

## Chapter 14

# Layer 2 Tunneling Protocol Services Configuration Guidelines

The Layer 2 Tunneling Protocol (L2TP) enables you to set up client services for establishing Point-to-Point Protocol (PPP) tunnels across a network and negotiate Multilink PPP if it is implemented. To configure L2TP services, you include the following statements at the [edit services l2tp] hierarchy level of the configuration:

```
[edit services]
l2tp {
  tunnel-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-number;
      }
    }
    tunnel-timeout seconds;
  }
  traceoptions {
    debug-level level;
    filter {
      protocol name;
    }
    flag flag;
    interfaces interface-name {
      debug-level level;
      flag flag;
    }
  }
}
```

You configure other components of this feature at the [edit access] and [edit interfaces] hierarchy levels. Those configurations are summarized in this chapter; for more information, see the *JUNOS System Basics Configuration Guide* or the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

This chapter contains the following sections:

L2TP Services Components on page 164

L2TP Minimum Configuration on page 165

Configuring L2TP Group Properties on page 167

Configuring the Logical Interface Identifier on page 172

Tracing Layer 2 Tunneling Protocol Operations on page 172

Example: Configuring L2TP Services on page 174

## L2TP Services Components

---

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 Physical Interface Card (AS 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 Remote Authentication Dial-In User Service (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 System Basics Configuration Guide*.

## 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.

```
[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.

```
[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.

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

```
[edit access]
group-profile westcoast_users {
  ppp {
    keepalive 0;
  }
}
profile westcoast_bldg_1_tunnel {
  client production {
    l2tp {
      interface-id test;
      shared-secret "$9$n8HX6A01RhivL1R"; # 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 Group Properties

---

This section describes the tasks for configuring L2TP tunnel group properties:

Configuring a Tunnel Group on page 167

Configuring Access Profiles on page 168

Configuring Addressing on page 168

Configuring Window Size on page 169

Configuring Timers on page 169

Hiding Attribute-Value Pairs on page 170

Configuring System Log Properties on page 170

### Configuring a Tunnel Group

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:

```

[edit services l2tp]
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-number;
    }
  }
  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 local gateway address or the service interface configuration, 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.

## Configuring Access Profiles

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 System Basics Configuration Guide*. A profile example is included in “Example: Configuring L2TP Services” on page 174.

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:

```
[edit services l2tp tunnel-group group-name]
l2tp-access-profile profile-name;
ppp-access-profile profile-name;
```

## Configuring Addressing

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:

```
[edit services l2tp tunnel-group group-name]
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:

```
[edit services l2tp tunnel-group group-name]
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.

## Configuring Window Size

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:

```
[edit services l2tp tunnel-group group-name]
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:

```
[edit services l2tp tunnel-group group-name]
maximum-send-window packets;
```

## Configuring Timers

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:

```
[edit services l2tp tunnel-group group-name]
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:

```
[edit services l2tp tunnel-group group-name]
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:

```
[edit services l2tp tunnel-group group-name]
tunnel-timeout seconds;
```

### **Hiding Attribute-Value Pairs**

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:

```
[edit services l2tp tunnel-group group-name]
hide-avps;
```

### **Configuring System Log Properties**

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:

```
[edit services l2tp tunnel-group group-name]
syslog {
  host hostname {
    services severity-level;
    facility-override facility-name;
    log-prefix prefix-number;
  }
}
```

Configure the host statement with a hostname 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 included in inet.O. You can specify only one system logging hostname.

Table 9 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 9: System Log Message Severity Levels**

Severity Level	Description
any	Includes all severity levels
emergency	System panic or other condition that causes the routing platform 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 NAT functionality, set the level to info.

For more information about system log messages, see the *JUNOS 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:

```
[edit services l2tp tunnel-group group-name syslog host hostname]
  facility-override facility-name;
```

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

To specify an address 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:

```
[edit services l2tp tunnel-group group-name syslog host hostname]
  log-prefix prefix-number;
```

## Configuring the Logical Interface Identifier

---

You can configure L2TP services on adaptive services interfaces on M7i 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 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.

---

## Tracing Layer 2 Tunneling Protocol 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`.

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

```
[edit services l2tp]
traceoptions {
  debug-level level;
  filter {
    protocol name;
  }
  flag flag;
  interfaces interface-name {
    debug-level level;
    flag flag;
  }
}
```

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, 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, 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 PIC interface. To configure, include the `interfaces interface-name` statement at the [edit services l2tp traceoptions] hierarchy level:

```
[edit services l2tp traceoptions]
interfaces interface-name {
  debug-level level;
  flag flag;
}
```

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.

## Example: Configuring L2TP Services

---

The following is a complete example of an L2TP configuration with multiple group and user profiles and a pool of logical interfaces for concurrent tunnel sessions:

```
[edit access]
address-pool customer_a {
    address 1.1.1.1/32;
}
address-pool customer_b {
    address-range low 2.2.2.1 high 2.2.3.2;
}
group-profile sunnyvale_users {
    ppp {
        framed-pool customer_a;
        idle-timeout 15;
        primary-dns 192.120.65.1;
        secondary-dns 192.120.65.2;
        primary-wins 192.120.65.3;
        secondary-wins 192.120.65.4;
        interface-id west;
    }
}
group-profile eastcoast_users {
    ppp {
        framed-pool customer_b;
        idle-timeout 20;
        primary-dns 192.120.65.5;
        secondary-dns 192.120.65.6;
        primary-wins 192.120.65.7;
        secondary-wins 192.120.65.8;
        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$3s2690leK8X7VKM7VwgaJn/Ctu1hclv87Ct87"; #
    SECRET-DATA
    ppp {
      idle-timeout 22;
      primary-dns 192.120.65.1;
      framed-ip-address 12.12.12.12/32;
      interface-id east;
    }
    group-profile sunnyvale_users;
  }
  client blue {
    chap-secret "$9$eq1KWxbwgZUHNdjmqmTF3uO1Rhr-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/t0BEleWFnRhrIXxbs2aJDHqf3nCP5";
      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 209.1.117.3;
    }
    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;
}
```