

## Chapter 29

# Configuring Access

To configure access, include the following statements at the [edit access] hierarchy level:

```
[edit access]
address-pool pool-name {
    address address-or-prefix;
    address-range low <lower-limit> high <upper-limit>;
}
group-profile profile-name {
    l2tp {
        interface-id interface-id;
        lcp-renegotiation;
        local-chap;
        maximum-sessions-per-tunnel number;
        multilink {
            drop-timeout milliseconds;
            fragmentation-threshold bytes;
        }
    }
}
ppp {
    framed-pool pool-id;
    idle-timeout seconds;
    interface-id interface-id;
    keepalive seconds;
    primary-dns primary-dns;
    primary-wins primary-win-server;
    secondary-dns secondary-dns;
    secondary-wins secondary-wins;
}
}
```

```

profile profile-name {
  authentication-order [ authentication-methods ];
  client client-name {
    chap-secret chap-secret;
    group-profile profile-name;
    l2tp {
      interface-id interface-id;
      lcp-renegotiation;
      local-chap;
      maximum-sessions-per-tunnel number;
      multilink {
        drop-timeout milliseconds;
        fragmentation-threshold bytes;
      }
      ppp-authentication (chap | pap);
      shared-secret shared-secret;
    }
    pap-password pap-password;
    ppp {
      framed-ip-address ip-address;
      framed-pool framed-pool;
      idle-timeout seconds;
      interface-id interface-id;
      keepalive seconds;
      primary-dns primary-dns;
      primary-wins primary-win-server;
      secondary-dns secondary-dns;
      secondary-wins secondary-wins;
    }
    user-group-profile profile-name;
  }
}
radius-disconnect {
  client-address {
    secret password;
  }
}
radius-disconnect-port port-number;
radius-server server-address {
  accounting-port port-number;
  port port-number;
  retry attempts;
  secret password;
  source-address source-address;
  timeout seconds;
}
traceoptions {
  flag all;
  flag authentication;
  flag chap;
  flag configuration;
  flag kernel;
  flag radius;
}

```

This chapter discusses the following topics:

Configuring the Point-to-Point Protocol on page 569

Tracing Access Processes on page 572

Configuring the Layer 2 Tunneling Protocol on page 573

## Configuring the Point-to-Point Protocol

---

To configure the Point-to-Point Protocol (PPP), do the following:

Configuring the Challenge Handshake Authentication Protocol on page 569

Configuring the Authentication Order on page 571

### **Configuring the Challenge Handshake Authentication Protocol**

The Challenge Handshake Authentication Protocol (CHAP) allows each end of a PPP link to authenticate its peer, as defined in RFC 1994. The authenticator sends its peer a randomly generated challenge that the peer must encrypt using a one-way hash; the peer must then respond with that encrypted result. The key to the hash is a secret known only to the authenticator and authenticated. When the response is received, the authenticator compares its calculated result with the peer's response. If they match, the peer is authenticated.

Each end of the link identifies itself to its peer by including its name in the CHAP challenge and response packets it sends to the peer. This name defaults to the local hostname, or you can explicitly set it using the `local-name` option. When a host receives a CHAP challenge or CHAP response packet on a particular interface, it uses the peer identity to look up the CHAP secret key to use. For more information about the `local-name` option, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

To configure CHAP, include the profile statement at the [edit access] hierarchy level:

```
[edit access]
profile profile-name {
  client client-name chap-secret chap-secret;
}
```

Then reference the CHAP profile name at the [edit interfaces] hierarchy level. For more information about how to reference CHAP, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

You can configure multiple profiles. You can also configure multiple clients for each profile.

profile is the mapping between peer identifiers and CHAP secret keys. The identity of the peer contained in the CHAP challenge or response queries the profile for the secret key to use.

client is the peer identity.

chap-secret secret is the secret key associated with that peer.

### Example: PPP Challenge Handshake Authentication Protocol

Configure the profile pe-A-ppp-clients at the [edit access] hierarchy level, then reference it at the [edit interfaces] hierarchy level:

```
[edit]
access {
  profile pe-A-ppp-clients {
    client cpe-1 chap-secret "$1$dQYsZ$B5ojUeUjDsUo.yKwcCZ0";
    # SECRET-DATA
    client cpe-2 chap-secret "$1$kdAsfaDAfkDjDsASxfafdKdFKJ";
    # SECRET-DATA
  }
}
interfaces {
  so-1/1/1 {
    encapsulation ppp;
    ppp-options {
      chap {
        access-profile pe-A-ppp-clients;
        local-name "pe-A-so-1/1/1";
      }
    }
  }
  so-1/1/2 {
    encapsulation ppp;
    ppp-options {
      chap {
        passive;
        access-profile pe-A-ppp-clients;
        local-name "pe-A-so-1/1/2";
      }
    }
  }
}
```

## Configuring the Authentication Order

You can configure the order in which the JUNOS software tries different authentication methods when authenticating peers. For each access attempt, the software tries the authentication methods in order, from first to last.

To configure the authentication order, include the authentication-order statement at the [edit access profile *name*] hierarchy level:

```
[edit access profile profile-name
 authentication-order [ authentication-methods ];
```

In *authentication-methods*, specify one or more of the following in the preferred order, from first tried to last tried:

radius—Verify the client using RADIUS authentication services.

password—Verify the client using the information configured at the [edit access profile *profile-name* client *client-name*] hierarchy level.

If you do not include the authentication-order statement, clients are verified by means of password authentication.

The CHAP authentication sequence cannot take more than 30 seconds. If it takes longer to authenticate a client, the authentication is abandoned and a new sequence is initiated.

For example, if you configure three RADIUS servers so that the router attempts to contact each server three times, and with each retry the server times out after 3 seconds, then the maximum time given to the RADIUS authentication method before CHAP considers it a failure is 27 seconds. If you add more RADIUS servers to this configuration, they might not be contacted because the authentication process might be abandoned before these servers are tried.

The JUNOS software enforces a limit to the number of standing authentication server requests that the CHAP authentication can have at one time. Thus, an authentication server method—RADIUS, for example—may fail to authenticate a client when this limit is exceeded. In the above example, any authentication method following this method is tried. If it fails, the authentication sequence is reinitiated by the router until authentication succeeds and the link is brought up.

RADIUS authentication servers are configured at the [edit system radius-server] hierarchy level. For more information about configuring RADIUS authentication servers, see “Configuring RADIUS Authentication” on page 360.

## Tracing Access Processes

---

To trace access processes, you can specify options in the `traceoptions` statement at the `[edit access]` hierarchy level:

```
[edit access]
traceoptions {
  flag all;
  flag authentication;
  flag chap;
  flag configuration;
  flag radius;
}
```

You can specify the following access tracing flags:

- `all`—All tracing operations
- `authentication`—All authentication module handling
- `chap`—All CHAP messages and handling
- `configuration`—Reading of configuration
- `radius`—All RADIUS messages and handling

## Configuring the Layer 2 Tunneling Protocol

For M7i routers, you can configure Layer 2 Tunneling Protocol (L2TP) tunneling security services on an Adaptive Services Physical Interface Card (PIC). The L2TP protocol allows the PPP to be tunneled within a network.



**NOTE:** For information about how to configure L2TP service, see the *JUNOS Services Interfaces Configuration Guide* and the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

To configure L2TP, include the following statements at the [edit access] hierarchy level:

```
[edit access]
address-pool pool-name {
    address address-or-prefix;
    address-range low <lower-limit> high <upper-limit>;
}
group-profile profile-name {
    l2tp {
        interface-id interface-id;
        lcp-renegotiation;
        local-chap;
        maximum-sessions-per-tunnel number;
    }
    ppp {
        framed-pool pool-id;
        idle-timeout seconds;
        interface-id interface-id;
        keepalive seconds;
        primary-dns primary-dns;
        primary-wins primary-win-server;
        secondary-dns secondary-dns;
        secondary-wins secondary-wins;
    }
}
profile profile-name {
    authentication-order [ authentication-methods ];
    client client-name {
        chap-secret chap-secret;
        group-profile profile-name;
        l2tp {
            interface-id interface-id;
            lcp-renegotiation;
            local-chap;
            maximum-sessions-per-tunnel number;
            ppp-authentication (chap | pap);
            shared-secret shared-secret;
        }
    }
    pap-password pap-password;
    ppp {
        framed-ip-address ip-address;
        framed-pool framed-pool;
        idle-timeout seconds;
        interface-id interface-id;
        keepalive seconds;
```

```

        primary-dns primary-dns;
        primary-wins primary-win-server;
        secondary-dns secondary-dns;
        secondary-wins secondary-wins;
    }
    user-group-profile profile-name;
}
radius-disconnect-port port-number {
    radius-disconnect {
        client-address {
            secret password;
        }
    }
}
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    secret password;
    source-address source-address;
    timeout seconds;
}

```

This section includes the following topics:

Minimum L2TP Configuration on page 575

Configuring the Address Pool on page 576

Configuring the Group Profile on page 577

Configuring the Profile on page 580

Example: Configuring L2TP on page 591

Configuring RADIUS Authentication for L2TP on page 593

Configuring the RADIUS Disconnect Server for L2TP on page 595

## Minimum L2TP Configuration

To define L2TP, include at least the following statements at the [edit access] hierarchy level:

```
[edit access]
address-pool pool-name {
    address address-or-prefix;
    address-range low <lower-limit> high <upper-limit>;
}
profile profile-name {
    authentication-order [ authentication-methods ];
    client client-name {
        chap-secret chap-secret;
        l2tp {
            interface-id interface-id;
            maximum-sessions-per-tunnel number;
            ppp-authentication (chap | pap);
            shared-secret shared-secret;
        }
        pap-password pap-password;
        ppp {
            framed-ip-address ip-address;
            framed-pool framed-pool;
            interface-id interface-id;
            primary-dns primary-dns;
            primary-wins primary-win-server;
            secondary-dns secondary-dns;
            secondary-wins secondary-wins;
        }
    }
}
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    secret password;
}
```

## Configuring the Address Pool

With an address pool, you configure an address or address range. When you define an address pool for a client, the L2TP network server (LNS) allocates IP addresses for clients from an address pool. If you do not want to use an address pool, you can specify an IP address by means of the `framed-ip-address` statement at the `[edit access profile profile-name client client-name ppp]` hierarchy level. For information about specifying an IP address, see “Configuring the PPP Properties for a Profile” on page 588.



**NOTE:** When an address pool is modified or deleted, all the sessions using that pool are deleted.

---

To define an address or a range of addresses, include the `address-pool` statement at the `[edit access]` hierarchy level:

```
[edit access]
address-pool pool-name;
```

*pool-name* is the name assigned to the address pool.

To configure an address, include the `address` statement at the `[edit access address-pool pool-name]` hierarchy level:

```
[edit access address-pool pool-name]
address address-or-prefix;
```

*address-or-prefix* is one address or a prefix value.

When you specify an address range, it cannot exceed 65,535 IP addresses. To configure the address range, include the `address-range` statement at the `[edit access address-pool pool-name]` hierarchy level:

```
[edit access address-pool pool-name]
address-range <low lower-limit> <high upper-limit>;
```

*low lower-limit*—The lower limit of an address range.

*high upper-limit*—The upper limit of an address range.

## Configuring the Group Profile

You can optionally configure the group profile to define the PPP or L2TP attributes. Any client referencing the configured group profile inherits all the group profile attributes.



**NOTE:** The group-profile statement overrides the user-group-profile statement, which is configured at the [edit access profile *profile-name*] hierarchy level. The profile statement overrides the attributes configured at the [edit access group-profile *profile-name*] hierarchy level. For information about the user-group-profile statement, see “Applying a Configured PPP Group Profile to a Tunnel” on page 589.

To configure the group profile, include the group-profile statement at the [edit access] hierarchy level:

```
[edit access]
group-profile profile-name;
```

*profile-name* is the name assigned to the group profile.

To configure the L2TP properties for a group profile, include the following statements at the [edit access group-profile *profile-name*] hierarchy level:

```
[edit access group-profile profile-name]
l2tp {
  interface-id interface-id;
  lcp-renegotiation;
  local-chap;
  maximum-sessions-per-tunnel number;
}
```

To configure the PPP properties for a group profile, include the following statements at the [edit access group-profile *profile-name*] hierarchy level:

```
[edit access group-profile profile-name]
ppp {
  framed-pool pool-id;
  idle-timeout seconds;
  interface-id interface-id;
  keepalive seconds;
  primary-dns primary-dns;
  primary-wins primary-win-server;
  secondary-dns secondary-dns;
  secondary-wins secondary-wins;
}
```

This section describes how to configure the group profile:

Configuring L2TP for a Group Profile on page 578

Configuring the PPP Attributes for a Group Profile on page 578

Example: Group Profile Configuration on page 579

### Configuring L2TP for a Group Profile

To configure the L2TP for the group profile, include the following statements at the [edit access group-profile *profile-name* l2tp] hierarchy level:

```
[edit access group-profile profile-name l2tp]
interface-id interface-id;
lcp-renegotiation;
local-chap;
maximum-sessions-per-tunnel number;
```

*interface-id* is the identifier for the interface representing an L2TP session configured at the [edit interfaces *interface-name* unit *local-unit-number* dial-options] hierarchy level. For more information about the interface ID, see the *JUNOS Services Interfaces Configuration Guide*.

You can configure the LNS so that it renegotiates the link control protocol (LCP) with the PPP client (in the renegotiation statement). By default, the PPP client negotiates the LCP with the L2TP access concentrator (LAC). When you do this, the LNS discards the last sent and the last received LCP configuration request attribute value pairs (AVPs) from the LAC; for example, the LCP negotiated between the PPP client and the LAC.

You can configure the JUNOS software so that the LNS ignores proxy authentication AVPs from the LAC and reauthenticates the PPP client using a CHAP challenge (in the local-chap statement). When you do this, the LNS directly authenticates the PPP client. By default, the PPP client is not reauthenticated by the LNS.

*number* is the maximum number of sessions per L2TP tunnel.

### Configuring the PPP Attributes for a Group Profile

To configure the PPP attributes for a group profile, include the following statements at the [edit access group-profile *profile-name* ppp] hierarchy level:

```
[edit access group-profile profile-name ppp]
framed-pool pool-id;
idle-timeout seconds;
interface-id interface-id;
keepalive seconds;
primary-dns primary-dns;
primary-wins primary-win-server;
secondary-dns secondary-dns;
secondary-wins secondary-wins;
```

*pool-id* (in the framed-pool statement) is the name assigned to the address pool.

*seconds* (in the idle-timeout statement) is the number of seconds a user can remain idle before the session is terminated. By default, idle timeout is set to "0". You can configure this to be a value in the range from 0 through 4,294,967,295.

*interface-id* (in the interface-id statement) is the identifier for the interface representing an L2TP session configured at the [edit interfaces *interface-name* unit *local-unit-number* dial-options] hierarchy level. For more information about the interface ID, see the *JUNOS Services Interfaces Configuration Guide*.

*seconds* (in the *keepalive* statement) is the time period that must elapse before the JUNOS software checks the status of the PPP session by sending an echo request to the peer. For each session, JUNOS software sends out three keepalives at 10-second intervals and the session is close if there is no response. By default, the time to send a keepalive messages is set to 10 seconds. You configure this to be a value in the range from 0 through 32,767.

*primary-dns* (in the *primary-dns* statement) is an IP version 4 (IPv4) address.

*secondary-dns* (in the *secondary-dns* statement) is an IPv4 address.

*primary-win-server* (in the *primary-wins* statement) is an IPv4 address.

*secondary-wins* (in the *secondary-wins* statement) is an IPv4 address.

### Example: Group Profile Configuration

Configure an L2TP and PPP group profile:

```
[edit access]
group-profile westcoast_users {
  ppp {
    framed-pool customer_a;
    keepalive 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;
    keepalive 15;
    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 westcoast_tunnel {
  l2tp {
    maximum-sessions-per-tunnel 100;
  }
}
group-profile east_tunnel {
  l2tp {
    maximum-sessions-per-tunnel 125;
  }
}
}
```

## Configuring the Profile

You can configure multiple profiles. You can also configure multiple clients for each profile. To configure the profile, include the profile statement at the [edit access] hierarchy level:

```
[edit access]
profile profile-name;
```

*profile-name* is the name assigned to the profile.



**NOTE:** The group-profile statement overrides the user-group-profile statement, which is configured at the [edit access profile *profile-name*] hierarchy level. The profile statement overrides the attributes configured at the [edit access group-profile *profile-name*] hierarchy level. For information about the user-group-profile statement, see “Applying a Configured PPP Group Profile to a Tunnel” on page 589.

When you configure a profile, you can only configure L2TP or PPP parameters. You cannot configure both.

---

To configure the L2TP properties for a profile, include the following statements at the [edit access profile *profile-name*] hierarchy level:

```
[edit access profile profile-name]
authentication-order [ authentication-methods ];
client client-name {
  group-profile profile-name;
  l2tp {
    interface-id interface-id;
    lcp-renegotiation;
    local-chap;
    maximum-sessions-per-tunnel number;
    ppp-authentication (chap | pap);
    shared-secret shared-secret;
  }
}
user-group-profile profile-name;
```

To configure the PPP properties for a profile, include the following statements at the [edit access profile *profile-name*] hierarchy level:

```
[edit access profile profile-name]
authentication-order [ authentication-methods ];
client client-name {
  chap-secret chap-secret;
  group-profile profile-name;
  pap-password pap-password;
  ppp {
    framed-ip-address ip-address;
    framed-pool framed-pool;
    idle-timeout seconds;
    interface-id interface-id;
    keepalive seconds;
    primary-dns primary-dns;
    primary-wins primary-win-server;
    secondary-dns secondary-dns;
    secondary-wins secondary-wins;
  }
}
```



**NOTE:** When you configure PPP properties for a profile, you typically configure the chap-secret statement or pap-password statement.

---

To configure the profile, do the following:

Configuring the Authentication Order on page 581

Configuring the Client on page 582

### Configuring the Authentication Order

You can configure the order in which the JUNOS software tries different authentication methods when authenticating peers. For each access attempt, the software tries the authentication methods in order, from first to last.

To configure the authentication order, include the authentication-order statement at the [edit access profile *profile-name*] hierarchy level:

```
[edit access profile profile-name]
authentication-order [ authentication-methods ];
```

In *authentication-methods*, specify one or more of the following in the preferred order, from first tried to last tried:

radius—Verify the client using RADIUS authentication services.

password—Verify the client using the information configured at the [edit access profile *profile-name* client *client-name*] hierarchy level.



**NOTE:** When you configure the authentication methods for L2TP, only the first configured authentication method is used.

For L2TP, RADIUS authentication servers are configured at the [edit access radius-server] hierarchy level. For more information about configuring RADIUS authentication servers, see “Configuring RADIUS Authentication for L2TP” on page 593.

If you do not include the authentication-order statement, clients are verified by means of password authentication.

### Configuring the Client

To configure the client, include the client statement at the [edit access profile *profile-name*] hierarchy level:

```
[edit access profile profile-name]  
client client-name;
```

*client-name* is the peer identity.

For L2TP, you can optionally use the wildcard (\*) to define a default tunnel client to authenticate multiple LACs with the same secret and L2TP attributes. If an LAC with a specific name is not defined in the configuration, the wildcard tunnel client authenticates it.

This section includes the following topics:

Example: Applying a User Group Profile on page 589

Example: Configuring the Profile on page 590

#### **Example: Defining the Default Tunnel Client**

Use the wildcard (\*) to define a default tunnel client to authenticate multiple LACs with the same secret:

```
[edit access profile profile-name]  
client * {  
  l2tp {  
    interface-id interface1;  
    lcp-renegotiation;  
    local-chap;  
    maximum-sessions-per-tunnel 500;  
    ppp-authentication chap;  
    shared-secret "$1$dQYsZ$B5ojUeUjDsUo.yKwcCZ0";  
  }  
}
```

For any tunnel client, you can optionally use the user group profile to define default PPP attributes for all users coming in through a tunnel. The user group profile must define PPP attributes. If the user group profile is specified, all users (PPP sessions) use the PPP attributes specified in the user group profile. The PPP attributes specified in the local or RADIUS server take precedence over those specified in the user group profile.

You can optionally use a wildcard client to define a user group profile. When you do this, any client entering this tunnel uses the PPP attributes (defined user group profile attributes) as its default PPP attributes.

**Example: Defining the User Group Profile**

Use a wildcard client to define a user group profile:

```
[edit access profile profile]
client * {
    user-group-profile user-group-profile1;
}
```

For information about how to configure the user group profile, see “Applying a Configured PPP Group Profile to a Tunnel” on page 589.

This section includes the following topics:

Configuring the CHAP Secret on page 584

Example: Configuring PPP CHAP on page 585

Referencing the Group Profile on page 585

Configuring L2TP Properties for a Profile on page 585

Example: PPP MP for L2TP on page 587

Configuring the Password Authentication Protocol Password on page 587

Example: PAP on page 587

Configuring the PPP Properties for a Profile on page 588

Applying a Configured PPP Group Profile to a Tunnel on page 589

Example: Applying a User Group Profile on page 589

Example: Configuring the Profile on page 590

### Configuring the CHAP Secret

CHAP allows each end of a PPP link to authenticate its peer, as defined in RFC 1994. The authenticator sends its peer a randomly generated challenge that the peer must encrypt using a one-way hash; the peer must then respond with that encrypted result. The key to the hash is a secret known only to the authenticator and authenticated. When the response is received, the authenticator compares its calculated result with the peer's response. If they match, the peer is authenticated.

Each end of the link identifies itself to its peer by including its name in the CHAP challenge and response packets it sends to the peer. This name defaults to the local hostname, or you can explicitly set it using the local-name option. When a host receives a CHAP challenge or CHAP response packet on a particular interface, it uses the peer identity to look up the CHAP secret key to use. For more information about the local-name option, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.



**NOTE:** When you configure PPP properties for a profile, you typically configure the chap-secret statement or pap-password statement.

---

To configure CHAP, include the profile statement and specify a profile name at the [edit access] hierarchy level:

```
[edit access]
profile profile-name {
    client client-name chap-secret data;
}
```

Then reference the CHAP profile name at the [edit interfaces *interface-name* ppp-options chap] hierarchy level. For more information about how to reference CHAP, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

You can configure multiple profiles. You can also configure multiple clients for each profile.

profile is the mapping between peer identifiers and CHAP secret keys. The identity of the peer contained in the CHAP challenge or response queries the profile for the secret key to use.

client is the peer identity.

chap-secret secret is the secret key associated with that peer.

**Example: Configuring PPP CHAP**

Configure the profile `profile westcoast_bldg1` at the `[edit access]` hierarchy level, then reference it at the `[edit interfaces]` hierarchy level:

```
[edit]
access {
  profile westcoast_bldg1 {
    client cpe-1 chap-secret "$1$dQYsZ$B5ojUeUjDsUo.yKwcCZ0";
    # SECRET-DATA
    client cpe-2 chap-secret "$1$kdAsfaDAfkdjDsASxfafdKdFKJ";
    # SECRET-DATA
  }
}
```

**Referencing the Group Profile**

You can reference a configured group profile from the L2TP tunnel profile.

To reference the group profile configured at the `[edit access group-profile profile-name]` hierarchy level, include the `group-profile` statement at the `[edit access profile profile-name client client-name]` hierarchy level:

```
[edit access profile profile-name client client-name]
group-profile profile-name;
```

*profile-name* references a configured group profile from a PPP user profile.

**Configuring L2TP Properties for a Profile**

To define L2TP properties for a profile, include one or more of the following statements at the `[edit access profile profile-name client client-name l2tp]` hierarchy level:



**NOTE:** When you configure the profile, you can only configure L2TP or PPP parameters. You cannot configure both.

---

```
[edit access profile profile-name client client-name l2tp]
interface-id interface-id;
lcp-renegotiation;
local-chap;
maximum-sessions-per-tunnel number;
multilink {
  drop-timeout milliseconds;
  fragmentation-threshold bytes;
}
ppp-authentication (chap | pap);
shared-secret shared-secret;
```

*interface-id* (in the `interface-id` statement) is the identifier for the interface representing an L2TP session configured at the `[edit interfaces interface-name unit local-unit-number dial-options]` hierarchy level. For more information about the interface ID, see the *JUNOS Services Interfaces Configuration Guide*.

*number* (in the `maximum-sessions-per-tunnel` statement) is the maximum number of sessions for an L2TP tunnel.

*shared-secret* (in the *shared-secret* statement) is the shared secret for authenticating the peer.

You can specify PPP authentication (in the *ppp-authentication* statement). By default, the PPP authentication uses CHAP. You can configure this to use Password Authentication Protocol (PAP).

You can configure LNS so it renegotiates LCP with the PPP client (in the *lcp-negotiation* statement). By default, the PPP client negotiates the LCP with the LAC. When you do this, the LNS discards the last sent LCP configuration request and last received LCP configuration request AVPs from the LAC; for example, the LCP negotiated between the PPP client and LAC.

You can configure the JUNOS software so that the LNS ignores proxy authentication AVPs from the LAC and reauthenticates the PPP client using a CHAP challenge (in the *local-chap* statement). By default, the PPP client is not reauthenticated by the LNS. When you do this, the LNS directly authenticates the PPP client.

You can configure the PPP MP for L2TP if the PPP sessions that are coming into the LNS from the LAC have multilink PPP negotiated. When you do this, you join multilink bundles based on the endpoint discriminator (in the *multilink* statement).

*milliseconds* (in the *drop-timeout* statement) specifies the number of milliseconds for the timeout that associated with the first fragment on the reassembly queue. If the timeout expires before all the fragments have been collected, the fragments at the beginning of the reassembly queue are dropped. If the drop timeout is not specified, the JUNOS software holds on to the fragments (fragments may still be dropped if the multilink reassembly algorithm determines that another fragment belonging to the packet on a reassembly queue has been lost).



**NOTE:** The drop timeout and fragmentation threshold for a bundled multilink might belong to different tunnels. The different tunnels might have different drop timeout and fragmentation thresholds. We recommend configuring group profiles instead of profiles when you have L2TP tunnels.

---

*bytes* specifies the maximum size of a packet, in bytes (in the *fragmentation-threshold* statement). If a packet exceeds the fragmentation threshold, the JUNOS software fragments it into two or more multilink fragments.

**Example: PPP MP for L2TP**

Join multilink bundles based on the endpoint discriminator:

```
[edit access]
profile tunnel-profile {
  client remote-host {
    l2tp {
      multilink {
        drop-timeout 600;
        fragmentation-threshold 100;
      }
    }
  }
}
```

**Configuring the Password Authentication Protocol Password**

When you configure PPP properties for a profile, you typically configure the `chap-secret` statement or `pap-password` statement. For information about how to configure the CHAP secret, see “Configuring the CHAP Secret” on page 584

To configure the PAP password, include the `pap-password` statement at the `[edit access profile profile-name client client-name]` hierarchy level:

```
[edit access profile profile-name client client-name]
pap-password pap-password;
```

*pap-password* is the password for the PAP authentication protocol.

**Example: PAP**

```
[edit access]
profile sunnyvale_bldg_2 {
  client green {
    pap-password "$9$24gGiPz6CuQFu1EyW8VwYgZUik.5z3";
    ppp {
      interface-id west;
    }
    group-profile sunnyvale_users;
  }
  client red {
    chap-secret "$9$24gGiPz6CuQFu1EyW8VwYgZUik.5z3";
    group-profile sunnyvale_users;
  }
  authentication-order radius;
}
profile Sunnyvale_bldg_1_tunnel {
  client test {
    l2tp {
      shared-secret "$9$24gGiPz6CuQFu1EyW8VwYgZUik.5z3";
      ppp-authentication pap;
    }
  }
}
```

### Configuring the PPP Properties for a Profile

To define PPP properties for a profile, include one or more of the following statements at the [edit access profile *profile-name* client *client-name* ppp] hierarchy level. The properties defined in the profile take precedence over the values defined in the group profile.

```
[edit access profile profile-name client client-name ppp]
framed-ip-address ip-address;
framed-pool pool-id;
idle-timeout seconds;
interface-id interface-id;
keepalive seconds;
primary-dns primary-dns;
primary-wins primary-win-server;
secondary-dns secondary-dns;
secondary-wins secondary-wins;
```



**NOTE:** When you configure a profile, you can only configure L2TP or PPP parameters. You cannot configure both.

---

*ip-address* (in the framed-ip-address statement) is the IPv4 prefix.

*pool-id* (in the framed-pool statement) is a configured address pool.

*seconds* (in the idle-timeout statement) is the number of seconds a user can remain idle before the session is terminated. By default, idle timeout is set to “0”. You can configure this to be a value in the range from 0 through 4,294,967,295.

*interface-id* (in the interface-id statement) is the identifier for the interface representing an L2TP session configured at the [edit interfaces *interface-name* unit *local-unit-number* dial-options] hierarchy level. For more information about the interface ID, see the *JUNOS Services Interfaces Configuration Guide*.

*seconds* (in the keepalive statement) is the time period that must elapse before the JUNOS software checks the status of the PPP session by sending an echo request to the peer. For each session, JUNOS software sends out three keepalives at 10-second intervals and the session is closed if there is no response. By default, the time to send a keepalive messages is set to 10 seconds. You configure this to be a value in the range from 0 through 32,767.

*primary-dns* (in the primary-dns statement) is an IPv4 address.

*secondary-dns* (in the secondary-dns statement) is an IPv4 address.

*primary-wins* (in the primary-wins statement) is an IPv4 address.

*secondary-wins* (in the secondary-wins statement) is an IPv4 address.

**Applying a Configured PPP Group Profile to a Tunnel**

You can optionally apply a configured PPP group profile to a tunnel. For any tunnel client, you can use the `user-group-profile` statement to define default PPP attributes for all users coming in through a tunnel. The user group profile must define PPP attributes. If the user group profile is specified, all users (PPP sessions) use the PPP attributes specified in the user group profile.

When a PPP client enters a tunnel, the JUNOS software first applies the PPP user group profile attributes and then any PPP attributes from the local or RADIUS server. The PPP attributes defined in the RADIUS or local server take precedence over the attributes defined in the user group profile.

To apply configured PPP attributes to a PPP client, include the `user-group-profile` statement at the `[edit access profile profile-name client client-name]` hierarchy level:

```
[edit access profile profile-name client client-name]
  user-group-profile profile-name;
```

*profile-name* is a PPP group profile configured at the `[edit access group-profile profile-name]` hierarchy level. When a client enters this tunnel, it uses the `user-group-profile` attributes as the default attributes.

**Example: Applying a User Group Profile**

Apply a configured PPP group profile to a tunnel:

```
[edit access]
  group-profile westcoast_users {
    ppp {
      idle-timeout 100;
    }
  }
  group-profile westcoast_default_configuration {
    ppp {
      framed-pool customer_b;
      idle-timeout 20;
      interface-id west;
      primary-dns 192.120.65.5;
      secondary-dns 192.120.65.6;
      primary-wins 192.120.65.7;
      secondary-wins 192.120.65.8;
    }
  }
  profile westcoast_bldg_1_tunnel {
    client test {
      l2tp {
        interface-id west;
        shared-secret "$9$r3HKvLg4ZUDkX7JGjif5p0BIRS8LN";
        # SECRET-DATA
        maximum-sessions-per-tunnel 75;
        ppp-authentication chap;
      }
      user-group-profile westcoast_default_configuration; # Apply default PPP
    } # attributes for users coming through a tunnel
  }
```

```

profile westcoast_bldg_1 {
  client white {
    chap-secret "$9$3s2690leK8X7VKM7VwgaJn/Ctu1hclv87Ct87";
    # SECRET-DATA
    ppp {
      idle-timeout 22;
      primary-dns 192.120.65.9;
      framed-ip-address 12.12.12.12/32;
    }
    group-profile westcoast_users; # Reference the west_users group
  }
  # profile
}

```

### **Example: Configuring the Profile**

Configure the profile:

```

[edit access]
profile westcoast_bldg_1 {
  client white {
    chap-secret "$9$3s2690leK8X7VKM7VwgaJn/Ctu1hclv87Ct87";
    # SECRET-DATA
    ppp {
      idle-timeout 22;
      primary-dns 192.120.65.10;
      framed-ip-address 12.12.12.12/32;
    }
    group-profile westcoast_users;
  }
  client blue {
    chap-secret "$9$eq1KWxbwgZUHNdjmqmTF3uO1Rhr-dsoJDNd";
    # SECRET-DATA
    group-profile sunnyvale_users;
  }
  authentication-order password;
}
profile westcoast_bldg_1_tunnel {
  client test {
    l2tp {
      shared-secret "$9$r3HKvLg4ZUDkX7JGjif5p0BIRS8LN";
      # SECRET-DATA
      maximum-sessions-per-tunnel 75;
      ppp-authentication chap;
    }
    group-profile westcoast_tunnel;
  }
  client production {
    l2tp {
      shared-secret "$9$R2QErV8X-goGylVwg4jITz36/tOBEleWFnRh
rIXbs2aJDHqf3nCP5";
      # SECRET-DATA
      ppp-authentication chap;
    }
    group-profile westcoast_tunnel;
  }
}
}

```

**Example: Configuring L2TP**

Configure L2TP:

```

[edit]
access {
  address-pool customer_a {
    address 1.1.1.1/32;
  }
  address-pool customer_b {
    address-range low 2.2.2.2 high 2.2.3.2;
  }
  group-profile westcoast_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 westcoast_tunnel {
    l2tp {
      maximum-sessions-per-tunnel 100;
    }
  }
  group-profile east_tunnel {
    l2tp {
      maximum-sessions-per-tunnel 125;
    }
  }
  profile westcoast_bldg_1 {
    client white {
      chap-secret "$9$3s2690leK8X7VKM7VwgaJn/Ctu1hclv87Ct87";
      # SECRET-DATA
    }
    ppp {
      idle-timeout 22;
      primary-dns 192.120.65.10;
      framed-ip-address 12.12.12.12/32;
    }
    group-profile westcoast_users;
  }
}

```

```

client blue {
  chap-secret "$9$eq1KWxbwgZUHNdjqmTF3uO1Rhr-dsoJDNd";
  # SECRET-DATA
  group-profile sunnyvale_users;
}
authentication-order password;
}
profile west-coast_bldg_2 {
  client red {
    pap-password "$9$3s2690IeK8X7VKM8888Ctu1hclv87Ct87";
    # SECRET-DATA
    ppp {
      idle-timeout 22;
      primary-dns 192.120.65.11;
      framed-ip-address 12.12.12.12/32;
    }
    group-profile westcoast_users;
  }
}
profile westcoast_bldg_1_tunnel {
  client test {
    l2tp {
      shared-secret "$9$r3HKvLg4ZUDkX7JGjif5pOBIRS8LN";
      # SECRET-DATA
      maximum-sessions-per-tunnel 75;
      ppp-authentication chap;      #The default for PPP authentication
      # is CHAP
    }
    group-profile westcoast_tunnel;
  }
  client production {
    l2tp {
      shared-secret "$9$R2QErV8X-goGylVwg4jiTz36/t0BEIeWFnRh
        rIXxbs2aJDHqf3nCP5"; # SECRET-DATA
      ppp-authentication chap;
    }
    group-profile westcoast_tunnel;
  }
}
profile westcoast_bldg_2_tunnel {
  client black {
    l2tp {
      shared-secret "$9$R2QErV8X-goGylVwg4jiTz36/t0BEIeWFnRh
        rIXxbs2aJDHqf3nCP5";
      # SECRET-DATA
      ppp-authentication pap;
    }
    group-profile westcoast_tunnel;
  }
}
}
}

```

## Configuring RADIUS Authentication for L2TP

The LNS sends RADIUS authentication requests or accounting requests. Authentication requests are sent out to the authentication server port. Accounting requests are sent to the accounting port. To configure the RADIUS authentication for L2TP on an M7i routing platform, include following statements at the [edit access] hierarchy level:

```
[edit access]
radius-server server-address {
  accounting-port port-number;
  port port-number;
  retry attempts;
  secret password;
  source-address source-address;
  timeout seconds;
}
```



**NOTE:** The RADIUS servers at the [edit access] hierarchy level are not used by the network access server process (NASD).

---

You can specify an accounting port number on which to contact the accounting server (in the accounting-port statement). Most RADIUS servers use port number 1813 (as specified in RFC 2866, *Radius Accounting*).

*server-address* specifies the address of the RADIUS authentication server (in the radius-server statement).

You can specify a port number on which to contact the RADIUS authentication server (in the port statement). Most RADIUS servers use port number 1812 (as specified in RFC 2138, *Remote Authentication Dial In User Service (RADIUS)* ).

You must specify a password in the secret statement. Passwords can contain spaces. The secret used by the local router must match that used by the RADIUS authentication server.

Optionally, you can specify the amount of time that the local router waits to receive a response from a RADIUS server (in the timeout statement) and the number of times that the router attempts to contact a RADIUS authentication server (in the retry statement). By default, the router waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds. By default, the router retries connecting to the server three times. You can configure this to be a value in the range from 1 through 10 times.

In the source-address statement, specify a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. The source address is a valid IPv4 address configured on one of the router interfaces.

To configure multiple RADIUS servers, include multiple radius-server statements. For information about how to configure the RADIUS disconnect server for L2TP, see “Configuring the RADIUS Disconnect Server for L2TP” on page 595.

**Example: RADIUS Authentication**

```

[edit access]
profile sunnyvale_bldg_2 {
  client green {
    chap-secret "$9$24gGiPzf6CuQFu1EyW8VwYgZUik.5z3";
    ppp {
      interface-id west;
    }
    group-profile sunnyvale_users;
  }
  client red {
    chap-secret "$9$24gGiPzf6CuQFu1EyW8VwYgZUik.5z3";
    group-profile sunnyvale_users;
  }
  authentication-order radius;
}
radius-server {
  192.168.65.213 {
    port 1812;
    accounting-port 1813;
    secret "$9$24gGiPzf6CuQFu1EyW8VwYgZUik.5z3"; # SECRET-DATA
  }
  192.168.65.223 {
    port 1812;
    accounting-port 1813;
    secret "$9$24gGiPzf6CuQFu1EyW8VwYgZUik.5z3"; # SECRET-DATA
  }
}
radius-disconnect-port 2500;
radius-disconnect {
  192.168.65.152 secret "$9$rtkl87ws4ZDkgokPT3tpEcyIWL7-VY4a";
  # SECRET-DATA
  192.168.64.153 secret "$9$gB4UHf5F/A0z30Ihr8Lbs24GDHqmTFn";
  # SECRET-DATA
  192.168.64.157 secret "$9$Hk5FCA0IhruOrv87sYGDikfTFn/t0B";
  # SECRET-DATA
  192.168.64.173 secret "$9$Hk5FCA0IhruOrv87sYGDikfTFn/t0B";
  # SECRET-DATA
}

```

## Configuring the RADIUS Disconnect Server for L2TP

To configure the RADIUS disconnect server to listen for disconnect requests from an administrator and process them, include the following statements at the [edit access] hierarchy level:

```
[edit access]
radius-disconnect-port port-number;
radius-disconnect {
  client-address {
    secret password;
  }
}
```

*port-number* is the server port to which the RADIUS client sends disconnect requests. The LNS, which accepts these disconnect requests, is the server. You can specify a port number on which to contact the RADIUS disconnect server. Most RADIUS servers use port number 1700.



**NOTE:** The JUNOS software accepts only disconnect requests from the client address configured at the [edit access radius-disconnect *client-address*] hierarchy level.

---

*client-address* is the host sending disconnect requests to the RADIUS server. The client address is a valid IP address configured on one of the router interfaces.

*password* authenticates the RADIUS client. Passwords can contain spaces. The secret used by the local router must match that used by the server.

For information about how to configure RADIUS authentication for L2TP, see “Configuring RADIUS Authentication for L2TP” on page 593.

### Example: Configuring the RADIUS Disconnect Server

Configure the RADIUS disconnect server:

```
[edit access]
radius-disconnect-port 1700;
radius-disconnect {
  192.168.64.153 secret "$9$rtkl87ws4ZDkgokPT3tpEcyIWL7-VY4a";
  # SECRET-DATA
  192.168.64.162 secret "$9$rtkl87ws4ZDkgokPT3tpEcyIWL7-VY4a";
  # SECRET-DATA
}
```

