JUNIPER NETWORKS

Layer 2 Tunneling Protocol

Published: 2012-02-28

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

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

List of Tables

About the Documentation

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:

- M 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:

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:

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.xsl; }
   ```

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 *Junos OS CLI User Guide*.

Documentation Conventions

Table 1 on page ix 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.

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`

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

Convention	Description	Examples
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub** <**default-metric** *metric*>**;**
| (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.	**broadcast | multicast** (***string1*** **|** ***string2*** **|** ***string3***)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

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, 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: https://www.juniper.net/alerts/

- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol Overview

L2TP is defined in RFC 2661,*Layer Two Tunneling Protocol (L2TP)*.

L2TP facilitates the tunneling of PPP packets across an intervening network in a way that is as transparent as possible to both end users and applications. It employs access profiles for group and individual user access, and uses authentication to establish secure connections between the two ends of each tunnel. Multilink PPP functionality is also supported.

The L2TP services are supported on the following routers only:

- M7i routers with AS PICs
- M10i routers with AS and MultiServices 100 PICs
- M120 routers with AS, MultiServices 100, and MultiServices 400 PICs

For more information, see "L2TP Services Configuration Overview" on page 3.

L2TP Services Configuration Overview

The statements for configuring L2TP services are found at the following hierarchy levels:

- **[edit services l2tp tunnel-group** ***group-name*****]**

  The L2TP **tunnel-group** statement identifies an L2TP instance or L2TP server. Associated statements specify the local gateway address on which incoming tunnels and sessions are accepted, the Adaptive Services (AS) Physical Interface Card (PIC) that processes data for the sessions in this tunnel group, references to L2TP and PPP access profiles, and other attributes for configuring window sizes and timer values.

- **[edit interfaces sp-*fpc/pic/port* unit *logical-unit-number* dial-options]**

  The **dial-options** statement includes configuration for the **l2tp-interface-id** statement and the **shared/dedicated** flag. The interface identifier associates a user session with

a logical interface. Sessions can use either shared or dedicated logical interfaces. To run routing protocols, a session must use a dedicated logical interface.

- **[edit access profile *profile-name* client *name* l2tp]**

  Tunnel profiles are defined at the **[edit access]** hierarchy level. Tunnel clients are defined with authentication, multilink negotiation and fragmentation, and other L2TP attributes in these profiles.

- **[edit access profile *profile-name* client *name* ppp]**

  User profiles are defined at the **[edit access]** hierarchy level. User clients are defined with authentication and other PPP attributes in these profiles. These client profiles are used when local authentication is specified.

- **[edit access radius-server *address*]**

  When you configure **authentication-order radius** at the **[edit access profile *profile-name*]** hierarchy level, you must configure a RADIUS service at the **[edit access radius-server]** hierarchy level.

NOTE: For more information about configuring properties at the **[edit access]** hierarchy level, see the *Junos OS System Basics Configuration Guide*. For information about L2TP LAC and LNS configurations on MX Series routers for subscriber access, see L2TP for Subscriber Access Overview in the *Junos Subscriber Access Configuration Guide*.

AS PIC Redundancy for L2TP Services

L2TP services support AS PIC redundancy. To configure redundancy, you specify a redundancy services PIC (**rsp**) interface in which the primary AS PIC is active and a secondary AS PIC is on standby. If the primary AS PIC fails, the secondary PIC becomes active, and all service processing is transferred to it. If the primary AS PIC is restored, it remains in standby and does not preempt the secondary AS PIC; you need to manually restore the services to the primary PIC. To determine which PIC is currently active, issue the **show interfaces redundancy** command.

NOTE: On L2TP, the only service option supported is *warm standby*, in which one backup PIC supports multiple working PICs. Recovery times are not guaranteed, because the configuration must be completely restored on the backup PIC after a failure is detected. The tunnels and sessions are torn down upon switchover and need to be restarted by the LAC and PPP client, respectively. However, configuration is preserved and available on the new active PIC, although the protocol state needs to be reestablished.

As with the other AS PIC services that support warm standby, you can issue the **request interfaces (revert | switchover)** command to manually switch between primary and secondary L2TP interfaces.

For more information, see Configuring AS or Multiservices PIC Redundancy. For an example configuration, see "Examples: Configuring L2TP Services" on page 21. For information on operational mode commands, see the *Junos OS Interfaces Command Reference*.

PART 2

Configuration

CHAPTER 2

Configuration Tasks

L2TP Minimum Configuration

To configure L2TP services, you must perform at least the following tasks:

- Define a tunnel group at the **[edit services l2tp]** hierarchy level with the following attributes:
  - **l2tp-access-profile**—Profile name for the L2TP tunnel.
  - **ppp-access-profile**—Profile name for the L2TP user.
  - **local-gateway**—Address for the L2TP tunnel.
  - **service-interface**—AS PIC interface for the L2TP service.
  - Optionally, you can configure **traceoptions** for debugging purposes.

  The following example shows a minimum configuration for a tunnel group with trace options:

```
[edit services l2tp]
tunnel-group finance-lns-server {
   l2tp-access-profile westcoast_bldg_1_tunnel;
   ppp-access-profile westcoast_bldg_1;
   local-gateway {
      address 10.21.255.129;
   }
   service-interface sp-1/3/0;
}
traceoptions {
   flag all;
   filter {
      protocol udp;
      protocol l2tp;
      protocol ppp;
```

```
        protocol radius;
    }
}
```

- At the **[edit interfaces]** hierarchy level:
  - Identify the physical interface at which L2TP tunnel packets enter the router, for example **ge-0/3/0**.
  - Configure the AS PIC interface with **unit 0 family inet** defined for IP service, and configure another logical interface with **family inet** and the **dial-options** statement.

  The following example shows a minimum interfaces configuration for L2TP:

```
[edit interfaces]
ge-0/3/0 {
    unit 0 {
        family inet {
            address 10.58.255.129/28;
        }
    }
}
sp-1/3/0 {
    unit 0 {
        family inet;
    }
    unit 20 {
        dial-options {
            l2tp-interface-id test;
            shared;
        }
        family inet;
    }
}
```

- At the **[edit access]** hierarchy level:
  - Configure a tunnel profile. Each client specifies a unique L2TP Access Concentrator (LAC) name with an **interface-id** value that matches the one configured on the AS PIC interface unit; **shared-secret** is authentication between the LAC and the L2TP Network Server (LNS).
  - Configure a user profile. If RADIUS is used as the authentication method, it needs to be defined.
  - Define the RADIUS server with an IP address, port, and authentication data shared between the router and the RADIUS server.

NOTE: When the L2TP Network Server (LNS) is configured with RADIUS authentication, the default behavior is to accept the preferred RADIUS-assigned IP address. Previously, the default behavior was to accept and install the nonzero peer IP address that came into the IP-Address option of the IPCP Configuration Request packet.

- Optionally, you can define a group profile for common attributes, for example **keepalive 0** to turn off keepalive messages.

The following example shows a minimum profiles configuration for L2TP:

```
[edit access]
group-profile westcoast_users {
    ppp {
        keepalive 0;
    }
}
profile westcoast_bldg_1_tunnel {
    client production {
        l2tp {
            interface-id test;
            shared-secret "$9$n8HX6A01RhlvL1R"; # SECRET-DATA
        }
        user-group-profile westcoast_users;
    }
}
profile westcoast_bldg_1 {
    authentication-order radius;
}
radius-server {
    192.168.65.63 {
        port 1812;
        secret "$9$Vyb4ZHkPQ39mf9pORlexNdbgoZUjqP5"; # SECRET-DATA
    }
}
```

Configuring L2TP Tunnel Groups

To establish L2TP service on a router, you need to identify an L2TP tunnel group and specify a number of values that define which access profiles, interface addresses, and other properties to use in creating a tunnel. To identify the tunnel group, include the **tunnel-group** statement at the **[edit services l2tp]** hierarchy level:

```
tunnel-group group-name {
    hello-interval seconds;
    hide-avps;
    l2tp-access-profile profile-name;
    local-gateway address address;
    maximum-send-window packets;
    ppp-access-profile profile-name;
    receive-window packets;
    retransmit-interval seconds;
```

```
    service-interface interface-name;
    syslog {
      host hostname {
        services severity-level;
        facility-override facility-name;
        log-prefix prefix-value;
      }
    }
    tunnel-timeout seconds;
}
```

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

This following sections explain how to configure L2TP tunnel groups:

Configuring Access Profiles for L2TP Tunnel Groups

To validate L2TP connections and session requests, you set up access profiles by configuring the **profile** statement at the **[edit access]** hierarchy level. You need to configure two types of profiles:

- L2TP tunnel access profile, which validates all L2TP connection requests to the specified local gateway address
- PPP access profile, which validates all PPP session requests through L2TP tunnels established to the local gateway address

For more information on configuring the profiles, see the *Junos OS System Basics Configuration Guide*. A profile example is included in "Examples: Configuring L2TP Services" on page 21.

To associate the profiles with a tunnel group, include the **l2tp-access-profile** and **ppp-access-profile** statements at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

```
l2tp-access-profile profile-name;
ppp-access-profile profile-name;
```

Configuring the Local Gateway Address and PIC

When you configure an L2TP group, you must also define a local address for the L2TP tunnel connections and the AS PIC that processes the requests:

- To configure the local gateway IP address, include the **local-gateway** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

  local-gateway address *address*;

- To configure the AS PIC, include the **service-interface** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

  service-interface sp-*fpc/pic/port*;

You can optionally specify the logical unit number along with the service interface. If specified, the unit is used as a logical interface representing PPP sessions negotiated using this profile.

NOTE: If you change the local gateway address or the service interface configuration, all L2TP sessions using those settings are terminated.

Dynamic class-of-service (CoS) functionality is supported on L2TP LNS sessions or L2TP sessions with ATM VCs, as long as the L2TP session is configured to use an IQ2 PIC on the egress interface. For more information, see the *Junos OS Class of Service Configuration Guide*.

Configuring Window Size for L2TP Tunnels

You can configure the maximum window size for packet processing at each end of the L2TP tunnel:

- The receive window size limits the number of concurrent packets the server processes. By default, the maximum is 16 packets. To change the window size, include the **receive-window** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

  receive-window *packets*;

- The maximum-send window size limits the other end's receive window size. The information is transmitted in the receive window size attribute-value pair. By default, the maximum is 32 packets. To change the window size, include the **maximum-send-window** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

  maximum-send-window *packets*;

Configuring Timers for L2TP Tunnels

You can configure the following timer values that regulate L2TP tunnel processing:

- Hello interval—If the server does not receive any messages within a specified time interval, the router software sends a hello message to the tunnel's remote peer. By default, the interval length is 60 seconds. If you configure a value of 0, no hello messages are sent. To configure a different value, include the **hello-interval** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

  ```
  hello-interval seconds;
  ```

- Retransmit interval—By default, the retransmit interval length is 30 seconds. To configure a different value, include the **retransmit-interval** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

  ```
  retransmit-interval seconds;
  ```

- Tunnel timeout—If the server cannot send any data through the tunnel within a specified time interval, it assumes that the connection with the remote peer has been lost and deletes the tunnel. By default, the interval length is 120 seconds. To configure a different value, include the **tunnel-timeout** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

  ```
  tunnel-timeout seconds;
  ```

Hiding Attribute-Value Pairs for L2TP Tunnels

Once an L2TP tunnel has been established and the connection authenticated, information is encoded by means of attribute-value pairs. By default, this information is not hidden. To hide the attribute-value pairs once the shared secret is known, include the **hide-avps** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

```
hide-avps;
```

Configuring System Logging of L2TP Tunnel Activity

You can specify properties that control how system log messages are generated for L2TP services.

To configure interface-wide default system logging values, include the **syslog** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

```
syslog {
  host hostname {
    services severity-level;
    facility-override facility-name;
    log-prefix prefix-value;
  }
}
```

Configure the **host** statement with a hostname or IP address that specifies the system log target server. The hostname **local** directs system log messages to the Routing Engine. For external system log servers, the hostname must be reachable from the same routing

instance to which the initial data packet (that triggered session establishment) is delivered. You can specify only one system logging hostname.

Table 3 on page 15 lists the severity levels that you can specify in configuration statements at the **[edit services l2tp tunnel-group *group-name* syslog host *hostname*]** hierarchy level. The levels from **emergency** through **info** are in order from highest severity (greatest effect on functioning) to lowest.

Table 3: System Log Message Severity Levels

Severity Level	Description
any	Includes all severity levels
emergency	System panic or other condition that causes the router to stop functioning
alert	Conditions that require immediate correction, such as a corrupted system database
critical	Critical conditions, such as hard drive errors
error	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels
warning	Conditions that warrant monitoring
notice	Conditions that are not errors but might warrant special handling
info	Events or nonerror conditions of interest

We recommend setting the system logging severity level to **error** during normal operation. To monitor PIC resource usage, set the level to **warning**. To gather information about an intrusion attack when an intrusion detection system error is detected, set the level to **notice** for a specific service set. To debug a configuration or log Network Address Translation (NAT) events, set the level to **info**.

For more information about system log messages, see the *Junos OS System Log Messages Reference*.

To use one particular facility code for all logging to the specified system log host, include the **facility-override** statement at the **[edit services l2tp tunnel-group *group-name* syslog host *hostname*]** hierarchy level:

```
facility-override facility-name;
```

The supported facilities include: **authorization**, **daemon**, **ftp**, **kernel**, **user**, and **local0** through **local7**.

To specify a text prefix for all logging to this system log host, include the **log-prefix** statement at the **[edit services l2tp tunnel-group *group-name* syslog host *hostname*]** hierarchy level:

log-prefix *prefix-text*;

Configuring the Identifier for Logical Interfaces that Provide L2TP Services

You can configure L2TP services on adaptive services interfaces on M7i, M10i, and M120 routers only. You must configure the logical interface to be dedicated or shared. If a logical interface is dedicated, it can represent only one session at a time. A shared logical interface can have multiple sessions.

To configure the logical interface, include the **l2tp-interface-id** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* dial-options]** hierarchy level:

```
l2tp-interface-id name;
(dedicated | shared);
```

The **l2tp-interface-id** name configured on the logical interface must be replicated at the **[edit access profile *name*]** hierarchy level:

- For a user-specific identifier, include the **l2tp-interface-id** statement at the **[edit access profile *name* ppp]** hierarchy level.
- For a group identifier, include the **l2tp-interface-id** statement at the **[edit access profile *name* l2tp]** hierarchy level.

You can configure multiple logical interfaces with the same interface identifier, to be used as a pool for several users. For more information on configuring access profiles, see the *Junos OS System Basics Configuration Guide*.

NOTE: If you delete the dial-options statement settings configured on a logical interface, all L2TP sessions running on that interface are terminated.

Example: Configuring Multilink PPP on a Shared Logical Interface

Multilink PPP is supported on either shared or dedicated logical interfaces. The following example can be used to configure many multilink bundles on a single shared interface:

```
interfaces {
  sp-1/3/0 {
    traceoptions {
      flag all;
    }
    unit 0 {
      family inet;
    }
    unit 20 {
      dial-options {
        l2tp-interface-id test;
        shared;
      }
      family inet;
    }
  }
```

```
}
access {
    profile t {
        client test {
            l2tp {
                interface-id test;
                multilink;
                shared-secret "$9$n8HX6A01RhlvL1R"; # SECRET-DATA
            }
        }
    }
    profile u {
        authentication-order radius;
    }
    radius-server {
        192.168.65.63 {
            port 1812;
            secret "$9$Vyb4ZHkPQ39mf9pORlexNdbgoZUjqP5"; # SECRET-DATA
        }
    }
}
services {
    l2tp {
        tunnel-group 1 {
            l2tp-access-profile t;
            ppp-access-profile u;
            local-gateway {
                address 10.70.1.1;
            }
            service-interface sp-1/3/0;
        }
        traceoptions {
            flag all;
            debug-level packet-dump;
            filter {
                protocol l2tp;
                protocol ppp;
                protocol radius;
            }
        }
    }
}
```

Tracing L2TP Operations

Tracing operations track all AS PIC operations and record them in a log file in the **/var/log** directory. By default, this file is named **/var/log/l2tpd**.

NOTE: This topic refers to tracing L2TP LNS operations on M Series routers. To trace L2TP LAC operations on MX Series routers, see Tracing L2TP Operations for Subscriber Access.

To trace L2TP operations, include the **traceoptions** statement at the **[edit services l2tp]** hierarchy level:

```
traceoptions {
    debug-level level;
    file <filename> <files number> <match regular-expression > <size maximum-file-size>
        <world-readable | no-world-readable>;
    filter {
        protocol name;
        user-name username;
    }
    flag flag;
    interfaces interface-name {
        debug-level severity;
        flag flag;
    }
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
```

You can specify the following L2TP tracing flags:

- **all**—Trace everything.
- **configuration**—Trace configuration events.
- **protocol**—Trace routing protocol events.
- **routing-socket**—Trace routing socket events.
- **rpd**—Trace routing protocol process events.

You can specify a trace level for PPP, L2TP, RADIUS, and User Datagram Protocol (UDP) tracing. To configure a trace level, include the **debug-level** statement at the **[edit services l2tp traceoptions]** hierarchy level and specify one of the following values:

- **detail**—Detailed debug information
- **error**—Errors only
- **packet-dump**—Packet decoding information

You can filter by protocol. To configure filters, include the **filter protocol** statement at the **[edit services l2tp traceoptions]** hierarchy level and specify one or more of the following protocol values:

- **ppp**
- **l2tp**
- **radius**
- **udp**

To implement filtering by protocol name, you must also configure either **flag protocol** or **flag all**.

You can also configure traceoptions for L2TP on a specific adaptive services interface. To configure per-interface tracing, include the **interfaces** statement at the **[edit services l2tp traceoptions]** hierarchy level:

```
interfaces interface-name {
    debug-level level;
    flag flag;
}
```

NOTE: Implementing traceoptions consumes CPU resources and affects the packet processing performance.

You can specify the **debug-level** and **flag** statements for the interface, but the options are slightly different from the general L2TP traceoptions. You specify the debug level as **detail**, **error**, or **extensive**, which provides complete PIC debug information. The following flags are available:

- **all**—Trace everything.
- **ipc**—Trace L2TP Inter-Process Communication (IPC) messages between the PIC and the Routing Engine.
- **packet-dump**—Dump each packet's content based on debug level.
- **protocol**—Trace L2TP, PPP, and multilink handling.
- **system**—Trace packet processing on the PIC.

CHAPTER 3

Example

Examples: Configuring L2TP Services

Configure L2TP with multiple group and user profiles and a pool of logical interfaces for concurrent tunnel sessions:

```
[edit access]
address-pool customer_a {
   address 10.1.1.1/32;
}
address-pool customer_b {
   address-range low 10.2.2.1 high 10.2.3.2;
}
group-profile sunnyvale_users {
   ppp {
      framed-pool customer_a;
      idle-timeout 15;
      primary-dns 192.168.65.1;
      secondary-dns 192.168.65.2;
      primary-wins 192.168.65.3;
      secondary-wins 192.168.65.4;
      interface-id west;
   }
}
group-profile eastcoast_users {
   ppp {
      framed-pool customer_b;
      idle-timeout 20;
      primary-dns 192.168.65.5;
      secondary-dns 192.168.65.6;
      primary-wins 192.168.65.7;
      secondary-wins 192.168.65.8;
      interface-id east;
   }
}
group-profile sunnyvale_tunnel {
   l2tp {
      maximum-sessions-per-tunnel 100;
      interface-id west_shared;
   }
```

```
}
group-profile east_tunnel {
  l2tp {
    maximum-sessions-per-tunnel 125;
    interface-id east_shared;
  }
}
profile sunnyvale_bldg_1 {
  client white {
    chap-secret "$9$3s2690IeK8X7VKM7VwgaJn/Ctu1hclv87Ct87"; #       SECRET-DATA
    ppp {
      idle-timeout 22;
      primary-dns 192.168.65.1;
      framed-ip-address 10.12.12.12/32;
      interface-id east;
    }
    group-profile sunnyvale_users;
  }
  client blue {
    chap-secret "$9$eq1KWxbwgZUHNdjqmTF3uO1Rhr-dsoJDNd"; #       SECRET-DATA
    group-profile sunnyvale_users;
  }
  authentication-order password;
}
profile sunnyvale_bldg_1_tunnel {
  client test {
    l2tp {
      shared-secret "$9$r3HKvLg4ZUDkX7JGjif5p0BIRS8LN"; # SECRET-DATA
      maximum-sessions-per-tunnel 75;
      interface-id west_shared;
      ppp-authentication chap;
    }
    group-profile sunnyvale_tunnel;
  }
  client production {
    l2tp {
      shared-secret
        "$9$R2QErv8X-goGylVwg4jiTz36/t0BEleWFnRhrlXxbs2aJDHqf3nCP5";
      ppp-authentication chap;
    }
    group-profile sunnyvale_tunnel;
  }
}
[edit services]
l2tp {
  tunnel-group finance-lns-server {
    l2tp-access-profile sunnyvale_bldg_1_tunnel;
    ppp-access-profile sunnyvale_bldg_1;
    local-gateway {
      address 10.1.117.3;
    }
    service-interface sp-1/3/0;
    receive-window 1500;
    maximum-send-window 1200;
    retransmit-interval 5;
    hello-interval 15;
```

```
        tunnel-timeout 55;
    }
    traceoptions {
        flag all;
    }
}
[edit interfaces sp-1/3/0]
unit0 {
    family inet;
}
unit 10 {
    dial-options {
        l2tp-interface-id foo-user;
        dedicated;
    }
    family inet;
}
unit 11 {
    dial-options {
        l2tp-interface-id east;
        dedicated;
    }
    family inet;
}
unit 12 {
    dial-options {
        l2tp-interface-id east;
        dedicated;
    }
    family inet;
}
unit 21 {
    dial-options {
        l2tp-interface-id west;
        dedicated;
    }
    family inet;
}
unit 30 {
    dial-options {
        l2tp-interface-id west_shared;
        shared;
    }
    family inet;
}
unit 40 {
    dial-options {
        l2tp-interface-id east_shared;
        shared;
    }
    family inet;
}
```

Configure L2TP redundancy:

```
interfaces {
```

```
    rsp0 {
      redundancy-options {
        primary sp-0/0/0;
        secondary sp-1/3/0;
      }
      unit 0 {
        family inet;
      }
      unit 11 {
        dial-options {
          l2tp-interface-id east_shared;
          shared;
        }
        family inet;
      }
    }
}
```

CHAPTER 4

Configuration Statements

facility-override

Syntax facility-override *facility-name*;

Hierarchy Level [edit services l2tp tunnel-group *group-name* syslog host *hostname*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Override the default facility for system log reporting.

Options ***facility-name***—Name of the facility that overrides the default assignment. Valid entries include:

- **authorization**
- **daemon**
- **ftp**
- **kernel**
- **local0** through **local7**
- **user**

Usage Guidelines See "Configuring System Logging of L2TP Tunnel Activity" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

hello-interval

Syntax hello-interval *seconds*;

Hierarchy Level [edit services l2tp tunnel-group *name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the keepalive timer for L2TP tunnels.

NOTE: Subordinate statement support depends on the platform. See individual statement topics for more detailed support information.

Options ***seconds***—Interval, in seconds, after which the server sends a hello message if no messages are received. A value of **0** means that no hello messages are sent.

Default: 60 seconds

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Timers for L2TP Tunnels on page 14
- Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces

hide-avps

Syntax hide-avps;

Hierarchy Level [edit services l2tp tunnel-group *name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Hide L2TP attribute-value pairs if the secret shared between the two ends of the tunnel is known.

NOTE: This statement is not supported for L2TP LNS on MX Series routers.

Default Attribute-value pairs that can be hidden are exposed, even if the secret information is known.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Hiding Attribute-Value Pairs for L2TP Tunnels on page 14

host

Syntax
```
host hostname {
  services severity-level;
  facility-override facility-name;
  log-prefix prefix-value;
}
```

Hierarchy Level [edit services l2tp tunnel-group *group-name* syslog]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the hostname for the system logging utility.

Options ***hostname***—Name of the system logging utility host machine. This can be the local Routing Engine or an external server address.

The remaining statements are explained separately.

Usage Guidelines See "Configuring System Logging of L2TP Tunnel Activity" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

l2tp-access-profile

Syntax l2tp-access-profile *profile-name*;

Hierarchy Level [edit services l2tp tunnel-group *name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the profile used to validate all L2TP connection requests to the local gateway address.

Options ***profile-name***—Identifier for the L2TP connection profile.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring Access Profiles for L2TP Tunnel Groups on page 12
- Configuring an L2TP Access Profile on the LNS

local-gateway address

Syntax local-gateway address *address*;

Hierarchy Level [edit services l2tp tunnel-group *name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the local (LNS) IP address for L2TP tunnel.

Options ***address***—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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring the Local Gateway Address and PIC on page 13.
- Configuring L2TP Tunnel Groups on page 11
- Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces

log-prefix

Syntax log-prefix *prefix-value*;

Hierarchy Level [edit services l2tp tunnel-group *group-name* syslog host *hostname*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Set the system logging prefix value.

Options ***prefix-value***—System logging prefix value.

Usage Guidelines See "Configuring System Logging of L2TP Tunnel Activity" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

maximum-send-window

Syntax maximum-send-window *packets*;

Hierarchy Level [edit services l2tp tunnel-group *name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the size of the send window for L2TP tunnels, which limits the remote end's receive window size.

NOTE: This statement is not supported for L2TP LNS on MX Series routers.

Options ***packets***—Maximum number of packets the send window can hold at one time.
Default: 32

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Window Size for L2TP Tunnels on page 13

ppp-access-profile

Syntax ppp-access-profile *profile-name*;

Hierarchy Level [edit services l2tp tunnel-group *name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the profile used to validate all Point-to-Point Protocol (PPP) session requests through L2TP tunnels established to the local gateway address.

NOTE: This statement is not supported for L2TP LNS on MX Series routers.

Options *profile-name*—Identifier for the PPP profile.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring Access Profiles for L2TP Tunnel Groups on page 12

receive-window

Syntax receive-window *packets*;

Hierarchy Level [edit services l2tp tunnel-group *name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the size of the receive window for L2TP tunnels, which limits the number of packets the server processes concurrently.

NOTE: This statement is not supported for L2TP LNS on MX Series routers.

Options *packets*—Maximum number of packets the receive window can hold at one time.
Default: 16

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring Window Size for L2TP Tunnels on page 13

retransmit-interval

Syntax retransmit-interval *seconds*;

Hierarchy Level [edit services l2tp tunnel-group *name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the maximum retransmit interval for L2TP tunnels.

NOTE: This statement is not supported for L2TP LNS on MX Series routers.

Options ***seconds***—Interval, in seconds, after which the server retransmits data if no acknowledgment is received.

Default: 30 seconds

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Timers for L2TP Tunnels on page 14

service-interface

Syntax service-interface *interface-name*;

Hierarchy Level [edit services l2tp tunnel-group *name*]

Release Information Statement introduced before Junos OS Release 7.4.
Option **si-*fpc/pic/port*** introduced in Junos OS Release 11.4.

Description Specify the service interface responsible for handling L2TP processing.

NOTE: 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.

Options ***interface-name***—Name of the service interface. The interface type depends on the line card as follows:

- **sp-*fpc/pic/port***—On AS or Multiservices PICs on M7i, M10i, and M120 routers.
- **si-*fpc/pic/port***—On MPCs on MX Series routers.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Local Gateway Address and PIC on page 13
- Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces

services (Hierarchy)

Syntax services l2tp { ... }

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the service properties to be applied to traffic.

Options **l2tp**—Identifies the L2TP set of services statements.

Usage Guidelines See "L2TP Services Configuration Overview" on page 3.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

services (L2TP System Logging)

Syntax services *severity-level*;

Hierarchy Level [edit services l2tp tunnel-group *group-name* syslog host *hostname*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the system logging severity level.

Options ***severity-level***—Assigns a severity level to the facility. Valid entries include:

- **alert**—Conditions that should be corrected immediately.
- **any**—Matches any level.
- **critical**—Critical conditions.
- **emergency**—Panic conditions.
- **error**—Error conditions.
- **info**—Informational messages.
- **notice**—Conditions that require special handling.
- **warning**—Warning messages.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring System Logging of L2TP Tunnel Activity on page 14

syslog

Syntax

```
syslog {
  host hostname {
    services severity-level;
    facility-override facility-name;
    log-prefix prefix-value;
  }
}
```

Hierarchy Level [edit services l2tp tunnel-group *group-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the generation of system log messages for L2TP services. System log information is passed to the kernel for logging in the **/var/log/l2tpd** directory.

NOTE: This statement is not supported for L2TP LNS on MX Series routers.

Options The remaining statements are described separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring System Logging of L2TP Tunnel Activity on page 14

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-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:

- **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 protocol *name*—Additional filter for the specified protocol; this option does not apply to L2TP on MX Series routers:

- **l2tp**
- **ppp**
- **radius**
- **udp**

filter user-name *username*—Additional filter for the specified username; 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:

- **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.

- **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. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

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.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- Tracing L2TP Operations on page 17
- Tracing L2TP Operations for Subscriber Access

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;
    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-timeout seconds;
}
```

Hierarchy Level [edit services l2tp]

Release Information Statement introduced before Junos OS Release 7.4.

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 on page 11
- Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces

tunnel-timeout

Syntax tunnel-timeout *seconds*;

Hierarchy Level [edit services l2tp tunnel-group *name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the maximum downtime for an L2TP tunnel, after which the tunnel is terminated because the connection is presumed to have been lost.

Options ***seconds***—Interval after which the tunnel is terminated if no data can be sent.

Default: 120 seconds

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Timers for L2TP Tunnels on page 14
- Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces

PART 3

Administration

CHAPTER 5

Layer 2 Tunneling Protocol Operational Mode Commands

clear services l2tp multilink

Syntax clear services l2tp multilink (all <statistics> | bundle-id *number* <statistics> | statistics (all | bundle-id *number*))

Release Information Command introduced before Junos OS Release 7.4.

Description (M10i and M7i routers only) Close Layer 2 Tunneling Protocol (L2TP) multilink sessions or clear session statistics.

Options

all <statistics>—Close all L2TP multilink sessions or clear statistics for all L2TP multilink sessions.

bundle-id *number* <statistics>—L2TP multilink bundle ID. The value is an internally generated number from 1 to 65535. Close the specified L2TP multilink session, or using the **statistics** keyword with this option, clear statistics for the specified session.

statistics (all | bundle-id *number*)—Clear all session statistics or clear statistics for the specified multilink bundle ID.

Required Privilege Level view

Related Documentation

- show services l2tp multilink on page 49

List of Sample Output clear services l2tp multilink statistics all on page 44

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services l2tp multilink statistics all

```
user@host> clear services l2tp multilink statistics all
  Multilink 1 statistics cleared
```

clear services l2tp session

Syntax clear services l2tp session (all | 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* | tunnel-group *group-name* | user *username*)

Release Information Command introduced before Junos OS Release 7.4.

Description (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.

Options **all**—Close all L2TP sessions.

interface ***interface-name***—Clear only the L2TP sessions using 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***—Clear only the L2TP sessions associated with the specified local gateway address.

local-gateway-name ***gateway-name***—Clear only the L2TP sessions associated with the specified local gateway name.

local-session-id ***session-id*** —Clear only the L2TP sessions with this identifier for the local endpoint of the L2TP session.

local-tunnel-id ***tunnel-id***—Clear only the L2TP sessions associated with the specified local tunnel identifier.

peer-gateway ***gateway-address***—Clear only the L2TP sessions associated with the peer gateway with the specified address.

peer-gateway-name ***gateway-name***—Clear only the L2TP sessions associated with the peer gateway with the specified name.

tunnel-group ***group-name***—Clear only the L2TP sessions associated with the specified tunnel group. This option is not available for L2TP LAC on MX Series routers.

user ***username*** —Clear only the L2TP sessions for the specified username. This option is not available for L2TP LAC on MX Series routers.

Required Privilege Level clear

Related Documentation

- clear services l2tp session statistics
- show services l2tp session on page 57

List of Sample Output

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 tunnel statistics

Syntax clear services l2tp tunnel statistics (all | interface sp-*fpc/pic/port* | local-gateway *gateway-address* | local-gateway-name *gateway-name* | local-tunnel-id *tunnel-id* | peer-gateway *gateway-address* | peer-gateway-name *gateway-name* | tunnel-group *group-name*)

Release Information Command introduced before Junos OS Release 7.4.
Support for MX Series routers added in Junos OS Release 10.4.

Description (M10i and M7i routers: LNS only. MX Series routers: LAC only.) Clear statistics for Layer 2 Tunneling Protocol (L2TP) tunnels.

Options

all—Clear statistics for all L2TP tunnels.

interface sp-*fpc/pic/port*—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.

local-gateway *gateway-address*—Clear statistics for only the L2TP tunnels associated with the local gateway with the specified address.

local-gateway-name *gateway-name*—Clear statistics for only the L2TP tunnels associated with the local gateway with the specified name.

local-tunnel-id *tunnel-id*—Clear statistics for only the L2TP tunnels that have the specified local tunnel identifier.

peer-gateway *gateway-address*—Clear statistics for only the L2TP tunnels associated with the peer gateway with the specified address.

peer-gateway-name *gateway-name*—Clear statistics for only the L2TP tunnels associated with the peer gateway with the specified name.

tunnel-group *group-name*—Clear statistics for only the L2TP tunnels in the specified tunnel group. This option is not available for L2TP LAC on MX Series routers.

Required Privilege Level clear

Related Documentation

- clear services l2tp tunnel
- show services l2tp tunnel on page 66

List of Sample Output clear services l2tp tunnel statistics all on page 48

Output Fields 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
```

show services l2tp multilink

Syntax
show services l2tp multilink
<brief | detail | extensive | statistics>
<bundle-id *number*>

Release Information
Command introduced before Junos OS Release 7.4.

Description
(M10i and M7i routers only) Display L2TP output organized by multilink bundle.

Options
none—Same as brief.

brief | detail | extensive | statistics—(Optional) Display the specified level of output. Use the **statistics** option to display packets and bytes that have been encapsulated in the Multilink Protocol. Nonmultilink packets received on member sessions are not counted here.

bundle-id *number*—(Optional) Display L2TP multilink bundle information for only the specified bundle.

Required Privilege Level
view

Related Documentation
- clear services l2tp multilink on page 44

List of Sample Output
show services l2tp multilink extensive on page 52

Output Fields
Table 4 on page 49 lists the output fields for the **show services l2tp multilink** command. Output fields are listed in the approximate order in which they appear.

Table 4: show services l2tp multilink Output Fields

Field Name	Field Description	Level of Output
Bundle ID	Bundle identifier.	All levels
Links	Number of links in the multilink bundle.	All levels
Bundle endpoint	Endpoint discriminator that represents the device transmitting the packet.	All levels
Input MRRU	Maximum packet size that the input interface can process.	detail
Output MRRU	Maximum packet size that the output interface can process.	detail
Session local ID	Identifier of the local endpoint of the L2TP session, as assigned by the L2TP network server (LNS).	detail

Table 4: show services l2tp multilink Output Fields *(continued)*

Field Name	Field Description	Level of Output
Session remote ID	Identifier of the remote endpoint of the L2TP session, as assigned by the L2TP access concentrator (LAC).	detail
State	Status of the L2TP session: • **Established**—The session is operating. • **closed**—The session is being closed. • **destroyed**—The session is being destroyed. • **clean-up**—The session is being cleaned up. • **lns-ic-accept-new**—A new session is being accepted. • **lns-ic-idle**—The session has been created and is idle. • **lns-ic-reject-new**—The new session is being rejected. • **lns-ic-wait-connect**—The session is waiting for the peer's incoming call connected (ICCN) message.	detail
Username	Name of the user logged in to the session.	detail
Mode	Mode of the interface representing the multilink bundle: **dedicated** or **shared**.	extensive
Local IP	IP address of the local endpoint of the Point-to-Point Protocol (PPP) session.	extensive
Remote IP	IP address of the remote endpoint of the PPP session.	extensive
Local name	Name of the LNS instance in which the session was created.	extensive
Remote name	Name of the LAC from which the session was created.	extensive
Local MRU	Maximum receive unit (MRU) setting of the local device, in bytes.	extensive
Remote MRU	MRU setting of the remote device, in bytes.	extensive

Table 4: show services l2tp multilink Output Fields *(continued)*

Field Name	Field Description	Level of Output
Statistics since	Date and time when collection of the following statistics began: • **Control Tx**—Amount of control information transmitted, in packets and bytes. • **Control Rx**—Amount of control information received, in packets and bytes. • **Data Tx**—Amount of data transmitted, in packets and bytes. • **Data Rx**—Amount of data received, in packets and bytes. • **Errors Tx**—Number of errors transmitted, in packets. • **Errors Rx**—Number of errors received, in packets. • **Lcp Echo Req Tx**—Number of LCP echo requests transmitted, in packets. • **Lcp Echo Req Rx**—Number of LCP echo requests received, in packets. • **Lcp Echo Rep Tx**—Number of LCP echo responses transmitted, in packets. • **Lcp Echo Rep Rx**—Number of LCP echo responses received, in packets. • **Lcp Echo Req Timeout**—Number of LCP echo requests that timed out. • **Lcp Echo Req Error**—Number of errors received for LCP echo packets. • **Lcp Echo Rep Error** —Number of errors transmitted for LCP echo packets. • **MRRU**—Maximum packet size processed. • **TX**—Number of packets transmitted. • **RX**—Number of packets received. • **link**—Link of the multilink bundle associated with the L2TP session.	extensive

Sample Output

show services l2tp multilink extensive

```
user@host> show services l2tp multilink extensive
Bundle ID: 1
  Links: 2, Bundle endpoint: user@juniper.com
  Input MRRU: 1524, Output MRRU: 1524
  Session local ID: 46122, Session remote ID: 39307
    State: Established, Username: user1@juniper.com, Mode: dedicated
    Local IP: 10.58.255.129:1701, Remote IP: 10.58.255.131:1701
    Local name: router3, Remote name: router4
  Session local ID:  4254, Session remote ID: 39308
    State: Established, Username: user2@juniper.com, Mode: dedicated
    Local IP: 10.1.255.1:1701, Remote IP: 10.1.255.2:1701
    Local name: router1, Remote name: router2
  Statistics since: Mon May 17 11:47:35 2004
                        Packets        Bytes
      Control Tx              7          196
      Control Rx              3           90
      Data Tx                 0            0
      Data Rx                 0            0
      Errors Tx               0
      Errors Rx               0
   Lcp Echo Req Tx         0
   Lcp Echo Req Rx         0
   Lcp Echo Rep Tx         0
   Lcp Echo Rep Rx         0
   Lcp Echo Req Timeout         0
   Lcp Echo Req Error           0
   Lcp Echo Rep Error           0
   MRRU 1486 droptime 0 maxfrag 0   minfrag 32  minmru 1482 maxqlen 3000
     TX: Packets 0    Frags 0    Txseq 0x0
     RX: Packets 24   Frags 24   Rxseq 0x18   mseq 23  maxdiff 1   reass 24
        fragments copied 0
     link 0 : seq 0x17 mru 1482 encaplen 8  qlen 0   context 0xea01eb0
```

show services l2tp radius

Syntax
show services l2tp radius
<accounting (servers | statistics)>
<authentication (servers | statistics)>
<servers>
<statistics>

Release Information Command introduced in Junos OS Release 9.0.

Description (M7i, M10i, and M120 routers only) Display RADIUS servers and statistics information for the RADIUS servers configured on the router.

Options You must include one of the following keywords to provide a valid completion for the command:

accounting (servers | statistics)—(Optional) Display RADIUS servers or statistical accounting information only.

authentication (servers | statistics)—(Optional) Display RADIUS servers or statistical authentication information only.

servers—(Optional) Display RADIUS authentication and accounting server information only.

statistics—(Optional) Display RADIUS authentication and accounting statistics information only.

Required Privilege Level view

List of Sample Output
show services l2tp radius servers on page 54
show services l2tp radius statistics on page 55

Output Fields Table 5 on page 53 lists the output fields for the **show services l2tp radius** command. Output fields are listed in the approximate order in which they appear.

Table 5: show services l2tp radius Output Fields

Field Name	Field Description
IP Address	IP address of the server.
State	(**servers** keyword only) Present state of the server.
UDP Port	Number of the UDP port used to send authentication or accounting messages to the server.
Retry Count	(**servers** keyword only) Number of times the RADIUS client resends a packet if no ACK is received.
Timeout	(**servers** keyword only) Length of time the client waits for an ACK before retransmission.
Pending Requests	(**servers** keyword only) Number of client pending authentication or accounting requests.

Table 5: show services l2tp radius Output Fields *(continued)*

Field Name	Field Description
Maximum Sessions	(**servers** keyword only) Maximum number of pending requests on each RADIUS client before the server moves to the next RADIUS client, which is 200 times the maximum number of clients that can be created on a server (which is 12).
Dead Time	(**servers** keyword only) Interval to wait before retrying a server after it fails to send a response to an authentication or accounting request.
Secret Type	(**servers** keyword only) Secret type configured on the RADIUS server.
Profile	(**servers** keyword only) Name of profile configured for the RADIUS server.
Access requests	(**statistics** keyword only) Number of access requests sent to the server.
Rollover requests	(**statistics** keyword only) Number of requests coming into the server as a result of the previous server timing out.
Retransmissions	(**statistics** keyword only) Number of retransmissions.
Access accepts	(**statistics** keyword only) Number of access accept messages received from the server.
Access rejects	(**statistics** keyword only) Number of access reject messages received from the server.
Access challenges	(**statistics** keyword only) Number of access challenges received from the server.
Malformed responses	(**statistics** keyword only) Number of responses with attributes having an invalid length or unexpected attributes (such as two attributes when the response is required to have at most one).
Bad authenticators	(**statistics** keyword only) Number of responses in which the authenticator is incorrect for the matching request. This can occur if the RADIUS secrets for the client and server do not match.
Requests pending	(**statistics** keyword only) Number of requests waiting for a response.
Request timeouts	(**statistics** keyword only) Number of requests that timed out.
Unknown responses	(**statistics** keyword only) Number of unknown responses. The RADIUS response type in the header is invalid or unsupported.
Packets dropped	(**statistics** keyword only) Number of packets dropped because they are too short or because the router receives a response for which there is no corresponding request. For example, if the router sends a request that times out, the router removes the request from the list and sends a new request. If the server is slow and sends a response to the first request after the router removes the request, the packet is dropped.

Sample Output

show services l2tp radius servers

```
user@host> show services l2tp radius servers
                                RADIUS Authentication Servers

                                    UDP  Retry        Pending  Maximum  Dead   Secret
```

```
    IP Address     State   Port Count Timeout Requests Sessions Time   Type
  17.1.1.1         Active  1812 2     25      0        2400     300  radius-key

  133.122.1.1      Active  1812 5     35      0        2400     300  radius-key

  134.141.1.1      Active  1812 2     25      0        2400     300  radius-key

  172.28.30.174    Active  1812 7     75      0        2400     300  radius-key

  172.28.30.175    Active  1812 7     75      0        2400     300  radius-key

  172.28.30.176    Active  1812 4     55      0        2400     300  radius-key

  172.128.30.176   Active  1812 3     3       0        2400     300  none-set
  172.128.130.174  Active  1812 7     75      0        2400     300  radius-key

                          RADIUS Accounting Servers

                          UDP  Retry         Pending  Maximum  Dead   Secret
    IP Address     State   Port Count Timeout Requests Sessions Time   Type
  17.1.1.1         Active  1813 2     25      0        2400     300  radius-key

  133.122.1.1      Active  1813 5     35      0        2400     300  radius-key

  134.141.1.1      Active  1813 2     25      0        2400     300  radius-key

  172.28.30.174    Active  1813 7     75      0        2400     300  radius-key

  172.28.30.175    Active  1813 7     75      0        2400     300  radius-key

  172.28.30.176    Active  1813 4     55      0        2400     300  radius-key

  172.128.30.176   Active  1813 3     3       0        2400     300  none-set
  172.128.130.174  Active  1813 7     75      0        2400     300  radius-key

                          RADIUS Accounting Servers

 Profile: user1
```

show services l2tp radius statistics

```
user@host> show services l2tp radius statistics
     RADIUS Authentication Statistics

Authentication statistics:
  Server 17.1.1.1, UDP port: 1812
    Access requests     : 40
    Rollover requests   : 5
    Retransmissions     : 2
    Access accepts      : 39
    Access rejects      : 1
    Access challenges   : 3
    Malformed responses : 0
    Bad authenticators  : 0
    Requests pending    : 1
    Request timeouts    : 0
    Unknown responses   : 0
    Packets dropped     : 0

     RADIUS Accounting Statistics
```

```
Accounting statistics:
 Server 172.128.130.174, UDP port: 1813
   Total requests      : 9
   Start requests      : 6
   Interim requests    : 1
   Stop requests       : 2
   Rollover requests   : 0
   Retransmissions     : 1
   Total response      : 9
   Start responses     : 6
   Interim responses   : 1
   Stop responses      : 2
   Malformed responses : 0
   Bad authenticators  : 0
   Requests pending    : 1
   Request timeouts    : 0
   Unknown responses   : 0
   Packets dropped     : 0
```

show services l2tp session

Syntax

show services l2tp session
<brief | detail | extensive | statistics>
<interface sp-*fpc/pic/port*>
<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*>
<tunnel-group *group-name*>
<user *username*>

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M10i and M7i routers only) Display a list of active L2TP sessions for LNS.

(MX Series routers only) Display a list of active L2TP sessions for LAC.

Options

none—Display standard information about all active L2TP sessions.

brief | detail | extensive | statistics—(Optional) Display the specified level of output. Use the **statistics** option to display packet and byte counts for each session.

interface sp-*fpc/pic/port*—(Optional) Display L2TP session information for only the specified adaptive services interface. This option is not available for L2TP LAC 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.

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*—(Optional) Display L2TP session information for only the specified username.

Required Privilege Level view

Related Documentation
- clear services l2tp session on page 45

List of Sample Output
show services l2tp session (LNS) on page 60
show services l2tp session (LAC) on page 61
show services l2tp session detail (LAC) on page 61
show services l2tp session extensive (LAC) on page 61
show services l2tp session extensive (LNS) on page 61

Output Fields Table 6 on page 58 lists the output fields for the **show services l2tp session** command. Output fields are listed in the approximate order in which they appear.

Table 6: show services l2tp session Output Fields

Field Name	Field Description	Level of Output
Interface	(LNS only) Name of an adaptive services interface.	All levels
Tunnel group	(LNS only) Name of a tunnel group.	All levels
Tunnel local ID	Identifier of the local endpoint of the tunnel, as assigned by the L2TP network server (LNS).	All levels
Session local ID	Identifier of the local endpoint of the L2TP session, as assigned by the LNS.	All levels
Session remote ID	Identifier of the remote endpoint of the L2TP session, as assigned by the L2TP access concentrator (LAC).	All levels
State	State of the L2TP session: • **Established**—The session is operating. This is the only state supported for the LAC. • **closed**—The session is being closed. • **destroyed**—The session is being destroyed. • **clean-up**—The session is being cleaned up. • **lns-ic-accept-new**—A new session is being accepted. • **lns-ic-idle**—The session has been created and is idle. • **lns-ic-reject-new**—The new session is being rejected. • **lns-ic-wait-connect**—The session is waiting for the peer's incoming call connected (ICCN) message.	All levels
Bundle ID	(LNS only) Bundle identifier. Indicates the session is part of a multilink bundle. Sessions that have a blank **Bundle** 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 **show services l2tp multilink extensive** command.	All levels

Table 6: show services l2tp session Output Fields *(continued)*

Field Name	Field Description	Level of Output
Mode	(LNS) Mode of the interface representing the session: **shared** or **exclusive**. (LAC) Mode of the interface representing the session: **shared** or **dedicated**. Only **dedicated** is currently supported for the LAC.	**extensive**
Local IP	IP address of local endpoint of the Point-to-Point Protocol (PPP) session.	**extensive**
Remote IP	IP address of remote endpoint of the PPP session.	**extensive**
Username	(LNS only) Name of the user logged in to the session.	All levels
Assigned IP address	(LNS only) IP address assigned to remote client.	**extensive**
Local name	For LNS, name of the LNS instance in which the session was created. For LAC, name of the LAC.	**extensive**
Remote name	For LNS, name of the LAC from which the session was created. For LAC, name of the LAC instance.	**extensive**
Local MRU	(LNS only) Maximum receive unit (MRU) setting of the local device, in bytes.	**extensive**
Remote MRU	(LNS only) MRU setting of the remote device, in bytes.	**extensive**
Tx speed	Transmit speed of the physical PPP link, in bps.	**extensive**
Rx speed	Receive speed of the physical PPP link, in bps.	**extensive**
Bearer type	Type of bearer enabled: • **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). • **1**—Digital access requested. • **2**—Analog access requested. • **4**—Asynchronous Transfer Mode (ATM) bearer support.	**extensive**
Framing type	Type of framing enabled: • **1**—Synchronous framing • **2**—Asynchronous framing	**extensive**
LCP renegotiation	(LNS only) Whether Link Control Protocol (LCP) renegotiation is configured: **On** or **Off**.	**extensive**
Authentication	Type of authentication algorithm used: Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).	**extensive**
Interface ID	(LNS only) Identifier used to look up the logical interface for this session.	**extensive**
Interface unit	Logical interface for this session.	All levels

Table 6: show services l2tp session Output Fields *(continued)*

Field Name	Field Description	Level of Output
Call serial number	Unique serial number assigned to the call.	**extensive**
Policer bandwidth	Maximum policer bandwidth configured for this session.	**extensive**
Policer burst size	Maximum policer burst size configured for this session.	**extensive**
Firewall filter	Configured firewall filter name.	**extensive**
Session encapsulation overhead	Overhead allowance configured for this session, in bytes.	**extensive**
Session cell overhead	Cell overhead activation (**On** or **Off**).	**extensive**
Create time	Date and time when the call was created.	**extensive**
Up time	Length of time elapsed since the call became active, in hours, minutes, and seconds.	**extensive**
Idle time	Length of time elapsed since the call became idle, in hours, minutes, and seconds.	**extensive**
Statistics since	Date and time when collection of the following statistics began: • **Control Tx**—Amount of control information transmitted, in packets and bytes. • **Control Rx**—Amount of control information received, in packets and bytes. • **Data Tx**—Amount of data transmitted, in packets and bytes. • **Data Rx**—Amount of data received, in packets and bytes. • **Errors Tx**—Number of errors transmitted, in packets. • **Errors Rx**—Number of errors received, in packets. • **LCP echo req Tx**—Number of LCP echo requests transmitted, in packets. • **LCP echo req Rx**—Number of LCP echo requests received, in packets. • **LCP echo rep Tx**—Number of LCP echo responses transmitted, in packets. • **LCP echo rep Rx**—Number of LCP echo responses received, in packets. • **LCP echo Req timout**—Number of LCP echo requests that timed out. • **LCP echo Req error**—Number of errors received for LCP echo packets. • **LCP echo Rep error** —Number of errors transmitted for LCP echo packets.	**extensive**

Sample Output

show services l2tp session (LNS)

```
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 (LAC)

```
user@host> show services l2tp session
Tunnel local ID: 31889
  Local  Remote   State                Interface         Interface
  ID     ID                            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 (LNS)

```
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: On
    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
  LCP echo req Tx       657
  LCP echo req Rx         0
  LCP echo rep Tx         0
  LCP echo rep Rx       657
  LCP echo Req timout   0
  LCP echo Req error    0
  LCP echo Rep error    0
```

show services l2tp summary

Syntax show services l2tp summary
<interface sp-*fpc/pic/port*>

Release Information Command introduced before Junos OS Release 7.4.

Description (M10i and M7i routers only) Display Layer 2 Tunneling Protocol (L2TP) summary information for LNS.

(MX Series routers only) Display L2TP summary information for LAC and LNS.

Options **none**—(M10i and M7i routers only) Display complete L2TP summary information for all adaptive services interfaces.

(MX Series routers only) Display complete L2TP summary information for all inline services interfaces.

interface sp-*fpc/pic/port*—(Optional) Display L2TP summary information for only the specified adaptive services interface. This option is not available for L2TP on MX Series routers.

Required Privilege Level view

List of Sample Output
show services l2tp summary (LAC) on page 65
show services l2tp summary (LAC on MX Series routers) on page 65
show services l2tp summary (LNS on MX Series routers) on page 65
show services l2tp summary (LNS on M Series routers) on page 65

Output Fields Table 7 on page 63 lists the output fields for the **show services l2tp summary** command. Output fields are listed in the approximate order in which they appear.

Table 7: show services l2tp summary Output Fields

Field Name	Field Description
Failover within a preference level	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.
Weighted load balancing	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.
Tunnel authentication challenge	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 **Enabled** when a secret is configured in the tunnel profile or on the RADIUS server in the Tunnel-Password attribute [69]. The state is **Disabled** when the secret is not present. Not displayed for LNS on M Series routers.

Table 7: show services l2tp summary Output Fields *(continued)*

Field Name	Field Description
Calling number avp	When the state is **Enabled**, the LAC includes the value of the Calling Number AVP 22 in ICRQ packets sent to the LNS. When the state is **Disabled**, the attribute is not sent to the LNS. Not displayed for LNS on M Series routers.
Failover Protocol	When the state is enabled, the LAC operates in the default *failover-protocol-fall-back-to-silent-failover* manner. When the state is disabled, the **disable-failover-protocol** statement has been issued and the LAC operates only in silent failover mode. Not displayed for LNS on M Series routers.
Tunnel assignment id	Format of the tunnel name. Format of the tunnel name, based on RADIUS attributes returned from the AAA server: • **authentication-id**—Name consists of only Tunnel Assignment-Id [82]. This is the default value. • **client-server-id**—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.
Max Retransmissions for Established Tunnel	Maximum number of times control messages are retransmitted for established tunnels.
Max Retransmissions for Not Established Tunnel	Maximum number of times control messages are retransmitted for tunnels that are not established.
Tunnel Idle Timeout	Period that a tunnel can be inactive—that is, carrying no traffic—before it times out and is torn down.
Destruct Timeout	Period that the router attempts to maintain dynamic destinations, tunnels, and sessions after they have been destroyed.
Destinations	Number of L2TP destinations for the LAC. Not displayed for LNS on M Series routers.
Tunnels	Number of L2TP tunnels established on the router.
Sessions	Number of L2TP sessions established on the router.
Control	Count of L2TP control packets and bytes sent and received.
Data	Count of L2TP data packets and bytes sent and received.
Errors	Count of L2TP error packets and bytes sent and received.

Sample Output

show services l2tp summary (LAC)

```
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 advisory
  Tunnel assignment id format is assignment-id
  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
Destinations: 0, Tunnels: 0, Sessions: 0
            Tx packets    Rx packets  Memory (bytes)
  Control            0             0        40886272
  Data               0             0               0
  Errors             0             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 advisory
Destinations: 4, Tunnels: 19, Sessions: 65
            Tx packets    Rx packets  Memory (bytes)
  Control          288           168       103931904
  Data               0             0               0
  Errors             0             0
```

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 tunnel

Syntax

show services l2tp tunnel
<brief | detail | extensive | statistics>
<interface sp-*fpc/pic/port*>
<local-gateway *gateway-address*>
<local-gateway-name *gateway-name*>
<local-tunnel-id *tunnel-id*>
<peer-gateway *gateway-address*>
<peer-gateway-name *gateway-name*>
<tunnel-group *group-name*>

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M10i and M7i routers only) Display a list of active Layer 2 Tunneling Protocol (L2TP) tunnels for LNS.

(MX Series routers only) Display a list of active L2TP tunnels for LAC and LNS.

Options

none—Display standard information about all active L2TP tunnels.

brief | detail | extensive | statistics—(Default) Display the specified level of output. Use the statistics option to display L2TP tunnel statistics.

interface sp-*fpc/pic/port*—(Optional) Display L2TP tunnel information for only the specified adaptive services interface. This option is not available for L2TP on MX Series routers.

local-gateway *gateway-address*—(Optional) Display L2TP tunnel information for only the specified local gateway address.

local-gateway-name *gateway-name*—(Optional) Display L2TP tunnel information for only the specified local gateway name.

local-tunnel-id *tunnel-id*—(Optional) Display L2TP tunnel information for only the specified local tunnel identifier.

peer-gateway *gateway-address*—(Optional) Display L2TP tunnel information for only the specified peer gateway address.

peer-gateway-name *gateway-name*—(Optional) Display L2TP tunnel information for only the specified peer gateway name.

tunnel-group *group-name*—(Optional) Display L2TP tunnel information for only the specified tunnel group.

Required Privilege Level

view

List of Sample Output

show services l2tp tunnel (LAC) on page 68
show services l2tp tunnel detail (LAC) on page 68
show services l2tp tunnel extensive (LAC) on page 68
show services l2tp tunnel extensive (LNS on M Series Routers) on page 69

show services l2tp tunnel extensive (LNS on MX Series Routers) on page 69

Output Fields Table 8 on page 67 lists the output fields for the **show services l2tp tunnel** command. Output fields are listed in the approximate order in which they appear.

Table 8: show services l2tp tunnel Output Fields

Field Name	Field Description
Interface	(LNS only) Name of an adaptive services interface.
Tunnel group	(LNS only) Name of a tunnel group.
Local ID	On the LNS, number assigned by the LNS that identifies the local endpoint of the tunnel relative to the LNS: the LNS. On the LAC, number assigned by the LAC that identifies the local endpoint of the tunnel relative to the LAC: the LAC.
Remote ID	On the LNS, number assigned by the LAC that identifies the remote endpoint of the tunnel relative to the LNS: the LAC. On the LAC, number assigned by the LNS that identifies the remote endpoint of the tunnel relative to the LAC: the LNS.
Remote IP	IP address of the peer endpoint of the tunnel.
Sessions	Number of L2TP sessions established through the tunnel.
State	State of the L2TP tunnel: • **cc_responder_accept_new**—The tunnel has received and accepted the start control connection request (SCCRQ). • **cc_responder_reject_new**—The tunnel has received and rejected the SCCRQ. • **cc_responder_idle**—The tunnel has just been created. • **cc_responder_wait_ctl_conn**—The tunnel has sent the start control connection response (SCCRP) and is waiting for the start control connection connected (SCCCN) message. • **clean-up**—The tunnel is being cleaned up. • **closed**—The tunnel is being closed. • **destroyed**—The tunnel is being destroyed. • **Established**—The tunnel is operating. This is the only state supported for the LAC. • **Terminate**—The tunnel is terminating. • **Unknown**—The tunnel is not connected to the router.
Tunnel Name	(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].
Local IP	IP address of the local endpoint of the tunnel.
Local name	Name used for local tunnel endpoint during tunnel negotiation.
Remote name	Name used for remote tunnel endpoint during tunnel negotiation.

Table 8: show services l2tp tunnel Output Fields *(continued)*

Field Name	Field Description
Effective Peer Resync Mechanism	(LAC only) Peer resynchronization mechanism (PRM) in effect for the tunnel: • Failover protocol • Silent failover—Recovery takes place in the failed endpoint only using the proprietary silent failover protocol.
Max sessions	Maximum number of sessions that can be established on this tunnel.
Window size	Number of control messages that can be sent without receipt of an acknowledgment.
Hello interval	Interval between the transmission of hello messages, in seconds.
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 **Unknown** and the **Create time** value resets.
Up time	Amount of time elapsed since the tunnel became active, in hours, minutes, and seconds.
Idle time	Amount of time elapsed since the tunnel became idle, in hours, minutes, and seconds.
Statistics since	Date and time when collection of the following statistics began: • **Control Tx**—Amount of control information transmitted, in packets and bytes. • **Control Rx**—Amount of control information received, in packets and bytes. • **Data Tx**—Amount of data transmitted, in packets and bytes. • **Data Rx**—Amount of data received, in packets and bytes. • **Errors Tx**—Number of errors transmitted, in packets. • **Errors Rx**—Number of errors received, in packets.

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 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
    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 user

Syntax
show services l2tp user
<brief | detail | extensive | statistics>
<user *username*>

Release Information
Command introduced before Junos OS Release 7.4.

Description
(M10i and M7i routers only) Display a list of active Layer 2 Tunneling Protocol (L2TP) users.

Options
none—Display all active L2TP users.

brief | detail | extensive | statistics—(Optional) Display the specified level of output. Use the **statistics** option to display L2TP user statistics.

user *username*—(Optional) Display L2TP user information for only the specified username.

Required Privilege Level
view

List of Sample Output
show services l2tp user extensive on page 73

Output Fields
Table 9 on page 71 lists the output fields for the **show services l2tp user** command. Output fields are listed in the approximate order in which they appear.

Table 9: show services l2tp user Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Tunnel group	Name of a tunnel group.
Tunnel local ID	Local identifier of the tunnel, as assigned by the L2TP network server (LNS).
Session local ID	Local identifier of the session, as assigned by the L2TP network server (LNS).
Session remote ID	Remote identifier of the session, as assigned by the L2TP access concentrator (LAC).
State	State of the L2TP session: • **Established**—The session is operating. • **closed**—The session is being closed. • **destroyed**—The session is being destroyed. • **clean-up**—The session is being cleaned up. • **lns-ic-accept-new**—A new session is being accepted. • **lns-ic-idle**—The session has been created and is idle. • **lns-ic-reject-new**—The new session is being rejected. • **lns-ic-wait-connect**—The session is waiting for the peer's incoming call connected (ICCN) message.

Table 9: show services l2tp user Output Fields *(continued)*

Field Name	Field Description
Mode	Mode of the interface representing the session: **shared** or **exclusive**.
Local IP	IP address of the local endpoint of the tunnel.
Remote IP	IP address of the peer endpoint of the tunnel.
Username	Name of the user logged in to the session.
Assigned IP address	IP address assigned to remote client.
Local name	Name of the local device.
Remote name	Name of the remote device.
Local MRU	Maximum receive unit (MRU) setting of the local device, in bytes.
Remote MRU	MRU setting of the remote device, in bytes.
Tx speed	Transmit speed of the tunnel session, in bps.
Rx speed	Receive speed of the tunnel session, in bps.
Bearer type	Type of bearer enabled: • **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) • **1**—Digital access requested • **2**—Analog access requested • **4**—Asynchronous Transfer Mode (ATM) bearer support
Framing type	Type of framing enabled: • **1**—Synchronous framing • **2**—Asynchronous framing
LCP renegotiation	Whether Link Control Protocol (LCP) renegotiation is configured: **On** or **Off**.
Authentication	Type of authentication algorithm used: Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).
Interface ID	Name of the logical unit.
Interface unit	Logical unit number.
Call serial number	Unique serial number assigned to the call.
Create time	Date and time when the call was created.

Table 9: show services l2tp user Output Fields *(continued)*

Field Name	Field Description
Up time	Amount of time elapsed since the call became active, in hours, minutes, and seconds.
Idle time	Amount of time elapsed since the call became idle, in hours, minutes, and seconds.
Statistics sine	Date and time when collection of the following statistics began: • **Control Tx**—Amount of control information transmitted, in packets and bytes. • **Control Rx**—Amount of control information received, in packets and bytes. • **Data Tx**—Amount of data transmitted, in packets and bytes. • **Data Rx**—Amount of data received, in packets and bytes. • **Errors Tx**—Number of errors transmitted, in packets. • **Errors Rx**—Number of errors received, in packets.

Sample Output

show services l2tp user extensive

```
user@host> show services l2tp user extensive
Interface: sp-1/2/0, Tunnel group: group1, Tunnel local ID: 62746
  Session local ID: 56793, Session remote ID: 53304
    State: Established, 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 name: router-1, Remote name: router-2
    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
    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, Username: usr1@company_dns.com, Mode: shared
    Local IP: 10.128.11.1:1701, Remote IP: 10.128.11.2:1701
    Username: usr1@company_dns.com, Assigned IP address: 10.48.1.1/32
    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
    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
```

PART 4

Index

Index

M

N

P

R

S

T

W