b>NOTE:</b> Current rate refers to the current number of reassembly errors processed per second in the instant preceding the command's execution.</p>
<b>Aged out packets</b>	<p>Number of aged out packets and the current number of packets aged out per second in the instant preceding the command's execution.</p> <p><b>NOTE:</b> In some cases, aged out packets can refer to aged out fragments. If previous fragments of the packet have already been discarded then linking of the dropped fragments to the aged out fragments cannot occur.</p>
<b>Total Fragments Successfully Reassembled</b>	<p>Number of fragments successfully reassembled and the current number of fragments reassembled per second in the instant preceding the command's execution.</p>

Table 12: show services inline ip-reassembly statistics Output Fields (*continued*)

Field Name	Field Description
<b>Total Fragments Dropped</b>	<p>Total number of fragments dropped and the current rate of total number of fragments dropped. The number of fragments dropped and rate corresponding to each of the following reasons are also displayed:</p> <ul style="list-style-type: none"> <li>• Buffers not available</li> <li>• Fragments per packet exceeded</li> <li>• Packet length exceeded</li> <li>• Record insert error</li> <li>• Record in use error</li> <li>• Duplicate first fragments</li> <li>• Duplicate last fragments</li> <li>• Missing first fragment</li> <li>• Fragment not found</li> <li>• Fragment not in sequence</li> <li>• ASIC errors</li> <li>• Aged out fragments</li> </ul>
<b>Total fragments punted to UPIC</b>	Number of fragments sent to the backup user plane PIC (services PIC) and current rate of fragments sent per second in the instant preceding the command's execution

The following information applies to the **Total Fragments Dropped** field.

The following information applies to the **Total Fragments Dropped** field.

- These fields indicate *how many* of the packet fragments received were then dropped due to a particular reason.

For example, consider a packet that has 10 fragments, 9 of which have been received and stored in memory. When the tenth fragment arrives, if the memory runs out (Buffers not available), then this fragment is dropped. Because the tenth fragment has been dropped, the other 9 fragments must also be dropped. In this case, the **Buffers not available** field (under the **Fragments Dropped Reasons** field) is incremented by 1 and the **Buffers not available** field (under the **Total Fragments Dropped** field) is incremented by 10.

For the next packet arriving, which also has 10 fragments, the first four fragments are stored but the memory runs out for the fifth fragment. Then the first 5 fragments (fifth and the first four) are dropped. In this case, the **Buffers not available** field (under the **Fragments Dropped Reasons** field) is incremented by 1 and the **Buffers not available** field (under the **Total Fragments Dropped** field) is incremented by 5.

For the remaining fragments of the packet, if memory becomes available, the next 5 fragments (6 through 10) that arrive are stored in memory. The fragments are stored until the timeout period elapses, and are eventually dropped. In this case, the **Aged out packets** field is incremented by 1 and the **Aged out fragments** field (under the **Total Fragments Dropped** field) is incremented by 5.

The fragment counters (after both packets have been processed) are as follows:

- **Fragments Dropped Reasons**
  - Buffers not available 2
  - Aged out packets 1
- **Total Fragment Dropped**
  - Buffers not available 15
  - Aged out packets 5
- Current rate refers to the current total number fragments dropped per second in the instant preceding the command's execution.

## Sample Output

show services inline ip-reassembly statistics fpc

```

user@host> show services inline ip-reassembly statistics fpc 0
FPC: 0 PFE: 0
=====

```

	Total	Current Rate
Total Fragments Received	728177644	83529
First Fragments	260759430	29924
Intermediate Fragments	206658784	23681
Last Fragments	260759430	29924
Total Packets Successfully Reassembled	260746982	29924
Approximate Packets Pending Reassembly	4	
Fragments Dropped Reasons	34558	3
Buffers not available	0	0
Fragments per packet exceeded	0	0
Packet length exceeded	0	0
Record insert error	0	0
Record in use error	34558	3
Duplicate first fragments	0	0
Duplicate last fragments	0	0
Missing first fragment	0	0
Reassembly Errors Reasons	0	0
Fragment not found	0	0
Fragment not in sequence	0	0
ASIC errors	0	0
Aged out packets	63	0
Total Fragments Successfully Reassembled	728142977	83528
Total Fragments Dropped	34673	3
Buffers not available	0	0
Fragments per packet exceeded	0	0
Packet length exceeded	0	0
Record insert error	0	0
Record in use error	34558	3
Duplicate first fragments	0	0

Duplicate last fragments	0	0
Missing first fragment	0	0
Fragment not found	0	0
Fragment not in sequence	0	0
ASIC errors	0	0
Aged out fragments	115	0
Total fragments punted to UPIC	0	0



## show services l2tp destination

<b>Syntax</b>	show services l2tp destination <brief   detail   extensive> <local-gateway <i>gateway-address</i> > <peer-gateway <i>gateway-address</i> > <statistics>
<b>Release Information</b>	Command introduced in Junos OS Release 10.4.
<b>Description</b>	Display information about L2TP tunnel destinations.
<b>Options</b>	<p><b>brief   detail   extensive</b>—(Optional) Display the specified level of information.</p> <p><b>local-gateway <i>gateway-address</i></b>—(Optional) Display L2TP session information for only the specified local gateway address.</p> <p><b>peer-gateway <i>gateway-address</i></b>—(Optional) Display L2TP session information for only the specified peer gateway address.</p> <p><b>statistics</b>—(Optional) Display the number of control packets and bytes transmitted and received for the destination. You cannot include this option with any of the level options, <b>brief</b>, <b>detail</b>, or <b>extensive</b>.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear services l2tp destination on page 180</a></li> <li>• <a href="#">show services l2tp destination lockout on page 219</a></li> <li>• <a href="#">show services l2tp session on page 220</a></li> <li>• <a href="#">show services l2tp summary on page 244</a></li> <li>• <a href="#">show services l2tp tunnel on page 249</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show services l2tp destination on page 217</a> <a href="#">show services l2tp destination detail on page 217</a> <a href="#">show services l2tp destination extensive (LAC) on page 218</a> <a href="#">show services l2tp destination extensive (LNS) on page 218</a> <a href="#">show services l2tp destination statistics (LAC only on MX Series Routers) on page 218</a>
<b>Output Fields</b>	Table 13 on page 215 lists the output fields for the <b>show services l2tp destination</b> command. Output fields are listed in the approximate order in which they appear.

Table 13: show services l2tp destination Output Fields

Field Name	Field Description	Level of Output
Local Name	Name of this destination.	All levels
Remote IP	IP address of the remote peer (LNS).	All levels

Table 13: show services l2tp destination Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Tunnels</b>	Number of tunnel connections for the destination in the following categories:	All levels for total
	Number of tunnel connections for the destination in the following categories: <ul style="list-style-type: none"> <li>• total</li> <li>• active</li> <li>• failed</li> </ul>	<b>extensive</b> for active and failed
<b>Sessions</b>	Number of session connections for the destination in the following categories:	All levels for total
	Number of session connections for the destination in the following categories: <ul style="list-style-type: none"> <li>• total</li> <li>• active</li> <li>• failed</li> </ul>	<b>extensive</b> for active and failed
<b>State</b>	Administrative state of the L2TP destination:	All levels
	Administrative state of the L2TP destination: <ul style="list-style-type: none"> <li>• <b>Enabled</b>—No restrictions exist on creation or operation of sessions and tunnels for this destination.</li> <li>• <b>Disabled</b>—Existing sessions and tunnels for this destination have been disabled and no new sessions or tunnels are created while in the <b>Disabled</b> state.</li> </ul>	
<b>Local IP</b>	IP address of the local gateway (LAC).	<b>detail extensive</b>
<b>Transport</b>	Medium used for tunneling. Only <b>ipUdp</b> is supported.	<b>detail extensive</b>
<b>Logical System</b>	Logical system in which the tunnel is configured.	<b>detail extensive</b>
<b>Router Instance</b>	Routing instance in which the tunnel is configured.	<b>detail extensive</b>
<b>Lockout State</b>	Reachability state of the destination:	<b>detail extensive</b>
	Reachability state of the destination: <ul style="list-style-type: none"> <li>• <b>not locked</b>—Destination is considered reachable.</li> <li>• <b>waiting for lockout timeout</b>—Destination is locked out by L2TP because it is unreachable, so no attempts are made to reach the destination until the lockout timeout (300 seconds) expires, unless this is the only destination available for tunneling the subscriber.</li> </ul>	

Table 13: show services l2tp destination Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Access Line Information</b>	<p>State of tunnel support for L2TP AVPs that report attributes and traffic rates for subscriber access lines:</p> <p>State of tunnel support for L2TP AVPs that report attributes and traffic rates for subscriber access lines:</p> <ul style="list-style-type: none"> <li>• <b>enabled</b></li> <li>• <b>disabled</b></li> </ul>	<b>detail extensive</b>
<b>Speed Updates</b>	<p>State of tunnel support for L2TP AVP 97, which reports connection speed changes for subscriber access lines:</p> <p>State of tunnel support for L2TP AVP 97, which reports connection speed changes for subscriber access lines:</p> <ul style="list-style-type: none"> <li>• <b>enabled</b></li> <li>• <b>disabled</b></li> </ul>	<b>detail extensive</b>
<b>Connections</b>	Number of total, active, and failed tunnel and session connections for the destination.	<b>extensive</b>
<b>Control Tx</b>	Amount of control information transmitted, in packets and bytes.	<b>statistics</b>
<b>Control Rx</b>	Amount of control information received, in packets and bytes.	<b>statistics</b>
<b>Data Tx</b>	Amount of data transmitted, in packets and bytes.	<b>statistics</b>
<b>Data Rx</b>	Amount of data received, in packets and bytes.	<b>statistics</b>
<b>Error Tx</b>	Number of errors transmitted, in packets.	<b>statistics</b>
<b>Error Rx</b>	Number of errors received, in packets.	<b>statistics</b>

## Sample Output

### show services l2tp destination

```

user@host> show services l2tp destination
  Local Name  Remote IP    Tunnels    Sessions  State
  1           10.10.1.1    1           1         Enabled

```

### show services l2tp destination detail

```

user@host> show services l2tp destination detail
Local name: 1
Remote IP: 10.1.1.1
Tunnels: 1, Sessions: 1
State: Enabled
Local IP: 10.1.1.2
Transport: ipUdp, Logical System: default, Router Instance: default
Lockout State: not locked
Access Line Information: enabled, Speed Updates: enabled

```

```
Local name: 1
Remote IP: 10.1.1.8
Tunnels: 1, Sessions: 1
State: Enabled
Local IP: 10.1.1.2
Transport: ipUdp, Logical System: default, Router Instance: default
Lockout State: waiting for lockout timeout
Access Line Information: enabled, Speed Updates: enabled
```

#### show services l2tp destination extensive (LAC)

```
user@host> show services l2tp destination extensive
Local name: 1
Remote IP: 10.1.1.1
State: Enabled
Local IP: 10.1.1.2
Transport: ipUdp, Logical System: default, Router Instance: default
Lockout State: not locked
Access Line Information: enabled, Speed Updates: enabled
Connections      Totals      Active      Failed
Tunnels          1           1           0
Sessions         1           1           0
```

#### show services l2tp destination extensive (LNS)

```
user@host> show services l2tp destination extensive
Local name: 3
Remote IP: 11.1.1.3
State: Enabled
Local IP: 11.1.1.2
Transport: ipUdp, Logical System: default, Router Instance: default
Lockout State: not locked
Connections      Totals      Active      Failed
Tunnels          1           1           0
Sessions         1           1           0
```

#### show services l2tp destination statistics (LAC only on MX Series Routers)

```
user@host> show services l2tp destination statistics
Local name: 2, Tunnels: 1, Sessions: 210
Packets  Bytes
Control Tx    680  63.3k
Control Rx    283  10.6k
Data Tx      1129  14.3k
Data Rx       877  10.9k
Errors Tx         0
Errors Rx         0
```

## show services l2tp destination lockdown

<b>Syntax</b>	<b>show services l2tp destination lockdown</b>
<b>Release Information</b>	Command introduced in Junos OS Release 13.2.
<b>Description</b>	Display a list of destinations that are currently locked out and the time remaining for each to remain in the lockdown state.
<b>Options</b>	This command has no options.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear services l2tp destination on page 180</a></li> <li>• <a href="#">request services l2tp destination unlock on page 148</a></li> <li>• <a href="#">show services l2tp destination on page 215</a></li> <li>• <a href="#">show services l2tp session on page 220</a></li> <li>• <a href="#">show services l2tp summary on page 244</a></li> <li>• <a href="#">show services l2tp tunnel on page 249</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show services l2tp destination lockdown on page 219</a>
<b>Output Fields</b>	Table 14 on page 219 lists the output fields for the <b>show services l2tp destination lockdown</b> command. Output fields are listed in the approximate order in which they appear.

**Table 14: show services l2tp destination lockdown Output Fields**

Field Name	Field Description
<b>Destination</b>	Name of the destination.
<b>Time Remaining</b>	Time remaining for the destination to be locked out.
<b>L2TP lockdown destinations found</b>	Total count of lockdown destinations.

## Sample Output

### show services l2tp destination lockdown

```

user@host> show services l2tp destination lockdown
  Destination  Time Remaining
  4            45
  5            43
  6            8
3 L2TP lockdown destinations found

```

## show services l2tp session

---

**Syntax**    show services l2tp session  
              <brief | detail | extensive>  
              <interface *interface-name*>  
              <local-gateway *gateway-address*>  
              <local-gateway-name *gateway-name*>  
              <local-session-id *session-id*>  
              <local-tunnel-id *tunnel-id*>  
              <peer-gateway *gateway-address*>  
              <peer-gateway-name *gateway-name*>  
              <statistics>  
              <tunnel-group *group-name*>  
              <user *username*>

**Release Information**    Command introduced before Junos OS Release 7.4.  
                              Support for LAC on MX Series routers introduced in Junos OS Release 10.4.  
                              Support for LNS on MX Series routers introduced in Junos OS Release 11.4.

**Description**    (M10i and M7i routers only) Display information about active L2TP sessions for LNS.  
  
                      (MX Series routers only) Display information about active L2TP sessions for LAC and LNS.

**Options**    **none**—Display standard information about all active L2TP sessions.

**brief | detail | extensive**—(Optional) Display the specified level of output.

**interface *interface-name***—(Optional) Display L2TP session information for only the specified adaptive services or inline services interface. The interface type depends on the line card as follows:

- **si-*fpc/pic/port***—MPCs on MX Series routers only. This option is not available for L2TP on M Series routers.
- **sp-*fpc/pic/port***—AS or Multiservices PICs on M7i, M10i, and M120 routers only. This option is not available for L2TP on MX Series routers.

**local-gateway *gateway-address***—(Optional) Display L2TP session information for only the specified local gateway address.

**local-gateway-name *gateway-name***—(Optional) Display L2TP session information for only the specified local gateway name.

**local-session-id *session-id***—(Optional) Display L2TP session information for only the specified local session identifier.

**local-tunnel-id *tunnel-id***—(Optional) Display L2TP session information for only the specified local tunnel identifier.

**peer-gateway *gateway-address***—(Optional) Display L2TP session information for only the specified peer gateway address.

**peer-gateway-name gateway-name**—(Optional) Display L2TP session information for only the specified peer gateway name.

**statistics**—(Optional) Display the number of control packets and bytes transmitted and received for the session. You cannot include this option with any of the level options, **brief**, **detail**, or **extensive**.

**tunnel-group group-name**—(Optional) Display L2TP session information for only the specified tunnel group. To display information about L2TP CPU and memory usage, you can include the tunnel group name in the **show services service-sets memory-usage group-name** and **show services service-sets cpu-usage group-name** commands. This option is not available for L2TP LAC on MX Series routers.

**user username**—(M Series routers only) (Optional) Display L2TP session information for only the specified username.

**Required Privilege Level**

view

**Related Documentation**

- [L2TP Services Configuration Overview](#)
- [L2TP Minimum Configuration](#)
- [clear services l2tp session on page 181](#)

**List of Sample Output**

[show services l2tp session \(LNS on M Series Routers\) on page 224](#)  
[show services l2tp session \(LNS on MX Series Routers\) on page 224](#)  
[show services l2tp session \(LAC\) on page 224](#)  
[show services l2tp session detail \(LAC\) on page 224](#)  
[show services l2tp session extensive \(LAC\) on page 225](#)  
[show services l2tp session extensive \(LAC on MX Series Routers\) on page 225](#)  
[show services l2tp session extensive \(LNS on M Series Routers\) on page 225](#)  
[show services l2tp session extensive \(LNS on MX Series Routers\) on page 226](#)  
[show services l2tp session statistics \(MX Series Routers\) on page 226](#)

**Output Fields** [Table 15 on page 221](#) lists the output fields for the **show services l2tp session** command. Output fields are listed in the approximate order in which they appear.

**Table 15: show services l2tp session Output Fields**

Field Name	Field Description	Level of Output
<b>Interface</b>	(LNS only) Name of an adaptive services interface.	All levels
<b>Tunnel group</b>	(LNS only) Name of a tunnel group.	All levels
<b>Tunnel local ID</b>	Identifier of the local endpoint of the tunnel, as assigned by the L2TP network server (LNS).	All levels
<b>Session local ID</b>	Identifier of the local endpoint of the L2TP session, as assigned by the LNS.	All levels

Table 15: show services l2tp session Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Session remote ID</b>	Identifier of the remote endpoint of the L2TP session, as assigned by the L2TP access concentrator (LAC).	All levels
<b>State</b>	State of the L2TP session: <ul style="list-style-type: none"> <li>• <b>Established</b>—Session is operating. This is the only state supported for the LAC.</li> <li>• <b>closed</b>—Session is being closed.</li> <li>• <b>destroyed</b>—Session is being destroyed.</li> <li>• <b>clean-up</b>—Session is being cleaned up.</li> <li>• <b>lns-ic-accept-new</b>—New session is being accepted.</li> <li>• <b>lns-ic-idle</b>—Session has been created and is idle.</li> <li>• <b>lns-ic-reject-new</b>—New session is being rejected.</li> <li>• <b>lns-ic-wait-connect</b>—Session is waiting for the peer's incoming call connected (ICCN) message.</li> </ul>	All levels
<b>Bundle ID</b>	(LNS only) Bundle identifier. Indicates the session is part of a multilink bundle. Sessions that have a blank <b>Bundle</b> field are not participating in the Multilink Protocol. Sessions in a multilink bundle might belong to different L2TP tunnels. For L2TP output organized by bundle ID, issue the <b>show services l2tp multilink extensive</b> command.	All levels
<b>Mode</b>	(LNS) Mode of the interface representing the session: <b>shared</b> or <b>exclusive</b> . (LAC) Mode of the interface representing the session: <b>shared</b> or <b>dedicated</b> . Only <b>dedicated</b> is currently supported for the LAC.	extensive
<b>Local IP</b>	IP address of local endpoint of the Point-to-Point Protocol (PPP) session.	extensive
<b>Remote IP</b>	IP address of remote endpoint of the PPP session.	extensive
<b>Username</b>	(LNS only) Name of the user logged in to the session.	All levels
<b>Assigned IP address</b>	(LNS only) IP address assigned to remote client.	extensive
<b>Local name</b>	For LNS, name of the LNS instance in which the session was created. For LAC, name of the LAC.	extensive
<b>Remote name</b>	For LNS, name of the LAC from which the session was created. For LAC, name of the LAC instance.	extensive
<b>Local MRU</b>	(LNS only) Maximum receive unit (MRU) setting of the local device, in bytes.	extensive
<b>Remote MRU</b>	(LNS only) MRU setting of the remote device, in bytes.	extensive
<b>Tx speed</b>	Transmit speed of the session conveyed from the LAC to the LNS, in bits per second (bps).  Both the initial ( <b>initial</b> ) and current ( <b>update</b> ) line speeds can be displayed on MX Series routers.	extensive



Table 15: show services l2tp session Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Rx speed</b>	Receive speed of the session conveyed from the LAC to the LNS, in bits per second (bps).  Both the initial ( <b>initial</b> ) and current ( <b>update</b> ) line speeds can be displayed on MX Series routers.	<b>extensive</b>
<b>Bearer type</b>	Type of bearer enabled: <ul style="list-style-type: none"><li>• 0—Might indicate that the call was not received over a physical link (for example, when the LAC and PPP are located in the same subsystem).</li><li>• 1—Digital access requested.</li><li>• 2—Analog access requested.</li><li>• 4—Asynchronous Transfer Mode (ATM) bearer support.</li></ul>	<b>extensive</b>
<b>Framing type</b>	Type of framing enabled: <ul style="list-style-type: none"><li>• 1—Synchronous framing</li><li>• 2—Asynchronous framing</li></ul>	<b>extensive</b>
<b>LCP renegotiation</b>	(LNS only) Whether Link Control Protocol (LCP) renegotiation is configured: <b>On</b> or <b>Off</b> .	<b>extensive</b>
<b>Authentication</b>	Type of authentication algorithm used: Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).	<b>extensive</b>
<b>Interface ID</b>	(LNS only) Identifier used to look up the logical interface for this session.	<b>extensive</b>
<b>Interface unit</b>	Logical interface for this session.	All levels
<b>Call serial number</b>	Unique serial number assigned to the call.	<b>extensive</b>
<b>Policer bandwidth</b>	Maximum policer bandwidth configured for this session.	<b>extensive</b>
<b>Policer burst size</b>	Maximum policer burst size configured for this session.	<b>extensive</b>
<b>Firewall filter</b>	Configured firewall filter name.	<b>extensive</b>
<b>Session encapsulation overhead</b>	Overhead allowance configured for this session, in bytes.	<b>extensive</b>
<b>Session cell overhead</b>	Cell overhead activation ( <b>On</b> or <b>Off</b> ).	<b>extensive</b>
<b>Create time</b>	Date and time when the call was created.	<b>extensive</b>
<b>Up time</b>	Length of time elapsed since the call became active, in hours, minutes, and seconds.	<b>extensive</b>

Table 15: show services l2tp session Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Idle time</b>	Length of time elapsed since the call became idle, in hours, minutes, and seconds.	<b>extensive</b>
<b>Statistics since</b>	<p>Date and time when collection of the following statistics began:</p> <ul style="list-style-type: none"> <li><b>Control Tx</b>—Amount of control information transmitted, in packets and bytes.</li> <li><b>Control Rx</b>—Amount of control information received, in packets and bytes.</li> <li><b>Data Tx</b>—Amount of data transmitted, in packets and bytes.</li> <li><b>Data Rx</b>—Amount of data received, in packets and bytes.</li> <li><b>Errors Tx</b>—Number of errors transmitted, in packets.</li> <li><b>Errors Rx</b>—Number of errors received, in packets.</li> <li><b>LCP echo req Tx</b>—Number of LCP echo requests transmitted, in packets.</li> <li><b>LCP echo req Rx</b>—Number of LCP echo requests received, in packets.</li> <li><b>LCP echo rep Tx</b>—Number of LCP echo responses transmitted, in packets.</li> <li><b>LCP echo rep Rx</b>—Number of LCP echo responses received, in packets.</li> <li><b>LCP echo Req timeout</b>—Number of LCP echo requests that timed out.</li> <li><b>LCP echo Req error</b>—Number of errors received for LCP echo packets.</li> <li><b>LCP echo Rep error</b>—Number of errors transmitted for LCP echo packets.</li> </ul>	<b>extensive</b>

## Sample Output

### show services l2tp session (LNS on M Series Routers)

```

user@host> show services l2tp session
Interface: sp-1/2/0, Tunnel group: group1, Tunnel local ID: 8802
  Local Remote Interface State      Bundle Username
  ID    ID    unit
  37966    5        2 Established

```

### show services l2tp session (LNS on MX Series Routers)

```

user@host> show services l2tp session
Tunnel local ID: 40553
  Local Remote State      Interface      Interface
  ID    ID      State      unit          Name
  17967 1      Established 1073749824    si-5/2/0

```

### show services l2tp session (LAC)

```

user@host> show services l2tp session
Tunnel local ID: 31889
  Local Remote State      Interface      Interface
  ID    ID      State      unit          Name
  31694 1      Established 311           pp0

```

### show services l2tp session detail (LAC)

```

user@host> show services l2tp session detail
Tunnel local ID: 31889
  Session local ID: 31694, Session remote ID: 1, Interface unit: 311
  State: Established, Interface: pp0, Mode: Dedicated

```

Local IP: 10.1.1.2:1701, Remote IP: 10.1.1.1:1701  
 Local name: ce-lac, Remote name: ce-lns

#### show services l2tp session extensive (LAC)

```
user@host> show services l2tp session extensive
Tunnel local ID: 31889
Session local ID: 31694, Session remote ID: 1
Interface unit: 311
State: Established, Mode: Dedicated
Local IP: 10.10.1.2:1701, Remote IP: 10.10.1.1:1701
Local name: ce-lac, Remote name: ce-lns
Tx speed: 0, Rx speed: 0
Bearer type: 1, Framing type: 1
LCP renegotiation: N/A, Authentication: None, Interface ID: N/A
Interface unit: 311, Call serial number: 0
Policer bandwidth: 0, Policer burst size: 0
Policer exclude bandwidth: 0, Firewall filter: 0
Session encapsulation overhead: 0, Session cell overhead: 0
Create time: Tue Aug 24 14:38:23 2010, Up time: 01:06:25
Idle time: N/A
```

#### show services l2tp session extensive (LAC on MX Series Routers)

```
user@host> show services l2tp session extensive
Tunnel local ID: 31889
Session local ID: 31694, Session remote ID: 1
Interface unit: 311
State: Established, Mode: Dedicated
Local IP: 10.10.1.2:1701, Remote IP: 10.10.1.1:1701
Local name: ce-lac, Remote name: ce-lns
Tx speed: initial 64000, Update 256000
Rx speed: initial 64000, Update 256000
Bearer type: 1, Framing type: 1
LCP renegotiation: N/A, Authentication: None, Interface ID: N/A
Interface unit: 311, Call serial number: 0
Policer bandwidth: 0, Policer burst size: 0
Policer exclude bandwidth: 0, Firewall filter: 0
Session encapsulation overhead: 0, Session cell overhead: 0
Create time: Tue Aug 24 14:38:23 2010, Up time: 01:06:25
Idle time: N/A
```

#### show services l2tp session extensive (LNS on M Series Routers)

```
user@host> show services l2tp session extensive
Interface: sp-1/2/0, Tunnel group: group1, Tunnel local ID: 62746
Session local ID: 56793, Session remote ID: 53304
State: Established, Bundle ID: 5, Mode: shared
Local IP: 10.128.1.1:1701, Remote IP: 10.128.1.2:1701
Username: usr1@juniper_1.net, Assigned IP address: 10.50.2.1/32
Local MRU: 4000, Remote MRU: 1500, Tx speed: 64000, Rx speed: 64000
Bearer type: 2, Framing type: 1
LCP renegotiation: Off, Authentication: CHAP, Interface ID: unit_20
Interface unit: 20, Call serial number: 4137941434
Policer bandwidth: 64000, Policer burst size: 51200
Firewall filter: f1
Session encapsulation overhead: 16, Session cell overhead: 0n
Create time: Tue Mar 23 14:13:15 2004, Up time: 01:16:41
Idle time: 00:00:00
Statistics since: Tue Mar 23 14:13:13 2004
```

	Packets	Bytes
Control Tx	4	88

Control Rx	2	28
Data Tx	0	0
Data Rx	461	29.0k
Errors Tx	0	
Errors Rx	0	

Interface: sp-1/2/0, Tunnel group: group\_company\_dns, Tunnel local ID: 37266  
 Session local ID: 39962, Session remote ID: 53303  
 State: Established, Bundle ID: 5, Mode: shared  
 Local IP: 10.128.11.1:1701, Remote IP: 10.128.11.2:1701  
 Username: usr1@company.com, Assigned IP address: 10.46.2.3/24  
 Local name: router-1, Remote name: router-2  
 Local MRU: 4470, Remote MRU: 4470, Tx speed: 155000000, Rx speed: 155000000  
 Bearer type: 2, Framing type: 1  
 LCP renegotiation: Off, Authentication: CHAP, Interface ID: unit\_31  
 Interface unit: 31, Call serial number: 4137941433  
 Policer bandwidth: 64000, Policer burst size: 51200  
 Firewall filter: f1  
 Create time: Tue Mar 23 14:13:17 2004, Up time: 01:16:39  
 Idle time: 01:16:36  
 Statistics since: Tue Mar 23 14:13:15 2004

	Packets	Bytes
Control Tx	6	196
Control Rx	4	150
Data Tx	0	0
Data Rx	1	80
Errors Tx	0	
Errors Rx	0	

#### show services l2tp session extensive (LNS on MX Series Routers)

```
user@host> show services l2tp session extensive
Tunnel local ID: 40553
  Session local ID: 17967, Session remote ID: 1
    Interface unit: 1073749824
    State: Established
    Interface: si-5/2/0
    Mode: Dedicated
    Local IP: 11.1.1.2:1701, Remote IP: 11.1.1.3:1701
    Local name: lns-mx960, Remote name: testlac
    Tx speed: 56000, Rx speed: 0
    Bearer type: 2, Framing type: 1
    LCP renegotiation: Off, Authentication: None
    Call serial number: 1
    Create time: Mon Apr 25 20:27:50 2011, Up time: 00:01:48
    Idle time: N/A
    Statistics since: Mon Apr 25 20:27:50 2011
```

	Packets	Bytes
Control Tx	4	219
Control Rx	4	221
Data Tx	0	0
Data Rx	10	228
Errors Tx	0	
Errors Rx	0	

#### show services l2tp session statistics (MX Series Routers)

```
user@host> show services l2tp session statistics local session-id 1
Tunnel local ID: 17185
Session local ID: 1, Session remote ID: 14444, Interface unit: 1073788352
State: Established
```

```
Statistics since: Mon Aug 1 13:27:47 2011
Packets  Bytes
Data Tx   4    51
Data Rx   3    36
```

## show services l2tp tunnel-switch destination

<b>Syntax</b>	show services l2tp tunnel-switch destination < detail   extensive > <statistics>
<b>Release Information</b>	Command introduced in Junos OS Release 13.2.
<b>Description</b>	Display information about L2TP switched tunnel destinations.
<b>Options</b>	<p><b>none</b>—Display standard information for all L2TP switched tunnel destinations.</p> <p><b>detail   extensive</b>—(Optional) Display the specified level of information.</p> <p><b>statistics</b>—(Optional) Display the number of control packets and bytes transmitted and received for the destination. You cannot include this option with either of the level options, <b>detail</b> or <b>extensive</b>.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show services l2tp tunnel-switch session on page 232</a></li> <li>• <a href="#">show services l2tp tunnel-switch summary on page 242</a></li> <li>• <a href="#">show services l2tp tunnel-switch tunnel on page 237</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show services l2tp tunnel-switch destination on page 230</a> <a href="#">show services l2tp tunnel-switch destination detail on page 230</a> <a href="#">show services l2tp destination extensive on page 230</a> <a href="#">show services l2tp destination statistics on page 231</a>
<b>Output Fields</b>	Table 16 on page 228 lists the output fields for the <b>show services l2tp tunnel-switch destination</b> command. Output fields are listed in the approximate order in which they appear.

Table 16: show services l2tp tunnel-switch destination Output Fields

Field Name	Field Description	Level of Output
Local Name	Name of this destination.	All levels
Remote IP	IP address of the remote peer (LNS).	All levels

Table 16: show services l2tp tunnel-switch destination Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Tunnels</b>	<p>Number of tunnel connections for the destination in the following categories:</p> <p>Number of tunnel connections for the destination in the following categories:</p> <ul style="list-style-type: none"> <li>• total</li> <li>• active</li> <li>• failed</li> </ul>	<p>All levels for total</p> <p><b>extensive</b> for active and failed</p>
<b>Sessions</b>	<p>Number of session connections for the destination in the following categories:</p> <p>Number of session connections for the destination in the following categories:</p> <ul style="list-style-type: none"> <li>• total</li> <li>• active</li> <li>• failed</li> </ul>	<p>All levels for total</p> <p><b>extensive</b> for active and failed</p>
<b>Switched-sessions</b>	Number of L2TP sessions established by tunnel switching.	All levels
<b>State</b>	<p>Administrative state of the L2TP destination:</p> <p>Administrative state of the L2TP destination:</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b>—No restrictions exist on creation or operation of sessions and tunnels for this destination.</li> <li>• <b>Disabled</b>—Existing sessions and tunnels for this destination have been disabled and no new sessions or tunnels are created while in the <b>Disabled</b> state.</li> </ul>	All levels
<b>Local IP</b>	IP address of the local gateway (LAC).	<b>detail extensive</b>
<b>Transport</b>	Medium used for tunneling. Only <b>ipUdp</b> is supported.	<b>detail extensive</b>
<b>Logical System</b>	Logical system in which the tunnel is configured.	<b>detail extensive</b>
<b>Router Instance</b>	Routing instance in which the tunnel is configured.	<b>detail extensive</b>
<b>Lockout State</b>	<p>Reachability state of the destination:</p> <p>Reachability state of the destination:</p> <ul style="list-style-type: none"> <li>• <b>not locked</b>—Destination is considered reachable.</li> <li>• <b>waiting for lockout timeout</b>—Destination is locked out by L2TP because it is unreachable, so no attempts are made to reach the destination until the lockout timeout (300 seconds) expires, unless this is the only destination available for tunneling the subscriber.</li> </ul>	<b>detail extensive</b>
<b>Connections</b>	Number of total, active, and failed tunnel and session connections for the destination.	<b>extensive</b>

Table 16: show services l2tp tunnel-switch destination Output Fields (*continued*)

Field Name	Field Description	Level of Output
Control Tx	Amount of control information transmitted, in packets and bytes.	extensive statistics
Control Rx	Amount of control information received, in packets and bytes.	extensive statistics
Data Tx	Amount of data transmitted, in packets and bytes.	extensive statistics
Data Rx	Amount of data received, in packets and bytes.	extensive statistics
Error Tx	Number of errors transmitted, in packets.	extensive statistics
Error Rx	Number of errors received, in packets.	extensive statistics

## Sample Output

### show services l2tp tunnel-switch destination

```

user@host> show services l2tp tunnel-switch destination
  Local Name  Remote IP    Tunnels  Sessions  Switched-sessions  State
  1           192.168.20.3  1        1         1                  Enabled
  2           10.1.1.10    1        1         1                  Enabled

```

### show services l2tp tunnel-switch destination detail

```

user@host> show services l2tp destination detail
  Local name: 1
    Remote IP: 192.168.20.3
    Tunnels: 1, Sessions: 1, Switched sessions: 1
    State: Enabled
    Local IP: 10.50.1.1
    Transport: ipUdp, Logical System: default, Router Instance: default
    Lockout State: not locked
  Local name: 2
    Remote IP: 172.20.1.10
    Tunnels: 1, Sessions: 1, Switched sessions: 1
    State: Enabled
    Local IP: 10.30.1.1
    Transport: ipUdp, Logical System: default, Router Instance: default
    Lockout State: not locked

```

### show services l2tp destination extensive

```

user@host> show services l2tp destination extensive
Waiting for statistics...
  Local name: 1
    Remote IP: 192.168.20.3
    Tunnels: 1, Sessions: 1, Switched sessions: 1
    State: Enabled
    Local IP: 10.50.1.1
    Transport: ipUdp, Logical System: default, Router Instance: default
    Lockout State: not locked
    Connections  Totals      Active      Failed
    Tunnels      1           1           0
    Sessions     1           1           0
                  Packets      Bytes

```



```

Control Tx          6          239
Control Rx          6          267
Data Tx            67          815
Data Rx            0           0
Errors Tx           0
Errors Rx           0
Local name: 2
Remote IP: 172.20.1.10
Tunnels: 1, Sessions: 1, Switched sessions: 1
State: Enabled
Local IP: 10.30.1.1
Transport: ipUdp, Logical System: default, Router Instance: default
Lockout State: not locked
Connections      Totals      Active      Failed
Tunnels           1           1           0
Sessions          1           1           0
                Packets      Bytes
Control Tx         7          462
Control Rx         6          171
Data Tx            0           0
Data Rx           66          798
Errors Tx           0
Errors Rx           0

```

#### show services l2tp destination statistics

```

user@host> show services l2tp destination statistics
Waiting for statistics...
Local name: 2, Tunnels: 1, Sessions: 1
                Packets      Bytes
Control Tx         5          452
Control Rx         4          147
Data Tx            0           0
Data Rx            4           54
Errors Tx           0
Errors Rx           0
Local name: 1, Tunnels: 1, Sessions: 1
                Packets      Bytes
Control Tx         4          184
Control Rx         4          243
Data Tx            5           71
Data Rx            0           0
Errors Tx           0
Errors Rx           0

```

## show services l2tp tunnel-switch session

<b>Syntax</b>	show services l2tp tunnel-switch session <detail   extensive> <statistics>
<b>Release Information</b>	Command introduced in Junos OS Release 13.2.
<b>Description</b>	Display information about L2TP switched tunnel sessions.
<b>Options</b>	<p><b>none</b>—Display standard information about all active L2TP switched tunnel sessions.</p> <p><b>detail   extensive</b>—(Optional) Display the specified level of output.</p> <p><b>statistics</b>—(Optional) Display the number of control packets and bytes transmitted and received for the session. You cannot include this option with either of the level options, <b>detail</b> or <b>extensive</b>.</p>
<b>Additional Information</b>	
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show services l2tp tunnel-switch destination on page 228</a></li> <li>• <a href="#">show services l2tp tunnel-switch summary on page 242</a></li> <li>• <a href="#">show services l2tp tunnel-switch tunnel on page 237</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show services l2tp tunnel-switch session on page 234</a> <a href="#">show services l2tp tunnel-switch session detail on page 235</a> <a href="#">show services l2tp tunnel-switch session extensive on page 235</a>
<b>Output Fields</b>	Table 17 on page 232 lists the output fields for the <b>show services l2tp tunnel-switch session</b> command. Output fields are listed in the approximate order in which they appear.

Table 17: show services l2tp tunnel-switch session Output Fields

Field Name	Field Description	Level of Output
<b>Tunnel local ID</b>	Identifier of the local endpoint of the tunnel, as assigned by the L2TP network server (LNS).	All levels
<b>Local ID</b>	Identifier of the local endpoint of the L2TP session, as assigned by the LNS.	none
<b>Remote ID</b>	Identifier of the remote endpoint of the L2TP session, as assigned by the L2TP access concentrator (LAC).	none

Table 17: show services l2tp tunnel-switch session Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>State</b>	State of the L2TP session: <ul style="list-style-type: none"> <li>• <b>Established</b>—Session is operating. This is the only state supported for the LAC.</li> <li>• <b>closed</b>—Session is being closed.</li> <li>• <b>destroyed</b>—Session is being destroyed.</li> <li>• <b>clean-up</b>—Session is being cleaned up.</li> <li>• <b>lms-ic-accept-new</b>—New session is being accepted.</li> <li>• <b>lms-ic-idle</b>—Session has been created and is idle.</li> <li>• <b>lms-ic-reject-new</b>—New session is being rejected.</li> <li>• <b>lms-ic-wait-connect</b>—Session is waiting for the peer's incoming call connected (ICCN) message.</li> </ul>	All levels
<b>Interface unit</b>	Logical interface for this session.	All levels
<b>Interface Name</b>	(LNS only) Name of an adaptive services interface.	none
<b>Session local ID</b>	Identifier of the local endpoint of the L2TP session, as assigned by the LNS.	<b>detail extensive</b>
<b>Session remote ID</b>	Identifier of the remote endpoint of the L2TP session, as assigned by the L2TP access concentrator (LAC).	<b>detail extensive</b>
<b>Tunnel switch profile name</b>	Name of a tunnel switch profile.	<b>detail extensive</b>
<b>Mode</b>	(LNS) Mode of the interface representing the session: <b>shared</b> or <b>exclusive</b> .  (LAC) Mode of the interface representing the session: <b>shared</b> or <b>dedicated</b> . Only <b>dedicated</b> is currently supported for the LAC.	<b>detail extensive</b>
<b>Local IP</b>	IP address of local endpoint of the Point-to-Point Protocol (PPP) session.	<b>detail extensive</b>
<b>Remote IP</b>	IP address of remote endpoint of the PPP session.	<b>detail extensive</b>
<b>Local name</b>	For LNS, name of the LNS instance in which the session was created. For LAC, name of the LAC.	<b>detail extensive</b>
<b>Remote name</b>	For LNS, name of the LAC from which the session was created. For LAC, name of the LAC instance.	<b>detail extensive</b>
<b>Bearer type</b>	Type of bearer enabled: <ul style="list-style-type: none"> <li>• <b>0</b>—Might indicate that the call was not received over a physical link (for example, when the LAC and PPP are located in the same subsystem).</li> <li>• <b>1</b>—Digital access requested.</li> <li>• <b>2</b>—Analog access requested.</li> <li>• <b>4</b>—Asynchronous Transfer Mode (ATM) bearer support.</li> </ul>	<b>extensive</b>

Table 17: show services l2tp tunnel-switch session Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Framing type</b>	Type of framing enabled: <ul style="list-style-type: none"> <li>1—Synchronous framing</li> <li>2—Asynchronous framing</li> </ul>	<b>extensive</b>
<b>LCP renegotiation</b>	(LNS only) Whether Link Control Protocol (LCP) renegotiation is configured: <b>On</b> or <b>Off</b> .	<b>extensive</b>
<b>Authentication</b>	Type of authentication algorithm used: Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).	<b>extensive</b>
<b>Interface ID</b>	(LNS only) Identifier used to look up the logical interface for this session.	<b>extensive</b>
<b>Call serial number</b>	Unique serial number assigned to the call.	<b>extensive</b>
<b>Tx speed</b>	Transmit speed of the session conveyed from the LAC to the LNS, in bits per second (bps).	<b>extensive</b>
<b>Rx speed</b>	Receive speed of the session conveyed from the LAC to the LNS, in bits per second (bps).	<b>extensive</b>
<b>Create time</b>	Day, date, and time when the call was created.	<b>extensive</b>
<b>Up time</b>	Length of time elapsed since the call became active, in hours, minutes, and seconds.	<b>extensive</b>
<b>Idle time</b>	Length of time elapsed since the call became idle, in hours, minutes, and seconds.	<b>extensive</b>
<b>ToS Reflect</b>	Status of IP ToS value reflection, <b>Disabled</b> or <b>Enabled</b> .	<b>extensive</b>
<b>Statistics since</b>	Date and time when collection of the following statistics began: <ul style="list-style-type: none"> <li><b>Data Tx</b>—Amount of data transmitted, in packets and bytes.</li> <li><b>Data Rx</b>—Amount of data received, in packets and bytes.</li> </ul>	<b>extensive</b>

## Sample Output

### show services l2tp tunnel-switch session

```

user@host> show services l2tp tunnel-switch session
Tunnel local ID: 37602
  Local Remote State           Interface Interface
  ID    ID                    unit      Name
  13545 1      Established        1073741842 si-2/1/0

Tunnel local ID: 37060
  Local Remote State           Interface Interface
  ID    ID                    unit      Name
  58296 1      Established        1073741843 si-2/1/0

```

**show services l2tp tunnel-switch session detail**

```

user@host> show services l2tp tunnel-switch session detail
Tunnel local ID: 37602
  Session local ID: 13545, Session remote ID: 1, Interface unit: 1073741842
  State: Established, Interface: si-2/1/0
  Tunnel switch profile name: ce-lts-profile
  Mode: Dedicated
  Local IP: 10.50.1.1:1701, Remote IP: 192.168.20.3:1701
  Local name: ce-bras-mx240-f, Remote name: testlac

Tunnel local ID: 37060
  Session local ID: 58296, Session remote ID: 1, Interface unit: 1073741843
  State: Established, Interface: si-2/1/0
  Tunnel switch profile name: ce-lts-profile
  Mode: Dedicated
  Local IP: 10.30.1.1:1701, Remote IP: 172.20.1.10:1701
  Local name: lns, Remote name: lns

```

**show services l2tp tunnel-switch session extensive**

```

user@host> show services l2tp tunnel-switch session extensive
Tunnel local ID: 37602
  Session local ID: 13545, Session remote ID: 1
  Interface unit: 1073741842
  State: Established
  Interface: si-2/1/0
  Tunnel switch profile name: ce-lts-profile
  Mode: Dedicated
  Local IP: 10.50.1.1:1701, Remote IP: 192.168.20.3:1701
  Local name: ce-bras-mx240-f, Remote name: testlac
  Bearer type: 2, Framing type: 1
  LCP renegotiation: On, Authentication: None, Interface ID: si-2/1/0
  Call serial number: 0
  Tx speed: 56000, Rx speed: 0
  Create time: Fri Jan 18 03:01:11 2013, Up time: 00:06:50
  Idle time: N/A, ToS Reflect: Disabled
  Statistics since: Fri Jan 18 03:01:11 2013
    Packets      Bytes
  Data Tx       85     1031
  Data Rx        0        0

Tunnel local ID: 37060
  Session local ID: 58296, Session remote ID: 1
  Interface unit: 1073741843
  State: Established
  Interface: si-2/1/0
  Tunnel switch profile name: ce-lts-profile
  Mode: Dedicated
  Local IP: 10.30.1.1:1701, Remote IP: 172.20.1.10:1701
  Local name: lns, Remote name: lns
  Bearer type: 2, Framing type: 1
  LCP renegotiation: N/A, Authentication: None, Interface ID: N/A
  Call serial number: 0
  Tx speed: 56000, Rx speed: 0
  Create time: Fri Jan 18 03:01:14 2013, Up time: 00:06:48
  Idle time: N/A
  Statistics since: Fri Jan 18 03:01:14 2013
    Packets      Bytes
  Data Tx        0        0
  Data Rx       84     1014

```



## show services l2tp tunnel-switch tunnel

<b>Syntax</b>	show services l2tp tunnel-switch tunnel <detail   extensive> <statistics>
<b>Release Information</b>	Command introduced in Junos OS Release 13.2.
<b>Description</b>	Display information about L2TP switched tunnels.
<b>Options</b>	<p><b>none</b>—Display standard information about all active L2TP tunnels.</p> <p><b>detail   extensive</b>—(Default) Display the specified level of output.</p> <p><b>statistics</b>—(Optional) Display the number of control packets and bytes transmitted and received for the tunnel. You cannot include this option with either of the level options, <b>detail</b> or <b>extensive</b>.</p>
<b>Additional Information</b>	
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show services l2tp tunnel-switch destination on page 228</a></li> <li>• <a href="#">show services l2tp tunnel-switch session on page 232</a></li> <li>• <a href="#">show services l2tp tunnel-switch summary on page 242</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show services l2tp tunnel-switch tunnel on page 240</a> <a href="#">show services l2tp tunnel-switch tunnel detail on page 240</a> <a href="#">show services l2tp tunnel-switch tunnel extensive on page 240</a>
<b>Output Fields</b>	Table 18 on page 237 lists the output fields for the <b>show services l2tp tunnel-switch tunnel</b> command. Output fields are listed in the approximate order in which they appear.

Table 18: show services l2tp tunnel-switch tunnel Output Fields

Field Name	Field Description	Level of Output
<b>Local ID</b>	<p>On the LNS, number assigned by the LNS that identifies the local endpoint of the tunnel relative to the LNS: the LNS.</p> <p>On the LAC, number assigned by the LAC that identifies the local endpoint of the tunnel relative to the LAC: the LAC.</p>	none
<b>Remote ID</b>	<p>On the LNS, number assigned by the LAC that identifies the remote endpoint of the tunnel relative to the LNS: the LAC.</p> <p>On the LAC, number assigned by the LNS that identifies the remote endpoint of the tunnel relative to the LAC: the LNS.</p>	none
<b>Remote IP</b>	IP address of the peer endpoint of the tunnel.	All levels

Table 18: show services l2tp tunnel-switch tunnel Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Sessions</b>	Number of L2TP sessions established through the tunnel.	All levels
<b>Switched-sessions</b>	Number of L2TP sessions established by tunnel switching.	All levels
<b>State</b>	<p>State of the L2TP tunnel:</p> <ul style="list-style-type: none"> <li><b>cc_responder_accept_new</b>—The tunnel has received and accepted the start control connection request (SCCRQ).</li> <li><b>cc_responder_reject_new</b>—The tunnel has received and rejected the SCCRP.</li> <li><b>cc_responder_idle</b>—The tunnel has just been created.</li> <li><b>cc_responder_wait_ctl_conn</b>—The tunnel has sent the start control connection response (SCCRP) and is waiting for the start control connection connected (SCCCN) message.</li> <li><b>clean-up</b>—The tunnel is being cleaned up.</li> <li><b>closed</b>—The tunnel is being closed.</li> <li><b>destroyed</b>—The tunnel is being destroyed.</li> <li><b>Established</b>—The tunnel is operating. This is the only state supported for the LAC.</li> <li><b>Terminate</b>—The tunnel is terminating.</li> <li><b>Unknown</b>—The tunnel is not connected to the router.</li> </ul>	All levels
<b>Tunnel local ID</b>	<p>On the LNS, number assigned by the LNS that identifies the local endpoint of the tunnel relative to the LNS: the LNS.</p> <p>On the LAC, number assigned by the LAC that identifies the local endpoint of the tunnel relative to the LAC: the LAC.</p>	<b>detail extensive</b>
<b>Tunnel remote ID</b>	<p>On the LNS, number assigned by the LAC that identifies the remote endpoint of the tunnel relative to the LNS: the LAC.</p> <p>On the LAC, number assigned by the LNS that identifies the remote endpoint of the tunnel relative to the LAC: the LNS.</p>	<b>detail extensive</b>
<b>Tunnel Name</b>	(LAC only) Name of the created tunnel. This value includes the destination name followed by the value of the RADIUS Tunnel-Assignment-ID VSA [82].	<b>detail extensive</b>
<b>Local IP</b>	IP address of the local endpoint of the tunnel.	<b>detail extensive</b>
<b>Local name</b>	Name used for local tunnel endpoint during tunnel negotiation.	<b>detail extensive</b>
<b>Remote name</b>	Name used for remote tunnel endpoint during tunnel negotiation.	<b>detail extensive</b>
<b>Effective Peer Resync Mechanism</b>	<p>(LAC only) Peer resynchronization mechanism (PRM) in effect for the tunnel:</p> <p>(LAC only) Peer resynchronization mechanism (PRM) in effect for the tunnel:</p> <ul style="list-style-type: none"> <li>Failover protocol</li> <li>Silent failover—Recovery takes place in the failed endpoint only using the proprietary silent failover protocol.</li> </ul>	<b>detail extensive</b>



Table 18: show services l2tp tunnel-switch tunnel Output Fields (*continued*)

Field Name	Field Description	Level of Output
NAS Port Method	(LAC only) Status of interoperation with Cisco LNS devices: (LAC only) Status of interoperation with Cisco LNS devices: <ul style="list-style-type: none"> <li>• none—NAS port method is not enabled for interoperation.</li> <li>• cisco-avp—NAS port method is enabled for interoperation.</li> </ul>	detail extensive
Tunnel Logical System	Logical system in which the L2TP tunnel is brought up.	detail extensive
Tunnel Routing Instance	Routing instance in which the L2TP tunnel is brought up.	detail extensive
Max sessions	Maximum number of sessions that can be established on this tunnel.	extensive
Window size	Number of control messages that can be sent without receipt of an acknowledgment.	extensive
Hello interval	Interval between the transmission of hello messages, in seconds.	extensive
Create time	Date and time when the tunnel was created. While the LNS and LAC are connected, this value should correspond to the router's uptime. If connection to the LAC is severed, the State changes to <b>Unknown</b> and the <b>Create time</b> value resets.	extensive
Up time	Amount of time elapsed since the tunnel became active, in hours, minutes, and seconds.	extensive
Idle time	Amount of time elapsed since the tunnel became idle, in hours, minutes, and seconds.	extensive
ToS Reflect	Status of IP ToS value reflection, <b>Disabled</b> or <b>Enabled</b> .	extensive
Interface Name	(LNS only) Name of an adaptive services interface.	extensive
Tunnel Group Name	(LNS only) Name of a tunnel group.	extensive
Statistics since	Date and time when collection of the following statistics began: <ul style="list-style-type: none"> <li>• <b>Control Tx</b>—Amount of control information transmitted, in packets and bytes.</li> <li>• <b>Control Rx</b>—Amount of control information received, in packets and bytes.</li> <li>• <b>Data Tx</b>—Amount of data transmitted, in packets and bytes.</li> <li>• <b>Data Rx</b>—Amount of data received, in packets and bytes.</li> <li>• <b>Errors Tx</b>—Number of errors transmitted, in packets.</li> <li>• <b>Errors Rx</b>—Number of errors received, in packets.</li> </ul>	extensive

## Sample Output

### show services l2tp tunnel-switch tunnel

```
user@host> show services l2tp tunnel-switch tunnel
Local ID Remote ID Remote IP Sessions Switched-sessions State
37602 1 192.168.20.3:1701 1 1 Established
37060 1 172.20.1.10:1701 1 1 Established
```

### show services l2tp tunnel-switch tunnel detail

```
user@host> show services l2tp tunnel-switch tunnel detail
Tunnel local ID: 37602, Tunnel remote ID: 1
Remote IP: 192.168.20.3:1701
Sessions: 1, Switched sessions: 1, State: Established
Tunnel Name: 1/1
Local IP: 10.50.1.1:1701
Local name: ce-bras-mx240-f, Remote name: testlac
Effective Peer Resync Mechanism: silent failover
Nas Port Method: none
Tunnel Logical System: default, Tunnel Routing Instance: default
Tunnel local ID: 37060, Tunnel remote ID: 1
Remote IP: 172.20.1.10:1701
Sessions: 1, Switched sessions: 1, State: Established
Tunnel Name: 2/1
Local IP: 10.30.1.1:1701
Local name: lns, Remote name: lns
Effective Peer Resync Mechanism: silent failover
Nas Port Method: none
Tunnel Logical System: default, Tunnel Routing Instance: default
```

### show services l2tp tunnel-switch tunnel extensive

```
user@host> show services l2tp tunnel-switch tunnel extensive
Waiting for statistics...
Tunnel local ID: 37602, Tunnel remote ID: 1
Remote IP: 192.168.20.3:1701
Sessions: 1, Switched sessions: 1, State: Established
Tunnel Name: 1/1
Local IP: 10.50.1.1:1701
Local name: ce-bras-mx240-f, Remote name: testlac
Effective Peer Resync Mechanism: silent failover
Nas Port Method: none
Tunnel Logical System: default, Tunnel Routing Instance: default
Max sessions: 128100, Window size: 4, Hello interval: 60
Create time: Fri Jan 18 03:01:11 2013, Up time: 00:07:49
Idle time: 00:00:00, ToS Reflect: Disabled
Interface Name: si-2/1/0, Tunnel Group Name: ce-l2tp-tunnel-group
Statistics since: Fri Jan 18 03:01:11 2013
          Packets      Bytes
Control Tx          7      259
Control Rx          7      279
Data Tx           97     1175
Data Rx            0         0
Errors Tx            0
Errors Rx            0
Tunnel local ID: 37060, Tunnel remote ID: 1
Remote IP: 172.20.1.10:1701
Sessions: 1, Switched sessions: 1, State: Established
```

Tunnel Name: 2/1  
Local IP: 10.30.1.1:1701  
Local name: lns, Remote name: lns  
Effective Peer Resync Mechanism: silent failover  
Nas Port Method: none  
Tunnel Logical System: default, Tunnel Routing Instance: default  
Max sessions: 128100, Window size: 4, Hello interval: 60  
Create time: Fri Jan 18 03:01:14 2013, Up time: 00:07:46  
Idle time: 00:00:00  
Statistics since: Fri Jan 18 03:01:14 2013

	Packets	Bytes
Control Tx	8	482
Control Rx	7	183
Data Tx	0	0
Data Rx	96	1158
Errors Tx	0	
Errors Rx	0	

## show services l2tp tunnel-switch summary

<b>Syntax</b>	show services l2tp tunnel-switch summary <statistics>
<b>Release Information</b>	Command introduced in Junos OS Release 13.2.
<b>Description</b>	Display L2TP tunnel switch summary information.
<b>Options</b>	<p><b>none</b>—Display complete L2TP switched tunnel summary information.</p> <p><b>statistics</b>—(Optional) Display the number of control packets and bytes transmitted and received for all switched tunnels and sessions.</p>
<b>Additional Information</b>	
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show services l2tp tunnel-switch destination on page 228</a></li> <li>• <a href="#">show services l2tp tunnel-switch session on page 232</a></li> <li>• <a href="#">show services l2tp tunnel-switch tunnel on page 237</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show services l2tp tunnel-switch summary on page 243</a>
<b>Output Fields</b>	Table 19 on page 242 lists the output fields for the <b>show services l2tp tunnel-switch summary</b> command. Output fields are listed in the approximate order in which they appear.

**Table 19: show services l2tp tunnel-switch summary Output Fields**

Field Name	Field Description
<b>Tunnel switch profile name</b>	Name of a tunnel switch profile.
<b>LNS local session id</b>	Identifier assigned by the LNS function on the LTS to the local endpoint of the L2TP session originating on a remote LAC (the first session)
<b>LAC local session id</b>	Identifier assigned by the LAC function on the LTS to the local endpoint of the L2TP session originating on the LTS (the second session).
<b>LNS state</b>	State of the L2TP session (the first session) between a remote LAC and the LNS function on the LTS.
<b>LAC state</b>	State of the L2TP session (the second session) between the LAC function on the LTS and a remote LNS.

## Sample Output

### show services l2tp tunnel-switch summary

```
user@host> show services l2tp tunnel-switch summary
Tunnel switch profile name: ce-lts-profile
  LNS local  LAC local  LNS state    LAC state    Interface
  session ID session ID
  13545      58296      established  established  si-2/1/0
```

## show services l2tp summary

<b>Syntax</b>	show services l2tp summary <statistics> <interface sp-fpc/pic/port>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Support for LAC on MX Series routers introduced in Junos OS Release 10.4. Support for LNS on MX Series routers introduced in Junos OS Release 11.4. Support for <b>statistics</b> option introduced in Junos OS Release 13.1
<b>Description</b>	(M10i and M7i routers: LNS only. MX Series routers: LAC and LNS.) Display Layer 2 Tunneling Protocol (L2TP) summary information.
<b>Options</b>	<p><b>none</b>—Display complete L2TP summary information. For LNS on M Series routers, display L2TP summary information for all adaptive services interfaces. For LNS on MX Series routers, display L2TP summary information for all inline services interfaces.</p> <p><b>interface sp-fpc/pic/port</b>—(Optional) Display L2TP summary information for only the specified adaptive services interface. This option is not available for L2TP on MX Series routers.</p> <p><b>statistics</b>—(Optional) Display a summary of control packets and bytes transmitted and received.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">L2TP Services Configuration Overview</a></li> <li><a href="#">L2TP Minimum Configuration</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show services l2tp summary (LAC on M Series routers) on page 247</a> <a href="#">show services l2tp summary (LAC on MX Series routers) on page 247</a> <a href="#">show services l2tp summary (LNS on MX Series routers) on page 247</a> <a href="#">show services l2tp summary (LNS on M Series routers) on page 248</a> <a href="#">show services l2tp summary statistics (MX Series routers) on page 248</a>
<b>Output Fields</b>	Table 20 on page 244 lists the output fields for the <b>show services l2tp summary</b> command. Output fields are listed in the approximate order in which they appear.

**Table 20: show services l2tp summary Output Fields**

Field Name	Field Description
<b>Failover within a preference level</b>	State of this tunnel selection method on the LAC. When enabled, tunnel selection fails over within a preference level. When disabled, tunnel selection drops to the next lower preference level. Not displayed for LNS on M Series routers.

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

Field Name	Field Description
<b>Weighted load balancing</b>	State of this tunnel selection method on the LAC. When enabled, the maximum session limit of a tunnel determines its weight within a preference level. Tunnel selection proceeds from greatest to least weight. When disabled, selection defaults to a round robin method. Not displayed for LNS on M Series routers.
<b>Tunnel authentication challenge</b>	State of tunnel authentication, indicating whether the LAC and LNS exchange an authentication challenge and response during the establishment of the tunnel. The state is <b>Enabled</b> when a secret is configured in the tunnel profile or on the RADIUS server in the Tunnel-Password attribute [69]. The state is <b>Disabled</b> when the secret is not present. Not displayed for LNS on M Series routers.
<b>Calling number avp</b>	When the state is <b>Enabled</b> , the LAC includes the value of the Calling Number AVP 22 in ICRQ packets sent to the LNS. When the state is <b>Disabled</b> , the attribute is not sent to the LNS. Not displayed for LNS on M Series routers.
<b>Failover Protocol</b>	When the state is enabled, the LAC operates in the default <i>failover-protocol-fall-back-to-silent-failover</i> manner. When the state is disabled, the <b>disable-failover-protocol</b> statement has been issued and the LAC operates only in silent failover mode. Not displayed for LNS on M Series routers.
<b>Tx connect speed method</b>	The connection speed method configured to send the speed values in the L2TP Tx Connect Speed (AVP 24) and L2TP Rx Connect Speed (AVP 38). Possible values are: <ul style="list-style-type: none"> <li>• <b>ancp</b></li> <li>• <b>pppoe-ia-tag</b></li> <li>• <b>static</b></li> </ul>
<b>Rx speed avp when equal</b>	Indicates if the Rx connect speed when equal configuration is <b>enabled</b> or <b>disabled</b> .
<b>Tunnel assignment id</b>	Format of the tunnel name.  Format of the tunnel name, based on RADIUS attributes returned from the AAA server:  Format of the tunnel name, based on RADIUS attributes returned from the AAA server: <ul style="list-style-type: none"> <li>• <b>authentication-id</b>—Name consists of only Tunnel Assignment-Id [82]. This is the default value.</li> <li>• <b>client-server-id</b>—Name is a combination of Tunnel-Client-Auth-Id [90], Tunnel-Server-Endpoint [67], and Tunnel-Assignment-Id [82]. This format is available only on MX Series routers.</li> </ul>

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

Field Name	Field Description
<b>Tunnel Tx Address Change</b>	<p>Action taken by LAC when it receives a request from a peer to change the destination IP address, UDP port, or both:</p> <p>Action taken by LAC when it receives a request from a peer to change the destination IP address, UDP port, or both:</p> <ul style="list-style-type: none"> <li>• <b>accept</b>—Accepts change requests for the IP address or UDP port. This is the default action.</li> <li>• <b>ignore</b>—Ignores all change requests.</li> <li>• <b>ignore-ip-address</b>—Ignores change requests for the IP address but accepts them for the UDP port.</li> <li>• <b>ignore-udp-port</b>—Ignores change requests for the UDP port but accepts them for the IP address.</li> </ul>
<b>Min Retransmission Timeout for control packets</b>	Minimum number of seconds that the local peer waits for the initial response after transmitting an L2TP control packet. If no response has been received by the time the period expires, the local peer retransmits the packet.
<b>Max Retransmissions for Established Tunnel</b>	Maximum number of times control messages are retransmitted for established tunnels.
<b>Max Retransmissions for Not Established Tunnel</b>	Maximum number of times control messages are retransmitted for tunnels that are not established.
<b>Tunnel Idle Timeout</b>	Period that a tunnel can be inactive—that is, carrying no traffic—before it times out and is torn down.
<b>Destruct Timeout</b>	Period that the router attempts to maintain dynamic destinations, tunnels, and sessions after they have been destroyed.
<b>Destination Lockout Timeout</b>	Timeout period for which all future destinations are locked out, meaning that they are not considered for selection when a new tunnel is created.
<b>Reassembly Service Set</b>	Indicates active IP reassembly configured for the interface.
<b>Destinations</b>	Number of L2TP destinations for the LAC. Not displayed for LNS on M Series routers.
<b>Tunnels</b>	Number of L2TP tunnels established on the router.
<b>Sessions</b>	Number of L2TP sessions established on the router.
<b>Switched sessions</b>	Number of L2TP tunnel-switched sessions established on the router.
<b>Control</b>	Count of L2TP control packets and bytes sent and received.
<b>Data</b>	Count of L2TP data packets and bytes sent and received.



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

Field Name	Field Description
Errors	Count of L2TP error packets and bytes sent and received.

## Sample Output

### show services l2tp summary (LAC on M Series routers)

```

user@host> show services l2tp summary
Failover within a preference level is Disabled
Weighted load balancing is Enabled
Tunnel authentication challenge is Enabled
Calling number avp is Enabled
Failover Protocol is Disabled
Tunnel assignment id format is authentication-id
Destinations: 1 Tunnels: 1, Sessions: 1
  Tx packets    Rx packets  Memory (bytes)
Control      260          144          11513856
Data         7.5k         16.9k         8.3k
Errors              0              0

```

### show services l2tp summary (LAC on MX Series routers)

```

user@host> show services l2tp summary
Failover within a preference level is Disabled
  Weighted load balancing is Disabled
  Tunnel authentication challenge is Enabled
  Calling number avp is Enabled
  Failover Protocol is Disabled
  Tx Connect speed method is static
  Rx speed avp when equal is enabled
  Tunnel Tx Address Change is Accept
  Min Retransmissions Timeout for control packets is 2 seconds
  Max Retransmissions for Established Tunnel is 7
  Max Retransmissions for Not Established Tunnel is 5
  Tunnel Idle Timeout is 60 seconds
  Destruct Timeout is 300 seconds
  Destination Lockout Timeout is 300 seconds
Reassembly Service Set is ssnr3
Destinations: 0, Tunnels: 0, Sessions: 0, Switched sessions: 0

```

### show services l2tp summary (LNS on MX Series routers)

```

user@host show services l2tp summary
  Failover within a preference level is Disabled
  Weighted load balancing is Disabled
  Tunnel authentication challenge is Enabled
  Calling number avp is Enabled
  Failover Protocol is Enabled
  Tx Connect speed method is static

reassembly Service Set is ssnr3 Destinations: 4, Tunnels: 19, Sessions: 65,
Switched sessions: 2

```

**show services l2tp summary (LNS on M Series routers)**

```
user@host> show services l2tp summary
Tunnels: 2, Sessions: 2, Errors: 0
  Tx packets  Rx packets  Memory (bytes)
Control      6k          9k          688k
Data        70k         70k         3054
```

**show services l2tp summary statistics (MX Series routers)**

```
user@host>show services l2tp summary statistics
Failover within a preference level is Disabled
Weighted load balancing is Disabled
Tunnel authentication challenge is Enabled
Calling number avp is Enabled
Failover Protocol is Enabled
Tx Connect speed method is advisory
Tunnel assignment id format is assignment-id
Tunnel Tx Address Change is Accept
Min Retransmissions Timeout for control packets is 4 seconds
Max Retransmissions for Established Tunnel is 7
Max Retransmissions for Not Established Tunnel is 5
Tunnel Idle Timeout is 60 seconds
Destruct Timeout is 300 seconds
Destination Lockout Timeout is 300 secondsDestinations: 1, Tunnels: 1, Sessions:
31815, Switched sessions: 0
  Tx packets  Rx packets  Memory (bytes)
Control      90.4k       32.0k       245678080
Data        127.3k      100.8kk      0
Errors           0           0
```

## show services l2tp tunnel

<b>Syntax</b>	<pre>show services l2tp tunnel &lt;brief   detail   extensive&gt; &lt;interface sp-fpc/pic/port&gt; &lt;local-gateway gateway-address&gt; &lt;local-gateway-name gateway-name&gt; &lt;local-tunnel-id tunnel-id&gt; &lt;peer-gateway gateway-address&gt; &lt;peer-gateway-name gateway-name&gt; &lt;statistics&gt; &lt;tunnel-group group-name&gt;</pre>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	<p>(M10i and M7i routers only) Display information about active Layer 2 Tunneling Protocol (L2TP) tunnels for LNS.</p> <p>(MX Series routers only) Display information about L2TP tunnels for LAC and LNS.</p>
<b>Options</b>	<p><b>none</b>—Display standard information about all active L2TP tunnels.</p> <p><b>brief   detail   extensive</b>—(Default) Display the specified level of output.</p> <p><b>interface sp-fpc/pic/port</b>—(Optional) Display L2TP tunnel information for only the specified adaptive services interface. This option is not available for L2TP on MX Series routers.</p> <p><b>local-gateway gateway-address</b>—(Optional) Display L2TP tunnel information for only the specified local gateway address.</p> <p><b>local-gateway-name gateway-name</b>—(Optional) Display L2TP tunnel information for only the specified local gateway name.</p> <p><b>local-tunnel-id tunnel-id</b>—(Optional) Display L2TP tunnel information for only the specified local tunnel identifier.</p> <p><b>peer-gateway gateway-address</b>—(Optional) Display L2TP tunnel information for only the specified peer gateway address.</p> <p><b>peer-gateway-name gateway-name</b>—(Optional) Display L2TP tunnel information for only the specified peer gateway name.</p> <p><b>statistics</b>—(Optional) Display the number of control packets and bytes transmitted and received for the tunnel. You cannot include this option with any of the level options, <b>brief</b>, <b>detail</b>, or <b>extensive</b>.</p> <p><b>tunnel-group group-name</b>—(Optional) Display L2TP tunnel information for only the specified tunnel group.</p>
<b>Required Privilege Level</b>	view

- Related Documentation**
- [L2TP Services Configuration Overview](#)
  - [L2TP Minimum Configuration](#)

**List of Sample Output**

- [show services l2tp tunnel \(LAC\) on page 252](#)
- [show services l2tp tunnel detail \(LAC\) on page 252](#)
- [show services l2tp tunnel detail \(LAC on MX Series Routers\) on page 252](#)
- [show services l2tp tunnel detail \(LNS on MX Series Routers\) on page 252](#)
- [show services l2tp tunnel extensive \(LAC\) on page 253](#)
- [show services l2tp tunnel extensive \(LNS on M Series Routers\) on page 253](#)
- [show services l2tp tunnel extensive \(LNS on MX Series Routers\) on page 254](#)
- [show services l2tp tunnel statistics \(MX Series Routers\) on page 254](#)

**Output Fields** [Table 21 on page 250](#) lists the output fields for the **show services l2tp tunnel** command. Output fields are listed in the approximate order in which they appear.

**Table 21: show services l2tp tunnel Output Fields**

Field Name	Field Description
<b>Interface</b>	(LNS only) Name of an adaptive services interface.
<b>Tunnel group</b>	(LNS only) Name of a tunnel group.
<b>Local ID</b>	<p>On the LNS, number assigned by the LNS that identifies the local endpoint of the tunnel relative to the LNS: the LNS.</p> <p>On the LAC, number assigned by the LAC that identifies the local endpoint of the tunnel relative to the LAC: the LAC.</p>
<b>Remote ID</b>	<p>On the LNS, number assigned by the LAC that identifies the remote endpoint of the tunnel relative to the LNS: the LAC.</p> <p>On the LAC, number assigned by the LNS that identifies the remote endpoint of the tunnel relative to the LAC: the LNS.</p>
<b>Remote IP</b>	IP address of the peer endpoint of the tunnel.
<b>Sessions</b>	Number of L2TP sessions established through the tunnel.

Table 21: show services l2tp tunnel Output Fields (*continued*)

Field Name	Field Description
<b>State</b>	<p>State of the L2TP tunnel:</p> <ul style="list-style-type: none"> <li>• <b>cc_responder_accept_new</b>—The tunnel has received and accepted the start control connection request (SCCRQ).</li> <li>• <b>cc_responder_reject_new</b>—The tunnel has received and rejected the SCCRQ.</li> <li>• <b>cc_responder_idle</b>—The tunnel has just been created.</li> <li>• <b>cc_responder_wait_ctl_conn</b>—The tunnel has sent the start control connection response (SCCRP) and is waiting for the start control connection connected (SCCCN) message.</li> <li>• <b>clean-up</b>—The tunnel is being cleaned up.</li> <li>• <b>closed</b>—The tunnel is being closed.</li> <li>• <b>destroyed</b>—The tunnel is being destroyed.</li> <li>• <b>Established</b>—The tunnel is operating. This is the only state supported for the LAC.</li> <li>• <b>Terminate</b>—The tunnel is terminating.</li> <li>• <b>Unknown</b>—The tunnel is not connected to the router.</li> </ul>
<b>Tunnel Name</b>	(LAC only) Name of the created tunnel. This value includes the destination name followed by the value of the RADIUS Tunnel-Assignment-ID VSA [82].
<b>Local IP</b>	IP address of the local endpoint of the tunnel.
<b>Local name</b>	Name used for local tunnel endpoint during tunnel negotiation.
<b>Remote name</b>	Name used for remote tunnel endpoint during tunnel negotiation.
<b>Effective Peer Resync Mechanism</b>	<p>(LAC only) Peer resynchronization mechanism (PRM) in effect for the tunnel:</p> <p>(LAC only) Peer resynchronization mechanism (PRM) in effect for the tunnel:</p> <ul style="list-style-type: none"> <li>• Failover protocol</li> <li>• Silent failover—Recovery takes place in the failed endpoint only using the proprietary silent failover protocol.</li> </ul>
<b>Nas Port Method</b>	<p>NAS port method (type), which indicates whether the LAC sends Cisco NAS Port Info AVP (100) in ICRQs to the LNS:</p> <p>NAS port method (type), which indicates whether the LAC sends Cisco NAS Port Info AVP (100) in ICRQs to the LNS:</p> <ul style="list-style-type: none"> <li>• <b>cisco-avp</b>—sends the AVP.</li> <li>• <b>none</b>—does not send the AVP.</li> </ul>
<b>Tunnel Logical System</b>	Logical system in which the L2TP tunnel is brought up.
<b>Tunnel Routing Instance</b>	Routing instance in which the L2TP tunnel is brought up.
<b>Max sessions</b>	Maximum number of sessions that can be established on this tunnel.
<b>Window size</b>	Number of control messages that can be sent without receipt of an acknowledgment.

Table 21: show services l2tp tunnel Output Fields (*continued*)

Field Name	Field Description
<b>Hello interval</b>	Interval between the transmission of hello messages, in seconds.
<b>Create time</b>	Date and time when the tunnel was created. While the LNS and LAC are connected, this value should correspond to the router's uptime. If connection to the LAC is severed, the State changes to <b>Unknown</b> and the <b>Create time</b> value resets.
<b>Up time</b>	Amount of time elapsed since the tunnel became active, in hours, minutes, and seconds.
<b>Idle time</b>	Amount of time elapsed since the tunnel became idle, in hours, minutes, and seconds.
<b>Statistics since</b>	<p>Date and time when collection of the following statistics began:</p> <ul style="list-style-type: none"> <li>• <b>Control Tx</b>—Amount of control information transmitted, in packets and bytes.</li> <li>• <b>Control Rx</b>—Amount of control information received, in packets and bytes.</li> <li>• <b>Data Tx</b>—Amount of data transmitted, in packets and bytes.</li> <li>• <b>Data Rx</b>—Amount of data received, in packets and bytes.</li> <li>• <b>Errors Tx</b>—Number of errors transmitted, in packets.</li> <li>• <b>Errors Rx</b>—Number of errors received, in packets.</li> </ul>

## Sample Output

### show services l2tp tunnel (LAC)

```
user@host> show services l2tp tunnel
Local ID  Remote ID  Remote IP          Sessions  State
17185      1    10.10.1.1:1701      1    Established
```

### show services l2tp tunnel detail (LAC)

```
user@host> show services l2tp tunnel detail
Tunnel local ID: 31889, Tunnel remote ID: 1
Remote IP: 100.1.1.1:1701
Sessions: 1, State: Established
Tunnel Name: 1/tunnel-to-LNS-1
Local IP: 100.1.1.2:1701
Local name: ce-lac, Remote name: ce-lns
Effective Peer Resync Mechanism: silent failover
```

### show services l2tp tunnel detail (LAC on MX Series Routers)

```
user@host> show services l2tp tunnel detail
Tunnel local ID: 17301, Tunnel remote ID: 1
Remote IP: 10.10.1.1:1701
Sessions: 1, State: Established
Tunnel Name: 2/tunnel-to-LNS-2
Local IP: 100.1.1.2:1701
Local name: ce-lac, Remote name: ce-lns
Effective Peer Resync Mechanism: silent failover
Tunnel Logical System: default, Tunnel Routing Instance: default
```

### show services l2tp tunnel detail (LNS on MX Series Routers)

```
user@host> show services l2tp tunnel detail
```

```
Tunnel local ID: 17301, Tunnel remote ID: 1
Remote IP: 12.1.1.15:1701
Sessions: 1, State: Established
Tunnel Name: 2/2
Local IP: 12.1.1.5:1701
Local name: ce-bras-mx240-e, Remote name: testlac2
Effective Peer Resync Mechanism: silent failover
Tunnel Logical System: default, Tunnel Routing Instance: vrf1
```

#### show services l2tp tunnel extensive (LAC)

```
user@host> show services l2tp tunnel extensive
Tunnel local ID: 17185, Tunnel remote ID: 1
Remote IP: 10.10.1.1:1701
Sessions: 1, State: Established
Tunnel Name: 2/tunnel-to-LNS-2
Local IP: 100.1.1.2:1701
Local name: ce-lac, Remote name: ce-lns
Effective Peer Resync Mechanism: failover protocol
Max sessions: 32000, Window size: 4, Hello interval: 60
Create time: Tue Nov 9 15:23:29 2010, Up time: 00:00:26
Idle time: 00:00:00
```

#### show services l2tp tunnel extensive (LNS on M Series Routers)

```
user@host> show services l2tp tunnel extensive
Interface: sp-1/2/0, Tunnel group: group1
Tunnel local ID: 62746, Tunnel remote ID: 16930
Remote IP: 10.128.1.2:1701
Sessions: 1, State: Established
Local IP: 10.128.1.1:1701
Local name: router-1, Remote name: router-2
Max sessions: 50, Window size: 32, Hello interval: 60
Create time: Tue Mar 23 14:13:15 2004, Up time: 01:14:58
Idle time: 00:00:07
Statistics since: Tue Mar 23 14:13:13 2004
```

	Packets	Bytes
Control Tx	80	1152
Control Rx	3	272
Data Tx	0	0
Data Rx	450	28.0k
Errors Tx	0	
Errors Rx	0	

```
Interface: sp-1/2/0, Tunnel group: group_company_dns
Tunnel local ID: 37266, Tunnel remote ID: 36217
Remote IP: 10.128.11.2:1701
Sessions: 1, State: Established
Local IP: 10.128.11.1:1701
Local name: router-1, Remote name: router-2
Max sessions: unlimited, Window size: 32, Hello interval: 60
Create time: Tue Mar 23 14:13:15 2004, Up time: 01:14:59
Idle time: 01:14:55
Statistics since: Tue Mar 23 14:13:13 2004
```

	Packets	Bytes
Control Tx	81	1164
Control Rx	3	273
Data Tx	0	0
Data Rx	1	80
Errors Tx	0	
Errors Rx	0	

**show services l2tp tunnel extensive (LNS on MX Series Routers)**

```
user@host> show services l2tp tunnel extensive
Tunnel local ID: 40553, Tunnel remote ID: 1
Remote IP: 192.168.1.3:1701
Sessions: 1, State: Established
Tunnel Name: 3/1838
Local IP: 10.1.1.2:1701
Local name: lns-mx960, Remote name: testlac
Effective Peer Resync Mechanism: silent failover
Nas Port Method: none
Tunnel Logical System: default, Tunnel Routing Instance: vrf1
Max sessions: 60000, Window size: 4, Hello interval: 60
Create time: Mon Apr 25 20:27:50 2011, Up time: 00:01:11
Idle time: 00:00:00, ToS Reflect: Enabled
Tunnel Group Name: tg1
Statistics since: Mon Apr 25 20:27:50 2011
```

	Packets	Bytes
Control Tx	4	219
Control Rx	4	221
Data Tx	0	0
Data Rx	6	64
Errors Tx	0	
Errors Rx		

**show services l2tp tunnel statistics (MX Series Routers)**

```
user@host> show services l2tp tunnel statistics
Tunnel local ID: 17185, Tunnel remote ID: 1
Sessions: 31.8k, State: Established
Statistics since: Mon Aug 1 13:21:38 2011
```

	Packets	Bytes
Control Tx	90.3k	9.0M
Control Rx	32.0k	1296.9k
Data Tx	127.3k	1591.6k
Data Rx	100.8k	1273.4k
Errors Tx	0	
Errors Rx	0	



## show subscribers

**Syntax** show subscribers  
 <detail | extensive | terse>  
 <aci-interface-set-name *aci-interface-set-name*>  
 <address *address*>  
 <agent-circuit-identifier *agent-circuit-identifier-substring*>  
 <client-type *client-type*>  
 <count>  
 <id>  
 <interface *interface*>  
 <logical-system *logical-system*>  
 <mac-address *mac-address*>  
 <physical-interface *physical-interface-name*>  
 <profile-name *profile-name*>  
 <routing-instance *routing-instance*>  
 <stacked-vlan-id *stacked-vlan-id*>  
 <subscriber-state *subscriber-state*>  
 <user-name *user-name*>  
 <vci *vci-identifier*>  
 <vpi *vpi-identifier*>  
 <vlan-id *vlan-id*>

**Release Information** Command introduced in Junos OS Release 9.3.  
 Command introduced in Junos OS Release 9.3 for EX Series switches.  
**client-type**, **mac-address**, **subscriber-state**, and **extensive** options introduced in Junos OS Release 10.2.  
**count** option usage with other options introduced in Junos OS Release 10.2.  
 Command introduced in Junos OS Release 11.1 for the QFX Series.  
 Options **aci-interface-set-name** and **agent-circuit-identifier** introduced in Junos OS Release 12.2.  
 The **physical-interface** and **user-name** options introduced in Junos OS Release 12.3.  
 Options **vci** and **vpi** introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases.  
 Options **vci** and **vpi** supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

**Description** Display information for active subscribers.

**Options** **detail | extensive | terse**—(Optional) Display the specified level of output.

**aci-interface-set-name**—(Optional) Display all dynamic subscriber sessions that use the specified agent circuit identifier (ACI) interface set. Use the ACI interface set name generated by the router, such as aci-1003-ge-1/0/0.4001, and not the actual ACI value found in the DHCP or PPPoE control packets.

**address**—(Optional) Display subscribers whose IP address matches the specified address. You must specify the IPv4 or IPv6 address prefix without a netmask (for example, 192.168.17.1). If you specify the IP address as a prefix with a netmask (for example, 192.168.17.1/32), the router displays a message that the IP address is invalid, and rejects the command.

***agent-circuit-identifier-substring***—(Optional) Display all dynamic subscriber sessions whose ACI value matches the specified substring.

***client-type***—(Optional) Display subscribers whose client type matches the specified client type (DHCP, L2TP, PPP, PPPOE, VLAN, or static).

***count***—(Optional) Display the count of total subscribers and active subscribers for any specified option. You can use the ***count*** option alone or with the ***address***, ***client-type***, ***interface***, ***logical-system***, ***mac-address***, ***profile-name***, ***routing-instance***, ***stacked-vlan-id***, ***subscriber-state***, or ***vlan-id*** options.

***id***—(Optional) Display a specific subscriber session whose session id matches the specified subscriber ID. You can display subscriber IDs by using the ***show subscribers extensive*** or the ***show subscribers interface extensive*** commands.

***interface***—(Optional) Display subscribers whose interface matches the specified interface.

***logical-system***—(Optional) Display subscribers whose logical system matches the specified logical system.

***mac-address***—(Optional) Display subscribers whose MAC address matches the specified MAC address.

***physical-interface-name***—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose physical interface matches the specified physical interface.

***profile-name***—(Optional) Display subscribers whose dynamic profile matches the specified profile name.

***routing-instance***—(Optional) Display subscribers whose routing instance matches the specified routing instance.

***stacked-vlan-id***—(Optional) Display subscribers whose stacked VLAN ID matches the specified stacked VLAN ID.

***subscriber-state***—(Optional) Display subscribers whose subscriber state matches the specified subscriber state (ACTIVE, CONFIGURED, INIT, TERMINATED, or TERMINATING).

***user-name***—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose username matches the specified subscriber name.

***vci-identifier***—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual circuit identifier (VCI) matches the specified VCI identifier. The range of values is **0** through **255**.

***vpi-identifier***—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual path identifier (VPI) matches the specified VPI identifier. The range of values is **0** through **65535**.

***vlan-id***—(Optional) Display subscribers whose VLAN ID matches the specified VLAN ID.



**NOTE:** Due to display limitations, logical system and routing instance output values are truncated when necessary.

**Required Privilege Level**

view

**Related Documentation**

- [show subscribers summary on page 273](#)
- *Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration*

**List of Sample Output**

[show subscribers \(IPv4\) on page 261](#)  
[show subscribers \(IPv6\) on page 261](#)  
[show subscribers \(IPv4 and IPv6 Dual Stack\) on page 261](#)  
[show subscribers \(LNS on MX Series Routers\) on page 262](#)  
[show subscribers \(L2TP Switched Tunnels\) on page 262](#)  
[show subscribers client-type dhcp detail on page 262](#)  
[show subscribers count on page 262](#)  
[show subscribers address detail \(IPv6\) on page 262](#)  
[show subscribers detail \(IPv4\) on page 263](#)  
[show subscribers detail \(IPv6\) on page 263](#)  
[show subscribers detail \(IPv6 Static Demux Interface\) on page 264](#)  
[show subscribers detail \(L2TP LNS Subscribers on MX Series Routers\) on page 264](#)  
[show subscribers detail \(L2TP Switched Tunnels\) on page 264](#)  
[show subscribers detail \(Tunneled Subscriber\) on page 265](#)  
[show subscribers detail \(IPv4 and IPv6 Dual Stack\) on page 265](#)  
[show subscribers detail \(ACI Interface Set Session\) on page 266](#)  
[show subscribers detail \(PPPoE Subscriber Session with ACI Interface Set\) on page 266](#)  
[show subscribers extensive on page 266](#)  
[show subscribers extensive \(RPF Check Fail Filter\) on page 267](#)  
[show subscribers extensive \(L2TP LNS Subscribers on MX Series Routers\) on page 267](#)  
[show subscribers extensive \(IPv4 and IPv6 Dual Stack\) on page 267](#)  
[show subscribers extensive \(Effective Shaping-Rate\) on page 268](#)  
[show subscribers aci-interface-set-name detail \(Subscriber Sessions Using Specified ACI Interface Set\) on page 269](#)  
[show subscribers agent-circuit-identifier detail \(Subscriber Sessions Using Specified ACI Substring\) on page 269](#)  
[show subscribers interface extensive on page 270](#)  
[show subscribers logical-system terse on page 270](#)  
[show subscribers physical-interface count on page 271](#)  
[show subscribers routing-instance inst1 count on page 271](#)  
[show subscribers stacked-vlan-id detail on page 271](#)  
[show subscribers stacked-vlan-id vlan-id detail \(Combined Output\) on page 271](#)  
[show subscribers stacked-vlan-id vlan-id interface detail \(Combined Output for a Specific Interface\) on page 271](#)  
[show subscribers user-name detail on page 271](#)  
[show subscribers vlan-id on page 272](#)

[show subscribers vlan-id detail on page 272](#)

[show subscribers vpi vci extensive \(PPPoE-over-ATM Subscriber Session\) on page 272](#)

**Output Fields** Table 22 on page 258 lists the output fields for the **show subscribers** command. Output fields are listed in the approximate order in which they appear.

**Table 22: show subscribers Output Fields**

Field Name	Field Description
<b>Interface</b>	Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface.  The * character indicates a continuation of addresses for the same session.
<b>IP Address/VLAN ID</b>	Subscriber IP address or VLAN ID associated with the subscriber in the form <i>tpid.vlan-id</i>  No IP address or VLAN ID is assigned to an L2TP tunnel-switched session. For these subscriber sessions the value is <b>Tunnel-switched</b> .
<b>User Name</b>	Name of subscriber.
<b>LS:RI</b>	Logical system and routing instance associated with the subscriber.
<b>Type</b>	Subscriber client type (DHCP, L2TP, PPP, PPPoE, STATIC-INTERFACE, VLAN).
<b>IP Address</b>	Subscriber IPv4 address.
<b>IP Netmask</b>	Subscriber IP netmask.
<b>Primary DNS Address</b>	IP address of primary DNS server.
<b>Secondary DNS Address</b>	IP address of secondary DNS server.
<b>Primary WINS Address</b>	IP address of primary WINS server.
<b>Secondary WINS Address</b>	IP address of secondary WINS server.
<b>IPv6 Address</b>	Subscriber IPv6 address, or multiple addresses.
<b>IPv6 Prefix</b>	Subscriber IPv6 prefix. If you are using DHCPv6 prefix delegation, this is the delegated prefix.
<b>IPv6 User Prefix</b>	IPv6 prefix obtained through ND/RA.
<b>IPv6 Address Pool</b>	Subscriber IPv6 address pool. The IPv6 address pool is used to allocate IPv6 prefixes to the DHCPv6 clients.
<b>IPv6 Network Prefix Length</b>	Length of the network portion of the IPv6 address.
<b>IPv6 Prefix Length</b>	Length of the subscriber IPv6 prefix.

Table 22: show subscribers Output Fields (*continued*)

Field Name	Field Description
<b>Logical System</b>	Logical system associated with the subscriber.
<b>Routing Instance</b>	Routing instance associated with the subscriber.
<b>Interface Type</b>	Whether the subscriber interface is <b>Static</b> or <b>Dynamic</b> .
<b>Interface Set</b>	Internally generated name of the dynamic ACI interface set used by the subscriber session.
<b>Interface Set Type</b>	Interface type of the ACI interface set: <b>Dynamic</b> . This is the only ACI interface set type currently supported.
<b>Interface Set Session ID</b>	Identifier of the dynamic ACI interface set entry in the session database.
<b>Underlying Interface</b>	Name of the underlying interface for the subscriber session.
<b>Dynamic Profile Name</b>	Dynamic profile used for the subscriber.
<b>Dynamic Profile Version</b>	Version number of the dynamic profile used for the subscriber.
<b>MAC Address</b>	MAC address associated with the subscriber.
<b>State</b>	Current state of the subscriber session ( <b>Init</b> , <b>Configured</b> , <b>Active</b> , <b>Terminating</b> , <b>Tunneled</b> ).
<b>L2TP State</b>	Current state of the L2TP session, <b>Tunneled</b> or <b>Tunnel-switched</b> . When the value is <b>Tunnel-switched</b> , two entries are displayed for the subscriber; the first entry is at the LNS interface on the LTS and the second entry is at the LAC interface on the LTS.
<b>Tunnel switch Profile Name</b>	Name of the L2TP tunnel switch profile that initiates tunnel switching.
<b>Local IP Address</b>	IP address of the local gateway (LAC).
<b>Remote IP Address</b>	IP address of the remote peer (LNS).
<b>VLAN Id</b>	VLAN ID associated with the subscriber in the form <i>tpid.vlan-id</i> .
<b>Stacked VLAN Id</b>	Stacked VLAN ID associated with the subscriber in the form <i>tpid.vlan-id</i> .
<b>RADIUS Accounting ID</b>	RADIUS accounting ID associated with the subscriber.
<b>Agent Circuit ID</b>	Option 82 agent circuit ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.
<b>Agent Remote ID</b>	Option 82 agent remote ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.
<b>DHCP Relay IP Address</b>	IP address used by the DHCP relay agent.

Table 22: show subscribers Output Fields (*continued*)

Field Name	Field Description
<b>ATM VPI</b>	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual path identifier (VPI) on the subscriber's physical interface.
<b>ATM VCI</b>	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual circuit identifier (VCI) for each VPI configured on the subscriber interface.
<b>Login Time</b>	Date and time at which the subscriber logged in.
<b>Effective shaping-rate</b>	Actual downstream traffic shaping rate for the subscriber, in kilobits per second.
<b>IPv4 rpf-check Fail Filter Name</b>	Name of the filter applied by the dynamic profile to IPv4 packets that fail the RPF check.
<b>IPv6 rpf-check Fail Filter Name</b>	Name of the filter applied by the dynamic profile to IPv6 packets that fail the RPF check.
<b>DHCP Options</b>	len = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCP options, as defined in RFC 2132.
<b>Session ID</b>	ID number for a subscriber service session.
<b>Underlying Session ID</b>	For DHCPv6 subscribers on a PPPoE network, displays the session ID of the underlying PPPoE interface.
<b>Service Sessions</b>	Number of service sessions (that is, a service activated using RADIUS CoA) associated with the subscribers.
<b>Service Session Name</b>	Service session profile name.
<b>Session Timeout (seconds)</b>	Number of seconds of access provided to the subscriber before the session is automatically terminated.
<b>Idle Timeout (seconds)</b>	Number of seconds subscriber can be idle before the session is automatically terminated.
<b>IPv6 Delegated Address Pool</b>	Name of the pool used for DHCPv6 prefix delegation.
<b>IPv6 Delegated Network Prefix Length</b>	Length of the prefix configured for the IPv6 delegated address pool.
<b>IPv6 Interface Address</b>	Address assigned by the Framed-Ipv6-Prefix AAA attribute.
<b>IPv6 Framed Interface Id</b>	Interface ID assigned by the Framed-Interface-Id AAA attribute.
<b>ADF IPv4 Input Filter Name</b>	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.

Table 22: show subscribers Output Fields (*continued*)

Field Name	Field Description
<b>ADF IPv4 Output Filter Name</b>	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
<b>ADF IPv6 Input Filter Name</b>	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
<b>ADF IPv6 Output Filter Name</b>	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
<b>IPv4 Input Filter Name</b>	Name assigned to the IPv4 input filter (client or service session).
<b>IPv4 Output Filter Name</b>	Name assigned to the IPv4 output filter (client or service session).
<b>IPv6 Input Filter Name</b>	Name assigned to the IPv6 input filter (client or service session).
<b>IPv6 Output Filter Name</b>	Name assigned to the IPv6 output filter (client or service session).
<b>IFL Input Filter Name</b>	Name assigned to the logical interface input filter (client or service session).
<b>IFL Output Filter Name</b>	Name assigned to the logical interface output filter (client or service session).

## Sample Output

### show subscribers (IPv4)

```

user@host> show subscribers
Interface          IP Address/VLAN ID  User Name          LS:RI
ge-1/3/0.1073741824 100                 WHOLESALE-CLIENT  default:default
demux0.1073741824   100.0.0.10         RETAILER1-CLIENT  test1:retailer1
demux0.1073741825   101.0.0.3          RETAILER2-CLIENT  test1:retailer2
demux0.1073741826   102.0.0.3

```

### show subscribers (IPv6)

```

user@host> show subscribers
Interface          IP Address/VLAN ID  User Name          LS:RI
ge-1/0/0.0         2001::c0:0:0:0/74  WHOLESALE-CLIENT  default:default
*                  2002::1/128        subscriber-25      default:default

```

### show subscribers (IPv4 and IPv6 Dual Stack)

```

user@host> show subscribers
Interface          IP Address/VLAN ID  User Name
LS:RI
demux0.1073741834  0x8100.1002 0x8100.1
default:default
demux0.1073741835  0x8100.1001 0x8100.1
default:default
pp0.1073741836     61.1.1.1        dualstackuser1@ISP1.com

```

```
default:ASP-1
*                2041:1:1::/48
*                2061:1:1:1::/64
pp0.1073741837   23.1.1.3                dualstackuser2@ISP1.com
default:ASP-1
*                2001:1:2:5::/64
```

#### show subscribers (LNS on MX Series Routers)

```
user@host> show subscribers
Interface      IP Address/VLAN ID  User Name      LS:RI
si-4/0/0.1     192.168.4.1        xyz@example.com default:default
```

#### show subscribers (L2TP Switched Tunnels)

```
user@host> show subscribers
Interface      IP Address/VLAN ID  User Name      LS:RI
si-2/1/0.1073741842 Tunnel-switched    ap@lts.com     default:default
si-2/1/0.1073741843 Tunnel-switched    ap@lts.com     default:default
```

#### show subscribers client-type dhcp detail

```
user@host> show subscribers client-type dhcp detail
Type: DHCP
IP Address: 100.20.9.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Login Time: 2009-08-25 14:43:52 PDT

Type: DHCP
IP Address: 100.20.10.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744383
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:94:00:01:f3
State: Active
Radius Accounting ID: jnpr :2560
Login Time: 2009-08-25 14:43:56 PDT
```

#### show subscribers count

```
user@host> show subscribers count
Total Subscribers: 188, Active Subscribers: 188
```

#### show subscribers address detail (IPv6)

```
user@host> show subscribers address 100.16.12.137 detail
```



```

Type: PPPoE
User Name: pppoeTerV6User1Svc
IP Address: 100.16.12.137
IP Netmask: 255.0.0.0
IPv6 User Prefix: 1016:0:0:c88::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073745151
Interface type: Dynamic
Underlying Interface: demux0.8201
Dynamic Profile Name: pppoe-client-profile
MAC Address: 00:0d:02:01:00:01
Session Timeout (seconds): 31622400
Idle Timeout (seconds): 86400
State: Active
Radius Accounting ID: jnpr demux0.8201:6544
Session ID: 6544
Agent Circuit ID: if13720
Agent Remote ID: if13720
Login Time: 2012-05-21 13:37:27 PDT
Service Sessions: 1

```

#### show subscribers detail (IPv4)

```

user@host> show subscribers detail
Type: DHCP
IP Address: 100.20.9.7
IP Netmask: 255.255.0.0
Primary DNS Address: 192.168.17.1
Secondary DNS Address: 192.168.17.2
Primary WINS Address: 192.168.22.1
Secondary WINS Address: 192.168.22.2
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Idle Timeout (seconds): 600
Login Time: 2009-08-25 14:43:52 PDT
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
33 2d 37 2d 30 37 05 01 06 0f 21 2c
Service Sessions: 2

```

#### show subscribers detail (IPv6)

```

user@host> show subscribers detail
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2002:db2:ffff:1::/64
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:51:ff:ff:00:03
State: Active
Radius Accounting ID: 1

```

```
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00
00 00
```

#### show subscribers detail (IPv6 Static Demux Interface)

```
user@host> show subscribers detail
Type: STATIC-INTERFACE
User Name: demux0.1@jnpr.net
IPv6 Prefix: 1:2:3:4:5:6:7:aa/128
Logical System: default
Routing Instance: default
Interface: demux0.1
Interface type: Static
Dynamic Profile Name: junos-default-profile
State: Active
Radius Accounting ID: 185
Login Time: 2010-05-18 14:33:56 EDT
```

#### show subscribers detail (L2TP LNS Subscribers on MX Series Routers)

```
user@host> show subscribers detail
Type: L2TP
User Name: user1@jnpr.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
```

#### show subscribers detail (L2TP Switched Tunnels)

```
user@host> show subscribers detail
Type: L2TP
User Name: ap@example.com
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741842
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 10.50.1.1
Remote IP Address: 192.168.20.3
Radius Accounting ID: 21
Session ID: 21
Login Time: 2013-01-18 03:01:11 PST

Type: L2TP
User Name: ap@example.com
Logical System: default
```

```

Routing Instance: default
Interface: si-2/1/0.1073741843
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 10.30.1.1
Remote IP Address: 172.20.1.10
Session ID: 22
Login Time: 2013-01-18 03:01:14 PST

```

#### show subscribers detail (Tunneled Subscriber)

```

user@host> show subscribers detail
Type: PPPoE
User Name: user1@example.com
Logical System: default
Routing Instance: default
Interface: pp0.1
State: Active, Tunneled
Radius Accounting ID: 512

```

#### show subscribers detail (IPv4 and IPv6 Dual Stack)

```

user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@ISP1.com
IP Address: 61.1.1.1
IPv6 Prefix: 2041:1:1::/48
IPv6 User Prefix: 2061:1:1:1::/64
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST

Type: DHCP
IPv6 Prefix: 2041:1:1::/48
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:64:03:01:02

```

```
State: Active
Radius Accounting ID: jnpr :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

#### show subscribers detail (ACI Interface Set Session)

```
user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0
Interface Set: aci-1001-ge-1/0/0.2800
Interface Set Session ID: 0
Underlying Interface: ge-1/0/0.2800
Dynamic Profile Name: aci-vlan-set-profile-2
Dynamic Profile Version: 1
State: Active
Session ID: 1
Agent Circuit ID: aci-ppp-dhcp-20
Login Time: 2012-05-26 01:54:08 PDT
```

#### show subscribers detail (PPPoE Subscriber Session with ACI Interface Set)

```
user@host> show subscribers detail
Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.5
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Interface Set: aci-1001-demux0.1073741824
Interface Set Type: Dynamic
Interface Set Session ID: 2
Underlying Interface: demux0.1073741824
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:64:39:01:02
State: Active
Radius Accounting ID: 3
Session ID: 3
Agent Circuit ID: aci-ppp-dhcp-dvlan-50
Login Time: 2012-03-07 13:46:53 PST
```

#### show subscribers extensive

```
user@host> show subscribers extensive
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2002:db2:ffff:1::/64
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:51:ff:ff:00:03
```

```

State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00
00 00
IPv6 Address Pool: pd_pool
IPv6 Network Prefix Length: 48

```

#### show subscribers extensive (RPF Check Fail Filter)

```

user@host> show subscribers extensive
...
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ae0.1073741824
Interface type: Dynamic
Dynamic Profile Name: vlan-prof
State: Active
Session ID: 9
VLAN Id: 100
Login Time: 2011-08-26 08:17:00 PDT
IPv4 rpf-check Fail Filter Name: rpf-allow-dhcp
IPv6 rpf-check Fail Filter Name: rpf-allow-dhcpv6
...

```

#### show subscribers extensive (L2TP LNS Subscribers on MX Series Routers)

```

user@host> show subscribers extensive
Type: L2TP
User Name: user1@jnpr.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
IPv4 Input Filter Name: classify-si-5/2/0.1073749824-in
IPv4 Output Filter Name: classify-si-5/2/0.1073749824-out

```

#### show subscribers extensive (IPv4 and IPv6 Dual Stack)

```

user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1

```

```
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@ISP1.com
IP Address: 61.1.1.1
IPv6 Prefix: 2041:1:1::/48
IPv6 User Prefix: 2061:1:1:1::/64
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST
IPv6 Delegated Network Prefix Length: 48
IPv6 Interface Address: 2061:1:1:1::1/64
IPv6 Framed Interface Id: 1:1:2:2
IPv4 Input Filter Name: FILTER-IN-pp0.1073741825-in
IPv4 Output Filter Name: FILTER-OUT-pp0.1073741825-out
IPv6 Input Filter Name: FILTER-IN6-pp0.1073741825-in
IPv6 Output Filter Name: FILTER-OUT6-pp0.1073741825-out

Type: DHCP
IPv6 Prefix: 2041:1:1::/48
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: jnpr :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00
00 00
IPv6 Delegated Network Prefix Length: 48
```

#### show subscribers extensive (Effective Shaping-Rate)

```
user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741837
Interface type: Dynamic
Interface Set: ifset-1
Underlying Interface: ae1
Dynamic Profile Name: svlan-dhcp-test
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.201
VLAN Id: 0x8100.201
Login Time: 2011-11-30 00:18:04 PST
```

Effective shaping-rate: 31000000k

...

#### show subscribers aci-interface-set-name detail (Subscriber Sessions Using Specified ACI Interface Set)

```
user@host> show subscribers aci-interface-set-name aci-1003-ge-1/0/0.4001 detail
```

```
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT
```

```
Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:65:26:01:02
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT
```

#### show subscribers agent-circuit-identifier detail (Subscriber Sessions Using Specified ACI Substring)

```
user@host> show subscribers agent-circuit-identifier aci-ppp-vlan detail
```

```
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT
```

```
Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
```

**Interface Set Type: Dynamic**  
**Interface Set Session ID: 13**  
Underlying Interface: ge-1/0/0.4001  
Dynamic Profile Name: aci-vlan-pppoe-profile  
Dynamic Profile Version: 1  
MAC Address: 00:00:65:26:01:02  
State: Active  
Radius Accounting ID: 14  
Session ID: 14  
**Agent Circuit ID: aci-ppp-vlan-10**  
Login Time: 2012-03-12 10:41:57 PDT

#### show subscribers interface extensive

```
user@host> show subscribers interface demux0.1073741826 extensive
Type: VLAN
User Name: test1@test.com
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Dynamic
Dynamic Profile Name: profile-vdemux-relay-23qos
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 12
Session ID: 12
Stacked VLAN Id: 0x8100.1500
VLAN Id: 0x8100.2902
Login Time: 2011-10-20 16:21:59 EST

Type: DHCP
User Name: test1@test.com
IP Address: 172.16.200.6
IP Netmask: 255.255.255.0
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Static
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 21
Session ID: 21
Login Time: 2011-10-20 16:24:33 EST
Service Sessions: 2

Service Session ID: 25
Service Session Name: SUB-QOS
State: Active

Service Session ID: 26
Service Session Name: service-cb-content
State: Active
IPv4 Input Filter Name: content-cb-in-demux0.1073741826-in
IPv4 Output Filter Name: content-cb-out-demux0.1073741826-out
```

#### show subscribers logical-system terse

```
user@host> show subscribers logical-system test1 terse
Interface      IP Address/VLAN ID  User Name      LS:RI
demux0.1073741825  101.0.0.3          RETAILER1-CLIENT test1:retailer1
demux0.1073741826  102.0.0.3          RETAILER2-CLIENT test1:retailer2
```



### show subscribers physical-interface count

```
user@host> show subscribers physical-interface ge-1/0/0 count
Total subscribers: 3998, Active Subscribers: 3998
```

### show subscribers routing-instance inst1 count

```
user@host> show subscribers routing-instance inst1 count
Total Subscribers: 188, Active Subscribers: 183
```

### show subscribers stacked-vlan-id detail

```
user@host> show subscribers stacked-vlan-id 101 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

### show subscribers stacked-vlan-id vlan-id detail (Combined Output)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

### show subscribers stacked-vlan-id vlan-id interface detail (Combined Output for a Specific Interface)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 interface ge-1/2/0.* detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

### show subscribers user-name detail

```
user@host> show subscribers user-name larry1 detail
Type: DHCP
User Name: larry1
IP Address: 100.0.0.37
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.1
Interface type: Static
Dynamic Profile Name: foo
MAC Address: 00:10:94:00:00:01
State: Active
Radius Accounting ID: 1
Session ID: 1
```

```
Login Time: 2011-11-07 08:25:59 PST
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 01 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 32 2f
37 2d 30 2d 30 37 05 01 06 0f 21 2c
```

#### show subscribers vlan-id

```
user@host> show subscribers vlan-id 100
Interface          IP Address          User Name
ge-1/0/0.1073741824
ge-1/2/0.1073741825
```

#### show subscribers vlan-id detail


```
user@host> show subscribers vlan-id 100 detail
Type: VLAN
Interface: ge-1/0/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT

Type: VLAN
Interface: ge-1/2/0.1073741825
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT
```

#### show subscribers vpi vci extensive (PPPoE-over-ATM Subscriber Session)

```
user@host> show subscribers vpi 40 vci 50 extensive
Type: PPPoE
User Name: testuser
IP Address: 100.0.0.2
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: pp0.0
Interface type: Static
MAC Address: 00:00:65:23:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
ATM VPI: 40
ATM VCI: 50
Login Time: 2012-12-03 07:49:26 PST
IP Address Pool: pool_1
IPv6 Framed Interface Id: 200:65ff:fe23:102
```

## show subscribers summary

<b>Syntax</b>	<pre>show subscribers summary &lt;all&gt; &lt; detail   extensive   terse&gt; &lt;count&gt; &lt;physical-interface <i>physical-interface-name</i>&gt; &lt;logical-system <i>logical-system</i> pic   port   routing-instance <i>routing-instance</i>   slot&gt;</pre>
<b>Release Information</b>	Command introduced in Junos OS Release 10.2.
<b>Description</b>	Display summary information for subscribers.
<b>Options</b>	<p><b>all</b>—(Optional) Display full subscriber summary.</p> <p><b>detail   extensive   terse</b>—(Optional) Display the specified level of output.</p> <p><b>count</b>—(Optional) Display the count of total subscribers and active subscribers for any specified option.</p> <p><b>logical-system</b>—(Optional) Display subscribers whose logical system matches the specified logical system.</p> <p><b>physical-interface-name</b>—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers whose physical interface matches the specified physical interface, by subscriber state, client type and LS:RI.</p> <p><b>pic</b>—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by PIC number and the total number of subscribers.</p> <p><b>port</b>—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by port number and the total number of subscribers.</p> <p><b>routing-instance</b>—(Optional) Display subscribers whose routing instance matches the specified routing instance.</p> <p><b>slot</b>—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by FPC slot number and the total number of subscribers.</p>
	<div>  <p><b>NOTE:</b> Due to display limitations, logical system and routing instance output values are truncated when necessary.</p> </div>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show subscribers on page 255</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show subscribers summary on page 275</a>

[show subscribers summary all on page 275](#)  
[show subscribers summary physical-interface on page 276](#)  
[show subscribers summary physical-interface pic on page 276](#)  
[show subscribers summary physical-interface port on page 276](#)  
[show subscribers summary physical-interface slot on page 276](#)  
[show subscribers summary pic on page 277](#)  
[show subscribers summary pic \(Aggregated Ethernet Interfaces\) on page 277](#)  
[show subscribers summary port on page 277](#)  
[show subscribers summary slot on page 277](#)  
[show subscribers summary terse on page 277](#)

**Output Fields** Table 23 on page 274 lists the output fields for the **show subscribers** command. Output fields are listed in the approximate order in which they appear.

**Table 23: show subscribers Output Fields**

Field Name	Field Description
<b>Subscribers by State</b>	<p>Number of subscribers summarized by state. The summary information includes the following:</p> <p>Number of subscribers summarized by state. The summary information includes the following:</p> <ul style="list-style-type: none"> <li>• Init—Number of subscriber currently in the initialization state.</li> <li>• Configured—Number of configured subscribers.</li> <li>• Active—Number of active subscribers.</li> <li>• Terminating—Number of subscribers currently terminating.</li> <li>• Terminated—Number of terminated subscribers.</li> <li>• Total—Total number of subscribers for all states.</li> </ul>
<b>Subscribers by Client Type</b>	Number of subscribers summarized by client type. Client types can include DHCP, L2TP, PPP, PPPOE, STATIC-INTERFACE, and VLAN. Also displays the total number of subscribers for all client types (Total).
<b>Subscribers by LS:RI</b>	Number of subscribers summarized by logical system:routing instance (LS:RI) combination. Also displays the total number of subscribers for all LS:RI combinations (Total).
<b>Interface</b>	<p>Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface.</p> <p>The * character indicates a continuation of addresses for the same session.</p> <p>For aggregated Ethernet interfaces, the output of the <b>summary (pic   port   slot)</b> options prefixes the interface name with <b>ae0:</b>.</p>
<b>Count</b>	Count of subscribers displayed for each PIC, port, or slot when those options are specified with the <b>summary</b> option. For an aggregated Ethernet configuration, the total subscriber count does not equal the sum of the individual PIC, port, or slot counts, because each subscriber can be in more than one aggregated Ethernet link.
<b>Total Subscribers</b>	Total number of subscribers for all physical interfaces, all PICS, all ports, or all LS:RI slots.
<b>IP Address/VLAN ID</b>	Subscriber IP address or VLAN ID associated with the subscriber in the form <i>tpid.vlan-id</i>
<b>User Name</b>	Name of subscriber.

Table 23: show subscribers Output Fields (*continued*)

Field Name	Field Description
LS:RI	Logical system and routing instance associated with the subscriber.

## Sample Output

### show subscribers summary

```
user@host> show subscribers summary
```

#### Subscribers by State

```
Init      3
Configured  2
Active    183
Terminating  2
Terminated  1
```

```
TOTAL      191
```

#### Subscribers by Client Type

```
DHCP      107
PPP        76
VLAN       8
```

```
TOTAL      191
```

### show subscribers summary all

```
user@host> show subscribers summary all
```

#### Subscribers by State

```
Init      3
Configured  2
Active    183
Terminating  2
Terminated  1
```

```
TOTAL      191
```

#### Subscribers by Client Type

```
DHCP      107
PPP        76
VLAN       8
```

```
TOTAL      191
```

#### Subscribers by LS:RI

```
default:default  1
default:ri1      28
default:ri2      16
ls1:default      22
ls1:riA          38
ls1:riB          44
logsysX:routinstY 42
```

```
TOTAL      191
```

### show subscribers summary physical-interface

```
user@host> show subscribers summary physical-interface ge-1/0/0
Subscribers by State
  Active: 3998
  Total: 3998

Subscribers by Client Type
  DHCP: 3998
  Total: 3998

Subscribers by LS:RI
  default:default: 3998
  Total: 3998
```

### show subscribers summary physical-interface pic

```
user@host> show subscribers summary physical-interface ge-0/2/0 pic
Subscribers by State
  Active: 4825
  Total: 4825

Subscribers by Client Type
  DHCP: 4825
  Total: 4825

Subscribers by LS:RI
  default:default: 4825
  Total: 4825
```

### show subscribers summary physical-interface port

```
user@host> show subscribers summary physical-interface ge-0/3/0 port
Subscribers by State
  Active: 4825
  Total: 4825

Subscribers by Client Type
  DHCP: 4825
  Total: 4825

Subscribers by LS:RI
  default:default: 4825
  Total: 4825
```

### show subscribers summary physical-interface slot

```
user@host> show subscribers summary physical-interface ge-2/0/0 slot
Subscribers by State
  Active: 4825
  Total: 4825

Subscribers by Client Type
  DHCP: 4825
  Total: 4825

Subscribers by LS:RI
  default:default: 4825
  Total: 4825
```

**show subscribers summary pic**

```

user@host> show subscribers summary pic
Interface          Count
ge-1/0             1000
ge-1/3             1000

Total Subscribers: 2000

```

**show subscribers summary pic (Aggregated Ethernet Interfaces)**

```

user@host> show subscribers summary pic
Interface          Count
ae0: ge-1/0        801
ae0: ge-1/3        801

Total Subscribers: 801

```

**show subscribers summary port**

```

user@host> show subscribers summary port
Interface          Count
ge-1               2000

Total Subscribers: 2000

```

**show subscribers summary slot**

```

user@host> show subscribers summary slot
Interface          Count
ge-1               2000

Total Subscribers: 2000

```

**show subscribers summary terse**

```

user@host> show subscribers summary terse
Interface          IP Address/VLAN ID  User Name          LS:RI
ge-1/3/0.1073741824  100                 WHOLESALE-CLIENT  default:default
demux0.1073741824    100.0.0.10          RETAILER1-CLIENT  test1:retailer1
demux0.1073741825    101.0.0.3           RETAILER2-CLIENT  test1:retailer2
demux0.1073741826    102.0.0.3           RETAILER2-CLIENT  test1:retailer2

```

## test services l2tp tunnel

<b>Syntax</b>	<b>test services l2tp tunnel user <i>user-name</i></b> <b>&lt;password <i>user-password</i>&gt;</b> <b>&lt;tunnel-name <i>name</i>&gt;</b>
<b>Release Information</b>	Command introduced in Junos OS Release 11.4.
<b>Description</b>	(MX Series routers only) Test and verify Layer 2 Tunneling Protocol (L2TP) tunnel configurations from the L2TP access concentrator (LAC). The test determines whether the user can be authenticated and tunneled according to the L2TP configuration. The establishment of all tunnels associated with the user is tested. You can optionally specify a particular tunnel to test for the user.
<b>Options</b>	<p><b>user <i>user-name</i></b>—Name of the user under test. You must use an existing configured username, although it can be created solely for testing a tunnel configuration.</p> <p><b>password <i>user-password</i></b>—(Optional) Authentication password for the specified user. If you omit this option, the test generates a dummy password—<i>testpass</i>—for the user.</p> <p><b>tunnel-name <i>name</i></b>—(Optional) Name of a tunnel to test.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Testing L2TP Tunnel Configurations from the LAC on page 176</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">test services l2tp tunnel (User authentication fails) on page 279</a> <a href="#">test services l2tp tunnel (Multiple tunnels tested) on page 279</a> <a href="#">test services l2tp tunnel (Specific tunnel tested) on page 279</a>
<b>Output Fields</b>	Table 24 on page 278 lists the output fields for the <b>test services l2tp tunnel</b> command. Output fields are listed in the approximate order in which they appear.

**Table 24: test services l2tp tunnel Output Fields**

Field Name	Field Description
<b>Tunnel-name</b>	Name of the tunnel as configured in the local tunnel profile.
<b>Tunnel-peer</b>	IP address of the tunnel's remote peer (the L2TP network server [LNS]).
<b>Logical-System</b>	Logical system in which the tunnel is created.
<b>Routing-Instance</b>	Routing instance in which the tunnel is created.
<b>Status</b>	Status of the tunnel.



## Sample Output

### test services l2tp tunnel (User authentication fails)

```
user@host> test services l2tp tunnel user testuser@example.com
Subscriber: testuser@example.com, authentication failed
```

### test services l2tp tunnel (Multiple tunnels tested)

```
user@host> test services l2tp tunnel user testuser@example.com
Subscriber: testuser@example.com, authentication success, l2tp tunneled
  Tunnel-name  Tunnel-peer  Logical-System  Routing-Instance  Status
  test1tunnel  192.168.2.3  default        default           Up
  test2tunnel  172.24.3.3   default        default           Peer unresponsive
  test3tunnel  172.24.5.1   default        test              Up
```

### test services l2tp tunnel (Specific tunnel tested)

```
user@host> test services l2tp tunnel user testuser@example.com tunnel-name test1tunnel
Subscriber: testuser@example.com, authentication success, l2tp tunneled
  Tunnel-name  Tunnel-peer  Logical-System  Routing-Instance  Status
  test1tunnel  192.168.2.3  default        default           Up
```



## PART 4

# Troubleshooting

- [Acquiring Troubleshooting Information on page 283](#)
- [Troubleshooting Configuration Statement on page 293](#)



# Acquiring Troubleshooting Information

- Tracing L2TP Operations for Subscriber Access on page 283
- Configuring the L2TP Trace Log Filename on page 284
- Configuring the Number and Size of L2TP Log Files on page 285
- Configuring Access to the L2TP Log File on page 285
- Configuring a Regular Expression for L2TP Messages to Be Logged on page 286
- Configuring the L2TP Tracing Flags on page 286
- Configuring Subscriber Filtering for L2TP Trace Operations on page 287
- Configuring the Severity Level to Filter Which L2TP Messages Are Logged on page 288
- Collecting Subscriber Access Logs Before Contacting Juniper Technical Support on page 289

## Tracing L2TP Operations for Subscriber Access

---

The Junos OS trace feature tracks L2TP operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.



**NOTE:** This topic refers to tracing L2TP operations on MX Series routers. To trace L2TP operations on M Series routers, see *Tracing L2TP Operations*.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file located in the `/var/log` directory. By default, the router uses the filename `jl2tpd`. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file **filename** reaches 128 kilobytes (KB), it is compressed and renamed **filename.0.gz**. Subsequent events are logged in a new file called **filename**, until it reaches capacity again. At this point, **filename.0.gz** is renamed **filename.1.gz** and **filename** is compressed and renamed **filename.0.gz**. This process repeats until

the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

You can optionally specify the number of trace files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB). (For more information about how log files are created, see the *Junos OS System Log Messages Reference*.)

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure L2TP tracing operations:

To configure L2TP tracing operations:

1. (Optional) Configure a trace log filename.  
See [“Configuring the L2TP Trace Log Filename” on page 284](#).
2. (Optional) Configure the number and size of trace logs.  
See [“Configuring the Number and Size of L2TP Log Files” on page 285](#).
3. (Optional) Configure user access to trace logs.  
See [“Configuring Access to the L2TP Log File” on page 285](#).
4. (Optional) Configure a regular expression to filter the information to be included in the trace log.  
See [“Configuring a Regular Expression for L2TP Messages to Be Logged” on page 286](#).
5. (Optional) Configure flags to specify which events are logged.  
See [“Configuring the L2TP Tracing Flags” on page 286](#).
6. (Optional) Configure a severity level for messages to specify which event messages are logged.  
See [“Configuring the Severity Level to Filter Which L2TP Messages Are Logged” on page 288](#).

---

## Configuring the L2TP Trace Log Filename

---

By default, the name of the file that records trace output for L2TP is **jl2tpd**. You can specify a different name with the **file** option.

To configure the filename for L2TP tracing operations:

To configure the filename for L2TP tracing operations:

- Specify the name of the file used for the trace output.

```
[edit services l2tp traceoptions]  
user@host# set file l2tp_logfile_1
```

- Related Documentation**
- [Tracing L2TP Operations for Subscriber Access on page 283](#)

## Configuring the Number and Size of L2TP Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format *.number.gz*. The newest archived file is *.0.gz* and the oldest archived file is *.(maximum number)-1.gz*. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, *filename*, reaches 2 MB, *filename* is compressed and renamed *filename.0.gz*, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until there are 20 trace files. Then the oldest file, *filename.19.gz*, is simply overwritten when the next oldest file, *filename.18.gz* is compressed and renamed to *filename.19.gz*.

To configure the number and size of trace files:

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output.

```
[edit services l2tp traceoptions]
user@host# set file l2tp_1_logfile_1 files 20 size 2097152
```

- Related Documentation**
- [Tracing L2TP Operations for Subscriber Access on page 283](#)

## Configuring Access to the L2TP Log File

By default, only the user who configures the tracing operation can access the log files. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

To specify that all users can read the log file:

- Configure the log file to be world-readable.

```
[edit services l2tp traceoptions]
user@host# set file l2tp_1_logfile_1 world-readable
```

To explicitly set the default behavior, only the user who configured tracing can read the log file:

To explicitly set the default behavior, only the user who configured tracing can read the log file:

- Configure the log file to be no-world-readable.

```
[edit services l2tp traceoptions]  
user@host# set file l2tp_1_logfile_1 no-world-readable
```

**Related  
Documentation**

- [Tracing L2TP Operations for Subscriber Access on page 283](#)

---

## Configuring a Regular Expression for L2TP Messages to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including regular expressions to be matched.

To configure regular expressions to be matched:

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit services l2tp traceoptions]  
user@host# set file l2tp_1_logfile_1 match regex
```

**Related  
Documentation**

- [Tracing L2TP Operations for Subscriber Access on page 283](#)

---

## Configuring the L2TP Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit services l2tp traceoptions]  
user@host# set flag flag
```

**Related  
Documentation**

- [Tracing L2TP Operations for Subscriber Access on page 283](#)



## Configuring Subscriber Filtering for L2TP Trace Operations

You can apply filters to L2TP to limit tracing to particular subscribers or domains. Subscriber filtering simplifies troubleshooting in a scaled environment by enabling you to focus on a reduced set of trace results.

For subscriber usernames that have the expected form of **user@domain**, you can filter on the user, the domain, or both. You can use an asterisk (\*) as a wildcard to substitute for characters at the beginning or end of either term or both terms to match a greater number of subscribers.



**NOTE:** You cannot filter results using a wildcard in the middle of the user or domain terms. For example, the following uses of the wildcard are not supported: tom\*25@example.com, tom125@ex\*.com.

When you enable filtering by username, traces that have insufficient information to determine the username are automatically excluded.

To configure subscriber filtering:

To configure subscriber filtering:

- Specify the filter.

```
[edit services l2tp traceoptions]
user@host# set filter user user@domain
```



**NOTE:** This syntax is different than the syntax used to filter subscribers on M Series routers.

Consider the following examples of using the wildcard for filtering:

Consider the following examples of using the wildcard for filtering:

- Filter results for the specific subscriber with the username, tom@example.com.

```
[edit services l2tp traceoptions]
user@host# set filter user tom@example.com
```

- Filter results for all subscribers whose username begins with tom.

```
[edit services l2tp traceoptions]
user@host# set filter user tom*
```

- Filter results for all subscribers whose username ends with tom.

```
[edit services l2tp traceoptions]
user@host# set filter user *tom
```

- Filter results for subscribers with the username tom at all domains beginning with ex.

```
[edit services l2tp traceoptions]
```

```
user@host# set filter user tom@ex*
```

- Filter results for all subscribers at all domains that end with ample.com.

```
[edit services l2tp traceoptions]  
user@host# set filter user *ample.com
```

- Filter results for all subscribers whose username begins with tom at domains that end with example.com.

```
[edit services l2tp traceoptions]  
user@host# set filter user tom*.*example.com
```

#### Related Documentation

- [Tracing L2TP Operations for Subscriber Access on page 283](#)

---

## Configuring the Severity Level to Filter Which L2TP Messages Are Logged

The messages associated with a logged event are categorized according to severity level. You can use the severity level to determine which messages are logged for the event type. A low severity level is less restrictive—filters out fewer messages—than a higher level. When you configure a severity level, all messages at that level and all higher (more restrictive) levels are logged.

The following list presents severity levels in order from lowest (least restrictive) to highest (most restrictive). This order also represents the significance of the messages; for example, **error** messages are of greater concern than **info** messages.

The following list presents severity levels in order from lowest (least restrictive) to highest (most restrictive). This order also represents the significance of the messages; for example, **error** messages are of greater concern than **info** messages.

- **verbose**
- **info**
- **notice**
- **warning**
- **error**

The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **all**. You can also specify **verbose** with the same result, because **verbose** is the lowest (least restrictive) severity level; it has nothing to do with the terseness or verbosity of the messages. Either choice generates a large amount of output. You can specify a more restrictive severity level, such as **notice** or **info** to filter the messages. By default, the trace operation output includes only messages with a severity level of **error**.

To configure the type of messages to be logged:

To configure the type of messages to be logged:

- Configure the message severity level.

```
[edit services l2tp traceoptions]  
user@host# set level severity
```

**Related  
Documentation**

- [Tracing L2TP Operations for Subscriber Access on page 283](#)

---

## Collecting Subscriber Access Logs Before Contacting Juniper Technical Support

---

**Problem**    **Description:** When you experience a subscriber access problem in your network, we recommend that you collect certain logs before you contact Juniper Technical Support. This topic shows you the most useful logs for a variety of network implementations. In addition to the relevant log information, you must also collect standard troubleshooting information and send it to Juniper Technical Support in your request for assistance.

**Solution**    To collect standard troubleshooting information:

To collect standard troubleshooting information:

- Redirect the command output to a file.

```
user@host> request support information | save rsi-1
```

To configure logging to assist Juniper Technical Support:

To configure logging to assist Juniper Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.

[edit]

```
set system syslog archive size 100m files 25
set system auto-configuration traceoptions file filename
set system auto-configuration traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions level all
set protocols ppp-service traceoptions flag all
set protocols ppp traceoptions file filename size 100m files 25
set protocols ppp traceoptions level all
set protocols ppp traceoptions flag all
set protocols ppp monitor-session all
set interfaces pp0 traceoptions flag all
set demux traceoptions file filename size 100m files 25
set demux traceoptions level all
set demux traceoptions flag all
set system processes dhcp-service traceoptions file filename
set system processes dhcp-service traceoptions file size 100m
set system processes dhcp-service traceoptions file files 25
set system processes dhcp-service traceoptions flag all
set class-of-service traceoptions file filename
set class-of-service traceoptions file size 100m
set class-of-service traceoptions flag all
set class-of-service traceoptions file files 25
set routing-options traceoptions file filename
set routing-options traceoptions file size 100m
set routing-options traceoptions flag all
set routing-options traceoptions file files 25
set interfaces traceoptions file filename
set interfaces traceoptions file size 100m
set interfaces traceoptions flag all
set interfaces traceoptions file files 25
set system processes general-authentication-service traceoptions file filename
set system processes general-authentication-service traceoptions file size 100m
set system processes general-authentication-service traceoptions flag all
set system processes general-authentication-service traceoptions file files 25
```

2. Copy the relevant statements into a text file and modify the log filenames as you want.
3. Copy the statements from the text file and paste them into the CLI on your router to configure logging.
4. Commit the logging configuration to begin collecting information.



**NOTE:** The maximum file size for DHCP local server and DHCP relay log files is 1 GB. The maximum number of log files for DHCP local server and DHCP relay is 1000.

---



**BEST PRACTICE:** Enable these logs only to collect information when troubleshooting specific problems. Enabling these logs during normal operations can result in reduced system performance.

**Related  
Documentation**

- *Compressing Troubleshooting Logs from /var/logs to Send to Juniper Technical Support*



## CHAPTER 12

# Troubleshooting Configuration Statement

- [traceoptions \(L2TP\) on page 294](#)

## traceoptions (L2TP)

---

**Syntax**    `traceoptions {  
          debug-level level;  
          file filename <files number> <match regular-expression > <size maximum-file-size>  
                  <world-readable | no-world-readable>;  
          filter {  
            protocol name;  
            user user@domain;  
            user-name username;  
          }  
          flag flag;  
          interfaces interface-name {  
            debug-level level;  
            flag flag;  
          }  
          level (all | error | info | notice | verbose | warning);  
          no-remote-trace;  
          }`

**Hierarchy Level**    [edit services [l2tp](#)]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Define tracing operations for L2TP processes.

**Options**    **debug-level *level***—Trace level for PPP, L2TP, RADIUS, and UDP; this option does not apply to L2TP on MX Series routers:

**debug-level *level***—Trace level for PPP, L2TP, RADIUS, and UDP; this option does not apply to L2TP on MX Series routers:

- **detail**—Trace detailed debug information.
- **error**—Trace error information.
- **packet-dump**—Trace packet decoding information.

**file *filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`.

**files *number***—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

**Range:** 2 through 1000

**Default:** 3 files

**filter**—Additional filter to refine the output to display particular subscribers. Filtering based on the following subscriber identifiers simplifies troubleshooting in a scaled environment.



**filter**—Additional filter to refine the output to display particular subscribers. Filtering based on the following subscriber identifiers simplifies troubleshooting in a scaled environment.

- **protocol *name***—One of the following protocols; this option does not apply to L2TP on MX Series routers:

**protocol *name***—One of the following protocols; this option does not apply to L2TP on MX Series routers:

- **l2tp**
- **ppp**
- **radius**
- **udp**
- **user *user@domain***—Username of a subscriber; this option does not apply to L2TP on M Series routers. Optionally use an asterisk (\*) as a wildcard to substitute for characters at the beginning or end of either term or both terms.
- **user-name *username***—Username of a subscriber; this option does not apply to L2TP on MX Series routers.

**flag flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

**flag flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **configuration**—Trace configuration events.
- **events**—Trace interface events.
- **general**—Trace general events.
- **gres**—Trace GRES events.
- **init**—Trace daemon initialization.
- **ipc-rx**—Trace IPC receive events.
- **ipc-tx**—Trace IPC transmit events.
- **memory**—Trace memory management code.
- **message**—Trace message processing code.
- **packet-error**—Trace packet error events.
- **parse**—Trace parsing events.
- **protocol**—Trace L2TP events.
- **receive-packets**—Trace received L2TP packets.
- **routing-process**—Trace routing process interactions.
- **routing-socket**—Trace routing socket events.
- **session-db**—Trace session database interactions.
- **states**—Trace state machine events.
- **timer**—Trace timer events.
- **transmit-packets**—Trace transmitted L2TP packets.
- **tunnel**—Trace tunnel events.

**interfaces *interface-name***—Apply L2TP traceoptions to a specific services interface. This option does not apply to L2TP on MX Series routers.

**interfaces *interface-name***—Apply L2TP traceoptions to a specific services interface. This option does not apply to L2TP on MX Series routers.

- **debug-level *level***—Trace level for the interface; this option does not apply to L2TP on MX Series routers:
  - **detail**—Trace detailed debug information.
  - **error**—Trace error information.
  - **extensive**—Trace all PIC debug information.
- **flag *flag***—Tracing operation to perform for the interface. This option does not apply to L2TP on MX Series routers. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:
  - **all**—Trace everything.
  - **ipc**—Trace L2TP Inter-Process Communication (IPC) messages between the PIC and the Routing Engine.
  - **packet-dump**—Dump each packet content based on debug level.
  - **protocol**—Trace L2TP, PPP, and multilink handling.
  - **system**—Trace packet processing on the PIC.

**level**—Specify level of tracing to perform. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

**level**—Specify level of tracing to perform. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

- **all**—Match messages of all levels.
- **error**—Match error messages.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure **verbose**, messages at all higher levels are traced. Therefore, the result is the same as when you configure **all**.
- **warning**—Match warning messages.

**Default:** error

**match *regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

**no-remote-trace**—Disable remote tracing.

**no-world-readable**—(Optional) Disable unrestricted file access.

**size** *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**Syntax:** *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

**Range:** 10240 through 1073741824

**world-readable**—(Optional) Enable unrestricted file access.

<b>Required Privilege Level</b>	trace—To view this statement in the configuration.
	trace-control—To add this statement to the configuration.

<b>Related Documentation</b>	• <i>Tracing L2TP Operations</i>
	• <a href="#">Tracing L2TP Operations for Subscriber Access on page 283</a>

## PART 5

# Index

- [Index on page 301](#)



# Index

## Symbols

#, comments in configuration statements.....	xvi
( ), in syntax descriptions.....	xvi
< >, in syntax descriptions.....	xvi
[ ], in configuration statements.....	xvi
{ }, in configuration statements.....	xvi
(pipe), in syntax descriptions.....	xvi

## A

aaa-access-profile statement	
L2TP LNS.....	96
access line information	
conveyed by L2TP.....	28
access-line-information statement	
L2TP.....	97
address statement	
L2TP LNS local gateway.....	97
tunnels	
LAC.....	98
LNS.....	98
address-assignment pool	
configuring for L2TP LNS.....	58
ANCP	
DSL line information for L2TP.....	28
assignment-id-format statement.....	99
avp statement	
L2TP tunnel switch profiles.....	100

## B

bandwidth statement	
inline services.....	100
bearer-type statement	
L2TP tunnel switch profiles.....	101
braces, in configuration statements.....	xvi
brackets	
angle, in syntax descriptions.....	xvi
square, in configuration statements.....	xvi

## C

Calling Number AVP 22	
preventing L2TP LAC from sending.....	42

calling-number statement	
L2TP tunnel switch profiles.....	102
chap statement.....	103, 104
dynamic PPP.....	104
cisco-nas-port-info statement	
L2TP tunnel switch profiles.....	105
clear services l2tp destination command.....	180
clear services l2tp session command.....	181
clear services l2tp session statistics	
command.....	183
clear services l2tp tunnel command.....	185
clear services l2tp tunnel statistics command.....	187
client statement.....	106
comments, in configuration statements.....	xvi
conventions	
text and syntax.....	xv
curly braces, in configuration statements.....	xvi
customer support.....	xvii
contacting JTAC.....	xvii

## D

destination lockout timeout	
L2TP.....	69
destination statement	
L2TP.....	107
destruct-timeout	
L2TP tunnels.....	76
destruct-timeout statement.....	108
dial-options statement.....	109
dynamic profiles.....	110
disable-calling-number-avp statement.....	110
disable-failover-protocol statement.....	111
documentation	
comments on.....	xvii
DSL line information	
conveyed by L2TP.....	28
dynamic PPP statements	
chap.....	104
pap.....	140
ppp-options.....	145
dynamic profiles statements	
dial-options.....	110
keepalives.....	128
dynamic-profile statement	
L2TP.....	111

## E

enable-snmp-tunnel-statistics statement	
L2TP.....	112

examples	
configuring IP fragment reassembly on L2TP LNS.....	61
<b>F</b>	
failover-within-preference statement.....	112
font conventions.....	xv
fpc statement	
MX Series routers.....	113
fragment reassembly	
configuring on L2TP LNS.....	61
on l2tp.....	26
<b>G</b>	
gateway-name statement	
tunnels	
LAC.....	115
LNS.....	114
graceful Routing Engine switchover (GRES)	
L2TP.....	10
GRES See graceful Routing Engine switchover (GRES)	
<b>H</b>	
hello-interval statement	
L2TP.....	117
<b>I</b>	
identification statement	
tunnels.....	117
idle-timeout	
L2TP tunnels.....	75
idle-timeout statement.....	118, 119
inline (FPC level) statements	
inline-services.....	120
inline service interfaces	
configuring for L2TP LNS.....	63
enabling for L2TP LNS.....	61
inline services statements	
bandwidth.....	100
inline-services.....	120
inline-services (FPC level) statement.....	120
inline-services statement.....	120
interface statement	
L2TP service interfaces.....	121
interface-id statement.....	122
IP fragment reassembly	
configuring on L2TP LNS.....	61
on l2tp.....	26
ip-reassembly statement	
L2TP LNS.....	123, 125
ip-reassembly-rules statement	
service-set.....	124
<b>K</b>	
keepalive statement.....	126
keepalives statement.....	127
dynamic profiles.....	128
<b>L</b>	
l2tp	
IP fragment reassembly overview.....	26
L2TP (Layer 2 Tunneling Protocol)	
ANCP-provided DSL line information.....	28
AVPs	
behavior at LTS.....	15
DSL line information.....	28
configuration example	
LNS.....	79
control message retransmission.....	8
defining.....	3
deleting destinations, session, statistics,	
tunnels.....	175
destination lockout timeout.....	69
destruct timeout.....	76
event logging.....	283
failover.....	24
flags for tracing operations.....	286
GRES.....	10
LNS	
configuration overview.....	51
locking out destinations.....	69
log file access for tracing operations.....	285
log file size and number.....	285
log filenames.....	284
maximum retransmission count.....	8
configuring.....	73
message severity levels for tracing	
operations.....	288
minimum retransmission interval.....	8
minimum retransmission time	
configuring.....	73
peer resynchronization.....	24
receive window size.....	76
regular expressions for tracing	
operations.....	286
retransmission attributes.....	8
configuring.....	73



subscriber filtering for tracing operations.....	287	summary information, displaying.....	244
terminology.....	5	switched tunnel	
tracing operations.....	283	displaying.....	237
tunnel idle timeout.....	75	switched tunnel destination	
tunnel profile configuration.....	37	displaying.....	228
LAC address.....	37	switched tunnel session	
LAC hostname.....	37	displaying.....	232
LNS address.....	37	switched tunnel summary	
LNS hostname.....	37	displaying.....	242
logical system.....	37	tunnel destination	
maximum sessions.....	37	displaying.....	215
NAS port method.....	37	lockout period.....	219
password.....	37	tunnel statistics, clearing.....	187
preference.....	37	tunnels, clearing.....	185
profile name.....	37	tunnels, displaying.....	249
routing instance.....	37	tunnels, testing.....	176, 278
tunnel assignment ID.....	37	l2tp statement.....	129
tunnel identifier.....	37	L2TP statements	
tunnel medium.....	37	LAC	
tunnel type.....	37	access-line-information.....	97
tunnel switching		address.....	98
configuring.....	70	assignment-id-format.....	99
overview.....	11	destruct-timeout.....	107, 108
verifying configuration.....	175	disable-calling-number-avp.....	110
L2TP access concentrator. See LAC (L2TP access		disable-failover-protocol.....	111
concentrator)		enable-snmp-tunnel-statistics.....	112
L2TP AVPs		failover-within-preference.....	112
reporting access line information.....	48	gateway-name.....	114, 115
L2TP failover protocol		identification.....	117
preventing L2TP LAC from negotiating.....	44	idle-timeout.....	119
L2TP LAC		l2tp.....	129
subscriber secure policy.....	19	logical-system.....	134
L2TP LAC services		max-sessions.....	135
destination		medium.....	136
clearing.....	180	minimum-retransmission-timeout.....	136
L2TP service interfaces statements		nas-port-method.....	137
interface.....	121	preference.....	146
pool.....	142	remote-gateway.....	147
service-device-pools.....	154	retransmission-count-established.....	149
L2TP services		retransmission-count-not-established.....	150
forcing destination lockout removal.....	148	routing-instance.....	150
forcing expiration of destination lockout		rx-connect-speed-when-equal.....	152
timeouts.....	69	rx-window-size.....	152
session statistics		secret.....	153
clearing.....	183	source-gateway.....	156
sessions		traceoptions.....	157, 294
clearing.....	181	tunnel.....	162, 163
displaying.....	220	tunnel-profile.....	166
subscriber, testing.....	176	tx-address-change.....	168

tx-connect-speed-method.....	169		
type.....	170		
weighted-load-balancing.....	171		
LNS			
aaa-access-profile.....	96		
address.....	97		
bandwidth.....	100		
chap.....	104		
destination.....	107		
destruct-timeout.....	108		
dial-options.....	110		
dynamic-profile.....	111		
enable-snmp-tunnel-statistics.....	112		
gateway-name.....	114		
idle-timeout.....	119		
inline-services.....	120		
interface.....	121		
ip-reassembly (service sets).....	125		
ip-reassembly (services).....	123		
ip-reassembly-rules.....	124		
l2tp.....	129		
l2tp-access-profile.....	131		
local-gateway.....	132		
lockout-timeout.....	133		
match-direction.....	134		
minimum-retransmission-timeout.....	136		
pap.....	140		
pool.....	142		
ppp-options.....	146		
retransmission-count-established.....	149		
retransmission-count-not-established.....	150		
rule.....	151		
rx-window-size.....	152		
service-device-pool.....	153		
service-device-pools.....	154		
service-interface.....	155		
shared-secret.....	155		
tos-reflect.....	156		
traceoptions.....	157, 294		
tunnel.....	163		
tunnel switching			
avp.....	100		
bearer-type.....	101		
calling-number.....	102		
cisco-nas-port-info.....	105		
tunnel-profile.....	165		
tunnel-switch-profile.....	167		
l2tp-access-profile statement.....	131		
		LAC (L2TP access concentrator)	
		access line information.....	48
		address change, ignoring.....	46, 47
		AVPs.....	48
		configuration overview.....	35
		disabling Calling Number AVP 22.....	42
		disabling L2TP failover protocol.....	44
		function.....	3
		interoperation.....	17
		NAS port method.....	17
		Receive Speed, determining.....	42
		reporting access line information.....	48
		Rx Connect Speed AVP	
		sending when transmit and receive speeds	
		are equal.....	44
		Transmit Speed, determining.....	42
		tunnel assignment ID format, setting.....	45
		tunnel name format, setting.....	45
		tunnel selection failover configuration.....	40
		tunnel selection methods.....	19
		tunnel selection parameter configuration.....	40
		weighted load balancing configuration.....	41
		Layer 2 Tunneling Protocol. See L2TP (Layer 2 Tunneling Protocol)	
		lcp-renegotiation statement.....	131
		LNS (L2TP network server)	
		AAA local access profile configuration.....	57
		access profile configuration.....	56
		address-assignment pool, configuring.....	58
		configuration example.....	79
		configuration overview.....	51
		configuring IP fragment reassembly.....	61
		dynamic profile, configuring.....	67
		enabling inline services.....	61
		inline service interface configuration.....	63
		logical interface options configuration.....	64
		peer interface configuration.....	60
		service device pool, configuring.....	66
		service interface pool, configuring.....	66
		subscriber PPP attributes, configuring	
		per si interface.....	54
		with user group profile.....	53
		tunnel group, configuring.....	64
		user group profile configuration.....	56
		user group profile, configuring.....	53
		local-gateway statement.....	132
		lockout-timeout statement	
		L2TP LNS.....	133

- 
- log files
    - collecting for Juniper Technical Support.....289
    - configuring L2TP trace.....283
    - filenames for L2TP.....284
    - number of L2TP.....285
    - size of L2TP.....285
  - logical-system statement
    - tunnels.....134
  - M**
  - manuals
    - comments on.....xvii
  - match-direction statement
    - IP reassembly rule.....134
  - max-sessions statement
    - tunnels.....135
  - maximum-sessions-per-tunnel statement.....135
  - medium statement
    - tunnels.....136
  - minimum-retransmission-timeout statement.....136
  - N**
  - NAS port method
    - LAC.....17
  - nas-port-method statement.....137
  - next-hop-service statement.....138
  - P**
  - pap statement.....139
    - dynamic PPP.....140
    - L2TP.....140
  - parentheses, in syntax descriptions.....xvi
  - pic statement
    - M Series and T Series routers.....141
  - pool statement
    - L2TP service interfaces.....142
  - PPP
    - interfaces, displaying.....200
  - PPP attributes
    - configuring for L2TP LNS subscribers
      - per interface.....54
      - user group profile.....53
  - ppp statement
    - group profile.....143
  - ppp-options statement.....144
    - dynamic PPP.....145
    - L2TP.....146
  - preference statement
    - tunnels.....146
  - processes
    - restarting.....189
  - R**
  - RADIUS attributes
    - defining L2TP tunnels.....37
  - receive connect speed
    - equal to transmit connect speed
      - enabling transmission of AVP 38.....44
      - setting L2TP.....42
  - remote-gateway statement
    - tunnels.....147
  - request services l2tp destination unlock
    - command.....148
  - restart command.....189
  - restarting
    - software processes.....189
  - resynchronization, peer
    - L2TP.....24
  - retransmission
    - L2TP control messages.....8
      - configuring.....73
  - retransmission-count-established statement.....149
  - retransmission-count-not-established
    - statement.....150
  - routing-instance statement
    - tunnels.....150
  - rule statement
    - IP reassembly.....151
  - Rx Connect Speed AVP
    - sending of
      - when transmit and receive speeds are
        - equal.....44
  - rx-connect-speed-when-equal statement.....152
  - rx-window-size
    - L2TP tunnels.....76
  - rx-window-size statement.....152
  - S**
  - secret statement
    - tunnels.....153
  - service-device-pool statement
    - L2TP.....153
  - service-device-pools statement
    - L2TP service interfaces.....154
  - service-interface statement.....155
  - shared-secret statement.....155
  - show ppp interface command.....200
  - show services l2tp destination command.....215

show services l2tp destination lockout	
command.....	219
show services l2tp session command.....	220
show services l2tp summary command.....	244
show services l2tp tunnel command.....	249
show services l2tp tunnel-switch destination	
command.....	228
show services l2tp tunnel-switch session	
command.....	232
show services l2tp tunnel-switch summary	
command.....	242
show services l2tp tunnel-switch tunnel	
command.....	237
show subscribers command.....	255
show subscribers summary command.....	273
silent failover	
L2TP.....	24
source-gateway statement	
tunnels.....	156
subscriber access	
subscriber information, displaying.....	255
subscriber summary information,	
displaying.....	273
subscriber interface statements	
chap.....	104
pap.....	140
ppp-options.....	145
subscriber secure policy	
L2TP LAC subscribers.....	19
subscribers	
displaying.....	255
displaying summary.....	273
support, technical See technical support	
syntax conventions.....	xv

## T

technical support	
collecting logs for.....	289
contacting JTAC.....	xvii
test services l2tp tunnel command.....	278
tos-reflect statement	
L2TP.....	156
trace operations	
collecting logs for Juniper technical	
support.....	289
traceoptions statement	
L2TP.....	157, 294
tracing operations	
L2TP.....	283

transmit connect speed	
equal to receive connect speed	
enabling transmission of AVP 38.....	44
setting L2TP.....	42
troubleshooting subscriber access	
collecting logs for Juniper Technical	
Support.....	289
tunnel assignment ID format	
L2TP LAC, setting.....	45
tunnel idle-timeout	
L2TP.....	75
tunnel name format	
L2TP LAC, setting.....	45
tunnel profile statements	
nas-port-method.....	137
tunnel profile, L2TP	
configuration.....	37
tunnel rx-window-size	
L2TP.....	76
tunnel selection failover	
configuring for L2TP LAC.....	40
tunnel statement.....	162, 163
tunnel statements	
address	
remote gateway.....	98
source gateway.....	98
gateway-name	
LNS gateway.....	114
remote gateway.....	114
source gateway.....	115
identification.....	117
logical-system.....	134
max-sessions.....	135
medium.....	136
preference.....	146
remote-gateway.....	147
routing-instance.....	150
secret.....	153
source-gateway.....	156
tunnel.....	162
tunnel-profile.....	166
type.....	170
tunnel switching statements	
avp.....	100
bearer-type.....	101
calling-number.....	102
cisco-nas-port-info.....	105

tunnel-profile.....	165
tunnel-switch-profile	
applying.....	167
defining.....	167
tunnel switching, L2TP	
AVP handling.....	15
configuring.....	70
overview.....	11
tunnel-group statement.....	164
tunnel-profile statement	
L2TP tunnel switch profiles.....	165
tunnels.....	166
tunnel-switch-profile statement	
L2TP tunnel switch profiles	
applying.....	167
defining.....	167
tx-address-change statement.....	168
tx-connect-speed-method statement.....	169
type statement	
tunnels.....	170
 <b>U</b>	
user group profile	
configuring for L2TP LNS.....	53
user-group-profile statement.....	170
 <b>V</b>	
vendor-specific attributes	
defining L2TP tunnels.....	37
 <b>W</b>	
weighted load balancing	
configuring for L2TP LAC.....	41
weighted-load-balancing statement.....	171

