JUNIPER NETWORKS

Junos® OS

Configuring Layer 2 Network Access Protocols, Junos OS Release 11.4

Release
11.4

Published: 2011-11-08
Revision 1

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

Junos® OS Configuring Layer 2 Network Access Protocols, Junos OS Release 11.4

Revision History
October 2011—Revision 1; initial release

The information in this document is current as of the date listed in the revision history.

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

PART 1

Overview

CHAPTER 1

Network Access Configuration Overview

Network Access Configuration Overview

The Junos OS enables you to configure network access features for the device at the **[edit access]** hierarchy level. This includes L2TP, PPP, and Subscriber Access configuration.

The Point-to-Point Protocol (PPP) is an encapsulation protocol for transporting IP traffic across point-to-point links. For M7i, M10i, and M120 routers, you can configure Layer 2 Tunneling Protocol (L2TP) tunneling security services on an Adaptive Services or a MultiServices Physical Interface Card (PIC).

The L2TP protocol allows Point-to-Point Protocol (PPP) to be tunneled within a network.

For a complete hierarchy of access configuration statements, see "Access Configuration Statements" on page 49.

For information about configuring Subscriber Access, see:

- AAA Service Framework for Subscriber Access
- Address-Assignment Pools for Subscriber Access
- DHCP Local Server for Subscriber Access
- PPP for Subscriber Access

Related Documentation

- Access Configuration Statements on page 49
- Configuring the PPP Authentication Protocol on page 8
- Configuring L2TP for Enabling PPP Tunneling Within a Network on page 12
- Defining the Minimum L2TP Configuration on page 13
- Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 14
- Configuring the Group Profile for Defining L2TP Attributes on page 16
- Configuring Access Profiles for L2TP or PPP Parameters on page 19

PART 2

Configuration

CHAPTER 2

Configuring PPP and L2TP

Configuring the PPP Authentication Protocol

The Point-to-Point Protocol (PPP) is an encapsulation protocol for transporting IP traffic across point-to-point links. To configure the Point-to-Point Protocol (PPP), you can configure the Challenge Handshake Authentication Protocol (CHAP). 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.

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.

You can configure multiple CHAP profiles, and 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 is the secret key associated with that peer.

Related Documentation

- Example: Configuring PPP CHAP on page 8
- Example: Configuring CHAP Authentication with RADIUS on page 9

Example: Configuring PPP CHAP

The following example shows how to 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";
            }
        }
    }
}
```

Related Documentation

- Configuring the PPP Authentication Protocol on page 8

Example: Configuring CHAP Authentication with RADIUS

You can send RADIUS messages through a routing instance to customer RADIUS servers in a private network. To configure the routing instance to send packets to a RADIUS server, include the **routing-instance** statement at the **[edit access profile profile-name radius-server]** hierarchy level and apply the profile to an interface with the **access-profile** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* ppp-options chap]** hierarchy level.

In this example, PPP peers of interfaces **at-0/0/0.0** and **at-0/0/0.1** are authenticated by a RADIUS server reachable via routing instance **A**. PPP peers of interfaces **at-0/0/0.2** and **at-0/0/0.3** are authenticated by a RADIUS server reachable via routing instance **B**.

For more information about RADIUS authentication, see Configuring RADIUS Authentication.

```
system {
    radius-server {
        1.1.1.1 secret $9$dalkfj;
        2.2.2.2 secret $9$adsfaszx;
    }
}
routing-instances {
    A {
        instance-type vrf;
        ...
```

```
    }
    B {
      instance-type vrf;
      ...
    }
  }
  access {
    profile A-PPP-clients {
      authentication-order radius;
      radius-server {
        3.3.3.3 {
          port 3333;
          secret "$9$LO/7NbDjqmPQGDmT"; # # SECRET-DATA
          timeout 3;
          retry 3;
          source-address 99.99.99.99;
          routing-instance A;
        }
        4.4.4.4 {
          routing-instance A;
          secret $9$adsfaszx;
        }
      }
    }
    profile B-PPP-clients {
      authentication-order radius;
      radius-server {
        5.5.5.5 {
          routing-instance B;
          secret $9$kljhlkhl;
        }
        6.6.6.6 {
          routing-instance B;
          secret $9$kljhlkhl;
        }
      }
    }
  }
  interfaces {
    at-0/0/0 {
      atm-options {
        vpi 0;
      }
      unit 0 {
        encapsulation atm-ppp-llc;
        ppp-options {
          chap {
            access-profile A-PPP-clients;
          }
        }
        keepalives {
          interval 20;
          up-count 5;
          down-count 5;
        }
        vci 0.128;
```

```
            family inet {
              address 21.21.21.21/32 {
                destination 21.21.21.22;
              }
            }
          }
          unit 1 {
            encapsulation atm-ppp-llc;
            ...
            ppp-options {
              chap {
                access-profile A-PPP-clients;
              }
            }
            ...
          }
          unit 2 {
            encapsulation atm-ppp-llc;
            ...
            ppp-options {
              chap {
                access-profile B-PPP-clients;
              }
            }
            ...
          }
          unit 3 {
            encapsulation atm-ppp-llc;
            ...
            ppp-options {
              chap {
                access-profile B-PPP-clients;
              }
            }
            ...
          }
          ...
        }
        ...
    }
```

Users who log in to the router with telnet or SSH connections are authenticated by the RADIUS server **1.1.1.1**. The backup RADIUS server for these users is **2.2.2.2**.

Each profile may contain one or more backup RADIUS servers. In this example, PPP peers are CHAP authenticated by the RADIUS server **3.3.3.3** (with **4.4.4.4**. as the backup server) or RADIUS server **5.5.5.5** (with **6.6.6.6** as the backup server).

Related Documentation

- Configuring the Authentication Order on page 21
- Example: Configuring PPP CHAP on page 8
- Configuring the PPP Authentication Protocol on page 8

Configuring L2TP for Enabling PPP Tunneling Within a Network

For M7i and M10i routers, you can configure Layer 2 Tunneling Protocol (L2TP) tunneling security services on an Adaptive Services Physical Interface Card (PIC) or a MultiServices PIC. The L2TP protocol allows Point-to-Point Protocol (PPP) to be tunneled within a network.

NOTE: For information about how to configure L2TP service, see the *Junos OS Services Interfaces Configuration Guide* and the *Junos OS Network Interfaces 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 {
      cell-overhead;
      encapsulation-overhead bytes;
      framed-pool pool-id;
      idle-timeout seconds;
      interface-id interface-id;
      keepalive seconds;
      primary-dns primary-dns;
      primary-wins primary-wins;
      secondary-dns secondary-dns;
      secondary-wins secondary-wins;
    }
  }
  profile profile-name {
    authentication-order [ authentication-methods ];
    accounting-order radius;
    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 {
        cell-overhead;
        encapsulation-overhead bytes;
        framed-ip-address ip-address;
        framed-pool framed-pool;
        idle-timeout seconds;
        interface-id interface-id;
        keepalive seconds;
        primary-dns primary-dns;
        primary-wins primary-wins;
        secondary-dns secondary-dns;
        secondary-wins secondary-wins;
      }
      user-group-profile profile-name;
    }
  }
  radius-disconnect-port port-number {
    radius-disconnect {
      client-address {
        secret password;
      }
    }
  }
  radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
    source-address source-address;
    timeout seconds;
  }
}
```

Related Documentation

- Defining the Minimum L2TP Configuration on page 13
- Configuring RADIUS Authentication for L2TP on page 37

Defining the Minimum L2TP Configuration

To define the minimum configuration for the Layer 2 Tunneling Protocol (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-wins;
        secondary-dns secondary-dns;
        secondary-wins secondary-wins;
      }
    }
  }
  radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    secret password;
  }
```

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 received in the Internet Protocol Control Protocol (IPCP) configuration request packet.

Related Documentation

- Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 14

Configuring the Address Pool for L2TP Network Server IP Address Allocation

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 PPP Properties for a Client-Specific Profile" on page 30.

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.

NOTE: The address pools for user access and Network Address Translation (NAT) can overlap. When you configure an address pool at the **[edit access address-pool *pool-name*]** hierarchy level, you can also configure an address pool at the **[edit services nat pool *pool-name*]** hierarchy level.

Related Documentation

- Configuring the Group Profile for Defining L2TP Attributes on page 16
- Defining the Minimum L2TP Configuration on page 13

Example: Configuring an Address-Assignment Pool

This example shows an address-assignment pool configuration that creates two pools, one for IPv4 DHCP clients (**isp_1**) , and a second pool (**chi-fiber-ra**) that is used for router advertisement.

```
[edit access]
address-assignment {
   network-discovery-router-advertisement chi-fiber-ra;
   pool isp_1 {
      family inet {
         network 192.168.0.0/16;
         range southeast {
            low 192.168.102.2 high 192.168.102.254;
         }
         range northeast {
            low 192.168.119.2 high 192.168.119.250;
         }
         host svale6.boston.net {
            hardware-address 90:00:00:01:00:01;
            ip-address 192.168.44.12;
         }
         dhcp-attributes {
```

```
            option-match {
              option-82 {
                circuit-id fiber range northeast;
              }
              option-82 {
                circuit-id cable_net range southeast;
              }
            }
            boot-file boot.client;
            boot-server 192.168.200.100;
            grace-period 3600;
            maximum-lease-time 18000;
            netbios-node-type p-node;
            router 192.168.44.44 192.168.44.45;
          }
        }
      }
      pool chi-fiber-ra {
        family inet6 {
          prefix 2008:2009:2010::/48;
          range fiber3 {
            low 2008:2009:2010::1/64;
            high 2008:2009:2010::5/64;
          }
        }
      }
    }
```

This example creates an IPv4 address-assignment pool named **isp-1**, which contains two named address ranges, **southeast** and **northeast**. The address-assignment pool also contains a static binding for client **host sval6.boston.net**. The ISP_1 pool configuration also includes the **dhcp-attributes** statement, indicating that the pool is used for DHCP clients. If the option 82 **circuit-id** entry matches the string **fiber**, then DHCP assigns the client an address from the **northeast** range. If the option 82 **circuit-id** matches the string **cable_net**, DHCP assigns an address from the **southeast** range.

The second address-assignment pool created in this example is **chi-fiber-ra**. The **neighbor-discovery-router-advertisement** statement at the beginning of the syntax specifies that this named address-assignment pool is used for router advertisement. The syntax at the end of the example configures the address-assignment pool named **chi-fiber-ra**.

Related Documentation

- Address-Assignment Pools Overview
- Configuring Address-Assignment Pools
- Configuring an Address-Assignment Pool for Router Advertisement

Configuring the Group Profile for Defining L2TP Attributes

Optionally, you can configure the group profile to define the Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol (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 32.

Tasks for configuring the group profile are:

1. Configuring L2TP for a Group Profile on page 17
2. Configuring the PPP Attributes for a Group Profile on page 17

Configuring L2TP for a Group Profile

To configure the Layer 2 Tunneling Protocol (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.

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 OS 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 Point-to-Point Protocol (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]
cell-overhead;
encapsulation-overhead bytes;
framed-pool pool-id;
idle-timeout seconds;
interface-id interface-id;
keepalive seconds;
primary-dns primary-dns;
```

primary-wins *primary-wins*;
secondary-dns *secondary-dns*;
secondary-wins *secondary-wins*;

The **cell-overhead** statement configures the session to use Asynchronous Transfer Mode (ATM)-aware egress shaping on the IQ2 PIC.

bytes (in the **encapsulation-overhead** statement) configures the number of bytes used as overhead for class-of-service calculations.

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.

seconds (in the **keepalive** statement) is the time period that must elapse before the Junos OS checks the status of the PPP session by sending an echo request to the peer. For each session, Junos OS 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 message 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-wins (in the **primary-wins** statement) is an IPv4 address.

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

Example: Group Profile Configuration

The following example shows how to 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;
      }
    }
```

Related Documentation

- Configuring the Group Profile for Defining L2TP Attributes on page 16
- Defining the Minimum L2TP Configuration on page 13
- Referencing the Group Profile from the L2TP Profile on page 26

Configuring Access Profiles for L2TP or PPP Parameters

To validate Layer 2 Tunneling Protocol (L2TP) connections and session requests, you set up access profiles by configuring the profile statement at the **[edit access]** hierarchy level. You can configure multiple profiles. You can also configure multiple clients for each profile.

Tasks for configuring the access profile are:

1. Configuring the Access Profile on page 19
2. Configuring the L2TP Properties for a Profile on page 20
3. Configuring the PPP Properties for a Profile on page 20
4. Configuring the Authentication Order on page 21
5. Configuring the Accounting Order on page 21

Configuring the Access 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 32.

When you configure a profile, you can only configure either L2TP or PPP parameters. You cannot configure both at the same time.

Configuring the L2TP Properties for a Profile

To configure the Layer 2 Tunneling Protocol (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 ];
accounting-order radius;
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;
```

Configuring the PPP Properties for a Profile

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 {
    cell-overhead;
    encapsulation-overhead bytes;
    framed-ip-address ip-address;
    framed-pool framed-pool;
    idle-timeout seconds;
    interface-id interface-id;
    keepalive seconds;
    primary-dns primary-dns;
    primary-wins primary-wins;
    secondary-dns secondary-dns;
```



```
        secondary-wins secondary-wins;
    }
}
```

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

Configuring the Authentication Order

You can configure the order in which the Junos OS 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 37.

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

Configuring the Accounting Order

You can configure RADIUS accounting for an L2TP profile.

With RADIUS accounting enabled, Juniper Networks routers or switches, acting as RADIUS clients, can notify the RADIUS server about user activities such as software logins, configuration changes, and interactive commands. The framework for RADIUS accounting is described in RFC 2866.

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

```
[edit access profile profile-name]
accounting-order radius;
```

When you enable RADIUS accounting for an L2TP profile, it applies to all the clients within that profile. You must enable RADIUS accounting on at least one LT2P profile for the RADIUS authentication server to send accounting stop and start messages.

NOTE: When you enable RADIUS accounting for an L2TP profile, you do not need to configure the **accounting-port** statement at the **[edit access radius-server *server-address*]** hierarchy level. When you enable RADIUS accounting for an L2TP profile, accounting is triggered on the default port of 1813.

For L2TP, RADIUS authentication servers are configured at the **[edit access radius-server]** hierarchy level.

Configuring an IKE Access Profile

An Internet Key Exchange (IKE) access profile is used to negotiate IKE and IPsec security associations with dynamic peers. You can configure only one tunnel profile per service set for all dynamic peers. The configured preshared key in the profile is used for IKE authentication of all dynamic peers terminating in that service set. You can also use the digital certificate method for IKE authentication with dynamic peers. Include the **ike-policy *policy-name*** statement at the **[edit access profile *profile-name* client * ike]** hierarchy level. ***policy-name*** is the name of the IKE policy you define at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level.

The IKE tunnel profile specifies all the information you need to complete the IKE negotiation. Each protocol has its own statement hierarchy within the client statement to configure protocol-specific attribute value pairs, but only one client configuration is allowed for each profile. The following is the configuration hierarchy.

```
[edit access]
profile profile-name {
   client * {
      ike {
         allowed-proxy-pair {
            remote remote-proxy-address local local-proxy-address;
         }
         pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
         ike-policy policy-name;
         initiate-dead-peer-detection;
         interface-id string-value;
         ipsec-policy ipsec-policy;
      }
   }
}
```

For dynamic peers, the Junos OS supports only IKE main mode with both the preshared key and digital certificate methods. In this mode, an IPv6 or IPv4 address is used to identify a tunnel peer to obtain the preshared key or digital certificate information. The client value * (wildcard) means that configuration within this profile is valid for all dynamic peers terminating within the service set accessing this profile.

The following statement makes up the IKE profile:

- **allowed-proxy-pair**—During phase 2 IKE negotiation, the remote peer supplies its network address (**remote**) and its peer's network address (**local**). Since multiple dynamic tunnels are authenticated through the same mechanism, this statement must include the list of possible combinations. If the dynamic peer does not present a valid combination, the phase 2 IKE negotiation fails.

By default, **remote 0.0.0.0/0 local 0.0.0.0/0** is used if no values are configured.

- **pre-shared-key**—Key used to authenticate the dynamic peer during IKE phase 1 negotiation. This key is known to both ends through an out-of-band secure mechanism. You can configure the value either in **hexadecimal** or **ascii-text** format. It is a mandatory value.
- **ike-policy**—Name of the IKE policy that defines either the local digital certificate or the preshared key used to authenticate the dynamic peer during IKE negotiation. You must include this statement to use the digital certificate method for IKE authentication with a dynamic peer. You define the IKE policy at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level.
- **initiate-dead-peer-detection**—Detects dead peers on dynamic IPsec tunnels.
- **interface-id**—Interface identifier, a mandatory attribute used to derive the logical service interface information for the session.
- **ipsec-policy**—Name of the IPsec policy that defines the IPsec policy information for the session. You define the IPsec policy at the **[edit services ipsec-vpn ipsec policy *policy-name*]** hierarchy level. If no policy is set, any policy proposed by the dynamic peer is accepted.

Related Documentation

- Configuring Access Profiles for L2TP or PPP Parameters on page 19

Configuring the L2TP 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.

NOTE: The * for the default client configuration applies only to M Series routers. On MX Series routers, use default instead. See Configuring an L2TP Access Profile on the LNS for more about MX Series routers.

Related Documentation

- Example: Defining the Default Tunnel Client on page 24

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.

Optionally, you can 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.

Related Documentation

- Configuring the L2TP Client on page 23
- Example: Defining the User Group Profile on page 24

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;
}
```

Related Documentation

- Applying a Configured PPP Group Profile to a Tunnel on page 32.

Configuring the CHAP Secret for an L2TP Profile

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.

NOTE: When you configure PPP properties for a Layer 2 Tunneling Protocol (L2TP) 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.

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.

Related Documentation

- Example: Configuring L2TP PPP CHAP on page 25

Example: Configuring L2TP PPP CHAP

Configure the 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
  }
}
```

Related Documentation

- Configuring the CHAP Secret for an L2TP Profile on page 25

Referencing the Group Profile from the L2TP 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.

Related Documentation

- Example: Defining the User Group Profile on page 24
- Configuring Access Profiles for L2TP or PPP Parameters on page 19
- Configuring L2TP Properties for a Client-Specific Profile on page 26

Configuring L2TP Properties for a Client-Specific Profile

To define L2TP properties for a client-specific 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 configure either L2TP or PPP parameters, but not both at the same time.

```
[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;
  fragment-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.

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 OS 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 OS 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 fragment-threshold statement). If a packet exceeds the fragmentation threshold, the Junos OS fragments it into two or more multilink fragments.

Related Documentation

- Configuring PPP Properties for a Client-Specific Profile on page 30
- Example: PPP MP for L2TP on page 28

- Example: L2TP Multilink PPP Support on Shared Interfaces on page 28

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;
      }
    }
  }
}
```

Related Documentation

- Referencing the Group Profile from the L2TP Profile on page 26
- Example: L2TP Multilink PPP Support on Shared Interfaces on page 28

Example: L2TP Multilink PPP Support on Shared Interfaces

On M7i and M10i routers, L2TP multilink PPP sessions are supported on both dedicated and shared interfaces. This example shows how to configure many multilink bundles on a single ASP shared interface.

```
[edit]
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 cholera {
      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 {
        tunnel-access-profile t;
        user-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;
        }
      }
    }
  }
```

Related Documentation

- Referencing the Group Profile from the L2TP Profile on page 26

Configuring the PAP Password for an L2TP Profile

When you configure PPP properties for an L2TP 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 for an L2TP Profile" on page 25.

To configure the Password Authentication Protocol (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 PAP.

Related Documentation

- Example: Configuring PAP for an L2TP Profile on page 30

Example: Configuring PAP for an L2TP Profile

The following examples shows you how to configure the password authentication protocol for an L2TP profile:

```
[edit access]
profile sunnyvale_bldg_2 {
   client green {
      pap-password "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3";
      ppp {
         interface-id west;
      }
      group-profile sunnyvale_users;
   }
   client red {
      chap-secret "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3";
      group-profile sunnyvale_users;
   }
   authentication-order radius;
}
profile Sunnyvale_bldg_1_tunnel {
   client test {
      l2tp {
         shared-secret "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3";
         ppp-authentication pap;
      }
   }
}
```

Related Documentation

- Configuring the PAP Password for an L2TP Profile on page 29

Configuring PPP Properties for a Client-Specific 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.

NOTE: 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]
cell-overhead;
encapsulation-overhead bytes;
framed-ip-address ip-address;
framed-pool pool-id;
idle-timeout seconds;
interface-id interface-id;
keepalive seconds;
keepalive-retries number-of-retries;
```

primary-dns *primary-dns*;
primary-wins *primary-wins*;
secondary-dns *secondary-dns*;
secondary-wins *secondary-wins*;

NOTE: When you configure a profile, you can configure either L2TP or PPP parameters, but not both at the same time.

The **cell-overhead** statement configures the session to use ATM-aware egress shaping on the IQ2 PIC.

bytes (in the **encapsulation-overhead** statement) configures the number of bytes used as overhead for class-of-service calculations.

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.

keepalive *seconds* is the time period that must elapse before the Junos OS checks the status of the PPP session by sending an echo request to the peer. For each session, Junos OS sends a maximum of ten 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 can configure this to be a value in the range from 0 through 32,767 seconds.

keepalive-retries *number-of-retries* is the number of retry attempts for checking the keepalive status of a Point-to-Point (PPP) protocol session. Configuring a lower number of retries helps reduce the detection time for PPP client session failures or timeouts if you have configured a **keepalive *seconds*** value. By default, the number of retries is set to 10 times. You can configure this to be a value in the range from 3 through 32,767 times.

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.

Related Documentation

- Configuring L2TP Properties for a Client-Specific Profile on page 26

Applying a Configured PPP Group Profile to a Tunnel

On Mi7 and M10i routers, 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 OS 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.

Related Documentation

- Example: Applying a User Group Profile on the M7i or M10i Router on page 32
- Example: Defining the User Group Profile on page 24

Example: Applying a User Group Profile on the M7i or M10i Router

The following example shows how to 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
    }
  }
  profile westcoast_bldg_1 {
    client white {
      chap-secret "$9$3s2690IeK8X7VKM7VwgaJn/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
    }
  }
```

Related Documentation

- Applying a Configured PPP Group Profile to a Tunnel on page 32

Example: Configuring the Access Profile

The following example shows you how to configure the access profile:

```
[edit access]
profile westcoast_bldg_1 {
  client white {
    chap-secret "$9$3s2690IeK8X7VKM7VwgaJn/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 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/t0BEleWFnRh
      rlXxbs2aJDHqf3nCP5";
      # SECRET-DATA
      ppp-authentication chap;
    }
    group-profile westcoast_tunnel;
  }
}
```

Related Documentation

- Configuring Access Profiles for L2TP or PPP Parameters on page 19

Example: Configuring L2TP

The following example shows how to 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$3s2690IeK8X7VKM7VwgaJn/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 "$9$r3HKvLg4ZUDkX7JGjif5p0BIRS8LN";
      # 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/t0BEleWFnRh
      rlXxbs2aJDHqf3nCP5"; # SECRET-DATA
      ppp-authentication chap;
    }
    group-profile westcoast_tunnel;
  }
}
profile westcoast_bldg_2_tunnel {
  client black {
```

```
        l2tp {
          shared-secret "$9$R2QErv8X-goGylVwg4jiTz36/t0BEleWFnRh
          rlXxbs2aJDHqf3nCP5";
          # SECRET-DATA
          ppp-authentication pap;
        }
        group-profile westcoast_tunnel;
      }
    }
  }
```

Related Documentation

- Configuring L2TP for Enabling PPP Tunneling Within a Network on page 12

CHAPTER 3

Configuring RADIUS Authentication for L2TP

Configuring RADIUS Authentication for L2TP

The L2TP network server (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 RADIUS authentication for L2TP on an M10i or M7i router, include the following statements at the **[edit access]** hierarchy level:

```
[edit access]
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    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*).

NOTE: If you enable RADIUS accounting at the **[edit access profile** *profile-name* **accounting-order]** hierarchy level, accounting is triggered on the default port of 1813 even if you do not specify a value for the **accounting-port** statement.

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 2865, *Remote Authentication Dial In User Service [RADIUS]*).

You must specify a password in the **secret** statement. If a password includes spaces, enclose the password in quotation marks. 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. If the maximum number of retries is reached, the radius server is considered dead for 5 minutes (300 seconds).

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 43.

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 received by the Internet Protocol Control Protocol (IPCP) configuration request packet.

Related Documentation

- RADIUS Attributes for L2TP on page 39
- Configuring L2TP for Enabling PPP Tunneling Within a Network on page 12
- Configuring the RADIUS Disconnect Server for L2TP on page 43

RADIUS Attributes for L2TP

The Junos OS supports the following types of RADIUS attributes for L2TP:

- Juniper Networks vendor-specific attributes
- Attribute-value pairs (AVPs) defined by the Internet Engineering Task Force (IETF)
- RADIUS accounting stop and start AVPs

Juniper Networks vendor-specific RADIUS attributes are described in RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*. These attributes are encapsulated with the vendor ID set to the Juniper Networks ID number 2636. Table 1 on page 39 lists the Juniper Networks vendor-specific attributes you can configure for L2TP.

Table 1: Juniper Networks Vendor-Specific RADIUS Attributes for L2TP

Attribute Name	Standard Number	Value
Juniper-Primary-DNS	31	IP address
Juniper-Primary-WINS	32	IP address
Juniper-Secondary-DNS	33	IP address
Juniper-Secondary-WINS	34	IP address
Juniper-Interface-ID	35	String
Juniper-IP-Pool-Name	36	String
Juniper-Keep-Alive	37	Integer

Table 2 on page 39 lists the IETF RADIUS AVPs supported for LT2P.

Table 2: Supported IETF RADIUS Attributes for L2TP

Attribute Name	Standard Number	Value
User-Name	1	String
User-Password	2	String
CHAP-Password	3	String
NAS-IP-Address	4	IP address
NAS-Port	5	Integer
Service-Type	6	Integer

Table 2: Supported IETF RADIUS Attributes for L2TP *(continued)*

Attribute Name	Standard Number	Value
Framed-Protocol	7	Integer
Framed-IP-Address	8	IP address
Framed-IP-Netmask	9	IP address
Framed-MTU	12	Integer
Framed-Route	22	String
Session-Timeout	27	Integer
Idle-Timeout	28	Integer
Called-Station-ID	30	String
Calling-Station-ID	31	String
CHAP-Challenge	60	String
NAS-Port-Type	61	Integer
Framed-Pool	88	Integer

Table 3 on page 40 lists the supported RADIUS accounting start AVPs for L2TP.

Table 3: Supported RADIUS Accounting Start Attributes for L2TP

Attribute Name	Standard Number	Value
User-Name	1	String
NAS-IP-Address	4	IP address
NAS-Port	5	Integer
Service-Type	6	Integer
Framed-Protocol	7	Integer
Framed-IP-Address	8	IP address
Called-Station-ID	30	String
Calling-Station-ID	31	String
Acct-Status-Type	40	Integer

Table 3: Supported RADIUS Accounting Start Attributes for L2TP *(continued)*

Attribute Name	Standard Number	Value
Acct-Delay-Time	41	Integer
Acct-Session-ID	44	String
Acct-Authentic	45	Integer
NAS-Port-Type	61	Integer
Tunnel-Client-Endpoint	66	String
Tunnel-Server-Endpoint	67	String
Acct-Tunnel-Connection	68	String
Tunnel-Client-Auth-ID	90	String
Tunnel-Server-Auth-ID	91	String

Table 4 on page 41 lists the supported RADIUS accounting stop AVPs for L2TP.

Table 4: Supported RADIUS Accounting Stop Attributes for L2TP

Attribute Name	Standard Number	Value
User-Name	1	String
NAS-IP-Address	4	IP address
NAS-Port	5	Integer
Service-Type	6	Integer
Framed-Protocol	7	Integer
Framed-IP-Address	8	IP address
Called-Station-ID	30	String
Calling-Station-ID	31	String
Acct-Status-Type	40	Integer
Acct-Delay-Time	41	Integer
Acct-Input-Octets	42	Integer

Table 4: Supported RADIUS Accounting Stop Attributes for L2TP *(continued)*

Attribute Name	Standard Number	Value
Acct-Output-Octets	43	Integer
Acct-Session-ID	44	String
Acct-Authentic	45	Integer
Acct-Session-Time	46	Integer
Acct-Input-Packets	47	Integer
Acct-Output-Packets	48	Integer
Acct-Terminate-Cause	49	Integer
Acct-Multi-Session-ID	50	String
Acct-Link-Count	51	Integer
NAS-Port-Type	61	Integer
Tunnel-Client-Endpoint	66	String
Tunnel-Server-Endpoint	67	String
Acct-Tunnel-Connection	68	String
Tunnel-Client-Auth-ID	90	String
Tunnel-Server-Auth-ID	91	String

Related Documentation

- Example: Configuring RADIUS Authentication for L2TP on page 42

Example: Configuring RADIUS Authentication for L2TP

The following example shows how to configure RADIUS authentication for L2TP:

```
[edit access]
profile sunnyvale_bldg_2 {
   client green {
      chap-secret "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3";
      ppp {
         interface-id west;
      }
      group-profile sunnyvale_users;
   }
   client red {
```

```
        chap-secret "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3";
        group-profile sunnyvale_users;
      }
      authentication-order radius;
    }
    radius-server {
      192.168.65.213 {
        port 1812;
        accounting-port 1813;
        secret "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3"; # SECRET-DATA
      }
      192.168.65.223 {
        port 1812;
        accounting-port 1813;
        secret "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3"; # SECRET-DATA
      }
    }
    radius-disconnect-port 2500;
    radius-disconnect {
      192.168.65.152 secret "$9$rtkl87ws4ZDkgokPT3tpEcylWL7-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
    }
```

Related Documentation

- Configuring RADIUS Authentication for L2TP on page 37

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 L2TP network server, 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 OS 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 or switch 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 37.

The following example shows the statements to be included at the **[edit access]** hierarchy level to configure the RADIUS disconnect server:

```
[edit access]
radius-disconnect-port 1700;
radius-disconnect {
   192.168.64.153 secret "$9$rtkl87ws4ZDkgokPT3tpEcylWL7-VY4a";
   # SECRET-DATA
   192.168.64.162 secret "$9$rtkl87ws4ZDkgokPT3tpEcylWL7-VY4a";
   # SECRET-DATA
}
```

Related Documentation

- Configuring RADIUS Authentication for L2TP on page 37

Configuring RADIUS Authentication for an L2TP Client and Profile

On an M10i or M7i router, L2TP supports RADIUS authentication and accounting for users with one set of RADIUS servers under the **[edit access]** hierarchy. You can also configure RADIUS authentication for each tunnel client or user profile.

To configure the RADIUS authentication for L2TP tunnel clients on an M10i or M7i router, include the **ppp-profile** statement with the **l2tp** attributes for tunnel clients:

```
[edit access profile profile-name client client-name l2tp]
ppp-profile profile-name;
```

ppp-profile *profile-name* specifies the profile used to validate PPP session requests through L2TP tunnels. Clients of the referenced profile must have only PPP attributes. The referenced group profile must be defined.

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

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

When a PPP user initiates a session and RADIUS authentication is configured for the user profile on the tunnel group, the following priority sequence is used to determine which RADIUS server is used for authentication and accounting:

- If the **ppp-profile** statement is configured under the tunnel client (LAC), the RADIUS servers configured under the specified **ppp-profile** are used.
- If RADIUS servers are configured under the user profile for the tunnel group, those servers will be used.
- If no RADIUS server is configured for the tunnel client (LAC) or user profile, then the RADIUS servers configured at the **[edit access]** hierarchy level are used.

Related Documentation

- Example: Configuring RADIUS Authentication for an L2TP Profile on page 45

Example: Configuring RADIUS Authentication for an L2TP Profile

The following example shows statements to be included at the **[edit access]** hierarchy level to configure RADIUS authentication for an L2TP profile:

```
[edit access]
profile t {
   client LAC_A {
      l2tp {
         ppp-profile u;
      }
   }
}
profile u {
   client client_1 {
      ppp {
      }
   }
   5.5.5.5 {
      port 3333;
      secret $9$dkafeqwrew;
      source-address 1.1.1.1;
      retry 3;
      timeout 3;
   }
   6.6.6.6 secret $9$fe3erqwrez;
   7.7.7.7 secret $9$f34929ftby;
}
```

Related Documentation

- Configuring RADIUS Authentication for an L2TP Client and Profile on page 44

Example: Configuring RADIUS-Based Subscriber Authentication and Accounting

This example shows a RADIUS-based authentication and accounting configuration.

```
[edit access]
radius-server {
```

```
    192.168.1.250 {
      port 1812;
      accounting-port 1813;
      retry 3;
      secret &tIUEI*7688+;
      source-address 192.168.1.100;
      timeout 45;
    }
    192.168.1.251 {
      port 1812;
      accounting-port 1813;
      retry 3;
      secret $Dyu*UY(877-;
      source-address 192.168.1.100;
      timeout 30;
    }
    192.168.1.252 {
      port 1812;
      secret $Dyu*UY(877-;
    }
  }
  profile isp-bos-metro-fiber-basic {
    authentication {
      order radius none;
    }
    accounting {
      order radius;
      accounting-stop-on-access-deny;
      accounting-stop-on-failure;
      immediate-update;
      statistics time;
      update-interval 12;
    }
    radius {
      authentication-server 192.168.1.251 192.168.1.252;
      accounting-server 192.168.1.250 192.168.1.251;
      options {
        accounting-session-id-format decimal;
        client-accounting-algorithm round-robin;
        client-authentication-algorithm round-robin;
        nas-identifier 56;
        nas-port-id-delimiter %;
        nas-port-id-format {
          nas-identifier;
          interface-description;
        }
        nas-port-type {
          ethernet {
            wireless-80211;
          }
        }
      }
      attributes {
        ignore {
          framed-ip-netmask;
        }
```

```
        exclude {
          accounting-delay-time [accounting-start accounting-stop];
          accounting-session-id [access-request accounting-on accounting-off
          accounting-start accounting-stop];
          dhcp-gi-address [access-request accounting-start accounting-stop];
          dhcp-mac-address [access-request accounting-start accounting-stop];
          nas-identifier [access-request accounting-start accounting-stop];
          nas-port [accounting-start accounting-stop];
          nas-port-id [accounting-start accounting-stop];
          nas-port-type [access-request accounting-start accounting-stop];
        }
      }
    }
}
[edit logical-systems isp-bos-metro-12 routing-instances isp-cmbrg-12-32]
interfaces {
    lo0 {
      unit 0 {
        family inet {
          address 192.168.1.100/24;
        }
      }
    }
    ge-0/0/0 {
      vlan-tagging;
      unit 0 {
        vlan-id 200;
        family inet {
          unnumbered-address lo0.0;
        }
      }
    }
}
```

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers

CHAPTER 4

Configuration Statements

Access Configuration Statements

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

```
[edit access]
address-assignment {
   neighbor-discovery-router-advertisement;
   pool pool-name {
      family inet {
           dhcp-attributes {
              [protocol-specific-attributes];
           }
           host hostname {
              hardware-address mac-address;
              ip-address ip-address;
           }
        network address-or-prefix </subnet-mask>;
           range name {
           high upper-limit;
           low lower-limit;
           prefix-length prefix-length;
        }
      }
   }
}
address-pool pool-name {
   address address-or-prefix;
   address-range low <lower-limit> high <upper-limit>;
}
domain {
   delimiter;
   map;
   parse-direction;
};
group-profile profile-name {
   l2tp {
      interface-id interface-id;
      lcp-renegotiation;
      local-chap;
```

```
        maximum-sessions-per-tunnel number;
        multilink {
          drop-timeout milliseconds;
          fragment-threshold bytes;
        }
      }
      ppp {
        cell-overhead;
        encapsulation-overhead bytes;
        framed-pool pool-id;
        idle-timeout seconds;
        interface-id interface-id;
        keepalive seconds;
        primary-dns primary-dns;
        primary-wins primary-wins;
        secondary-dns secondary-dns;
        secondary-wins secondary-wins;
      }
    }
    profile profile-name {
      accounting {
        accounting-stop-on-access-deny;
        accounting-stop-on-failure;
        coa-immediate-update;
        immediate-update;
        order [ accounting-method ];
        statistics (time | volume-time);
        update-interval minutes;
      }
      accounting-order radius;
      authentication-order [ authentication-methods ];
      client client-name {
        chap-secret chap-secret;
        group-profile profile-name;
        ike {
          allowed-proxy-pair {
            remote remote-proxy-address local local-proxy-address;
          }
          pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
          ike-policy policy-name;
          ipsec-policy ipsec-policy;
          interface-id interface-id;
        }
        l2tp {
          interface-id interface-id;
          lcp-renegotiation;
          local-chap;
          maximum-sessions-per-tunnel number;
          multilink {
            drop-timeout milliseconds;
            fragment-threshold bytes;
          }
          ppp-authentication (chap | pap);
          ppp-profile profile-name;
          shared-secret shared-secret;
        }
```

```
    pap-password pap-password;
    ppp {
      cell-overhead;
      encapsulation-overhead bytes;
      framed-ip-address ip-address;
      framed-pool framed-pool;
      idle-timeout seconds;
      interface-id interface-id;
      keepalive seconds;
      primary-dns primary-dns;
      primary-wins primary-wins;
      secondary-dns secondary-dns;
      secondary-wins secondary-wins;
    }
    user-group-profile profile-name;
  }
  radius {
    authentication-server [ ip-address ];
    accounting-server [ ip-address ];
    options {
      accounting-session-id-format (decimal | description);
      client-accounting-algorithm (direct | round-robin);
      client-authentication-algorithm (direct | round-robin);
      ethernet-port-type-virtual;
      interface-description-format [sub-interface | adapter];
      nas-identifier identifier-value;
      nas-port-extended-format {
        adapter-width width;
        port-width width;
        slot-width width;
        stacked-vlan-width width;
        vlan-width width;
      }
      revert-interval interval;
      vlan-nas-port-stacked-format;
    }
    attributes {
      ignore {
        framed-ip-netmask;
        input-filter;
        logical-system-routing-instance;
        output-filter;
      }
      exclude
        accounting-authentic [ accounting-on | accounting-off ];
        accounting-delay-time [ accounting-on | accounting-off ];
        accounting-session-id [ access-request | accounting-on | accounting-off |
          accounting-stop ];
        accounting-terminate-cause [ accounting-off ];
        called-station-id [ access-request | accounting-start | accounting-stop ];
        calling-station-id [ access-request | accounting-start | accounting-stop ];
        class [ accounting-start | accounting-stop ];
        dhcp-options [ access-request | accounting-start | accounting-stop ];
        dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
        dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
        output-filter [ accounting-start | accounting-stop ];
```

```
            event-timestamp [ accounting-on | accounting-off | accounting-start |
              accounting-stop ];
            framed-ip-address [ accounting-start | accounting-stop ];
            framed-ip-netmask [ accounting-start | accounting-stop ];
            input-filter [ accounting-start | accounting-stop ];
            input-gigapackets [ accounting-stop ];
            input-gigawords [ accounting-stop ];
            interface-description [ access-request | accounting-start | accounting-stop ];
            nas-identifier [ access-request | accounting-on | accounting-off | accounting-start
              | accounting-stop ];
            nas-port [ access-request | accounting-start | accounting-stop ];
            nas-port-id [ access-request | accounting-start | accounting-stop ];
            nas-port-type [ access-request | accounting-start | accounting-stop ];
            output-gigapackets [ accounting-stop ];
            output-gigawords [ accounting-stop ];
          }
        }
      }
      radius-server server-address {
        accounting-port port-number;
        port port-number;
        retry attempts;
        routing-instance routing-instance-name;
        secret password;
        source-address source-address;
        timeout seconds;
      }
    }
    radius-disconnect {
      client-address {
        secret password;
      }
    }
    radius-disconnect-port port-number;
    radius-server server-address {
      accounting-port port-number;
      port port-number;
      retry attempts;
      routing-instance routing-instance-name;
      secret password;
      source-address source-address;
      timeout seconds;
    }
```

Related Documentation

- Configuring the PPP Authentication Protocol on page 8
- Example: Configuring PPP CHAP on page 8
- Configuring the PPP Authentication Protocol on page 8
- Example: Configuring CHAP Authentication with RADIUS on page 9
- Configuring L2TP for Enabling PPP Tunneling Within a Network on page 12
- Defining the Minimum L2TP Configuration on page 13
- Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 14

- Configuring the Group Profile for Defining L2TP Attributes on page 16

accounting (access profile)

Syntax

```
accounting {
  accounting-stop-on-access-deny;
  accounting-stop-on-failure;
  coa-immediate-update;
  coa-no-override service-class-attribute;
  duplication;
  immediate-update;
  order [ accounting-method ];
  statistics (time | volume-time);
  update-interval minutes;
}
```

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access
- Configuring Per-Subscriber Session Accounting
- Understanding RADIUS Accounting Duplicate Reporting

accounting-order

Syntax accounting-order radius;

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

Release Information Statement introduced in Junos OS Release 8.0.

Description Enable RADIUS accounting for an L2TP profile.

Options **radius**—Use the RADIUS accounting method.

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

Related Documentation
- Configuring the Accounting Order on page 21

accounting-port

Syntax accounting-port *port-number*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the port number on which to contact the accounting server.

Options ***port-number***—Port number on which to contact the accounting server. Most RADIUS servers use port number 1813 (as specified in RFC 2866).

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

Related Documentation
- Configuring Router or Switch Interaction with RADIUS Servers
- Configuring Authentication and Accounting Parameters for Subscriber Access
- Configuring RADIUS Authentication for L2TP on page 37

accounting-server

Syntax accounting-server [*ip-address*];

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

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify a list of the RADIUS accounting servers used for accounting for DHCP, L2TP, and PPP clients.

Options ***ip-address***—IP version 4 (IPv4) address.

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

Related Documentation
- Configuring Authentication and Accounting Parameters for Subscriber Access

accounting-session-id-format

Syntax accounting-session-id-format (decimal | description);

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the format the router or switch uses to identify the accounting session.

Default **decimal**

Options **decimal**—Use the decimal format.

description—Use the generic format, in the form: **jnpr** *interface-specifier:subscriber-session-id*.

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

Related Documentation
- Configuring RADIUS Server Options for Subscriber Access
- Configuring Authentication and Accounting Parameters for Subscriber Access

accounting-stop-on-access-deny

Syntax accounting-stop-on-access-deny;

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure RADIUS accounting to send an Acct-Stop message when the AAA server refuses a client request for access.

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

Related Documentation
- Configuring Authentication and Accounting Parameters for Subscriber Access

accounting-stop-on-failure

Syntax accounting-stop-on-failure;

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure RADIUS accounting to send an Acct-Stop message when client access fails AAA but the AAA server grants access.

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

Related Documentation
- Configuring Authentication and Accounting Parameters for Subscriber Access

address

Syntax address *address-or-prefix*;

Hierarchy Level [edit access address-pool *pool-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the IP address or prefix value for clients.

Options ***address-or-prefix***—An address or prefix value.

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

Related Documentation

- Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 14

address-assignment (Address-Assignment Pools)

Syntax

```
address-assignment {
  abatedUtilization percentage;
  abatedUtilization-v6 percentage;
  highUtilization percentage;
  highUtilization-v6 percentage;
  neighbor-discovery-router-advertisement ndra-pool-name;
  pool pool-name {
    family family {
      dhcp-attributes {
        protocol-specific attributes;
      }
      host hostname {
        hardware-address mac-address;
        ip-address ip-address;
      }
      network ip-prefix/<prefix-length>;
      prefix ipv6-prefix;
      range range-name {
        high upper-limit;
        low lower-limit;
        prefix-length prefix-length;
      }
    }
    link pool-name;
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 9.0.
Support for LNS on MX Series routers introduced in Junos OS Release 11.4. Not all subordinate statements are supported for L2TP LNS on MX Series routers.

Description Configure address-assignment pools that can be used by different client applications.

Options *pool-name*—Name assigned to an address-assignment pool.

The remaining statements are explained separately.

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

Related Documentation

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

address-pool

Syntax

```
address-pool pool-name {
    address address-or-prefix;
    address-range <low lower-limit> <high upper-limit>;
}
```

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Allocate IP addresses for clients.

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

Options ***pool-name***—Name assigned to an address pool.

The remaining statements are explained separately.

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

Related Documentation

- Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 14

address-range

Syntax

```
address-range <low lower-limit> <high upper-limit>;
```

Hierarchy Level [edit access address-pool *pool-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the address range.

Options

- **high** ***upper-limit***—Upper limit of an address range.
- **low** ***lower-limit***—Lower limit of an address range.

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

Related Documentation

- Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 14

allowed-proxy-pair

Syntax

```
allowed-proxy-pair {
    remote remote-proxy-address local local-proxy-address;
}
```

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

Release Information Statement introduced in Junos OS Release 7.4.

Description Specify the network address of the local and remote peer associated with an IKE access profile.

Options

local *local-proxy-address*—Network address of the local peer.

Default: 0.0.0.0

remote *remote-proxy-address*—Network address of the remote peer.

Default: 0.0.0.0

Required Privilege Level

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

Related Documentation

- Configuring an IKE Access Profile on page 22

attributes

Syntax

```
attributes {
  exclude {
    ...
  }
  ignore {
    framed-ip-netmask;
    input-filter;
    logical-system-routing-instance;
    output-filter;
  }
}
```

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Specify how the router or switch processes RADIUS attributes.

The remaining statements are explained separately.

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

Related Documentation

- Configuring How RADIUS Attributes Are Used for Subscriber Access

authentication-order

Syntax authentication-order [*authentication-methods*];

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

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
none option introduced in Junos OS Release 11.2.

Description Set the order in which the Junos OS tries different authentication methods when verifying that a client can access the router or switch. For each login attempt, the software tries the authentication methods in order, from first to last.

Default password

Options *authentication-methods*

- **none**—Grants authentication without examining the client credentials. Can be used, for example, when the Diameter function Gx-Plus is employed for notification during subscriber provisioning.
- **password**—Verify the client using the information configured at the **[edit access profile *profile-name* client *client-name*]** hierarchy level.
- **radius**—Verify the client using RADIUS authentication services.

NOTE: For subscriber access management, you must always specify the radius method. Subscriber access management does not support the password option (the default), and authentication fails when no method is specified.

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

Related Documentation

- Example: Configuring CHAP Authentication with RADIUS on page 9
- Specifying the Authentication and Accounting Methods for Subscriber Access
- Configuring Access Profiles for L2TP or PPP Parameters on page 19

authentication-server

Syntax authentication-server [*ip-address*];

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

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify a list of the RADIUS authentication servers used to authenticate DHCP, L2TP, and PPP clients. The servers in the list are also used as RADIUS dynamic-request servers, from which the router accepts and processes RADIUS disconnect requests, CoA requests, and dynamic service activations and deactivations.

Options *ip-address*—IPv4 address.

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

Related Documentation
- Configuring RADIUS Server Parameters for Subscriber Access

boot-file

Syntax boot-file *filename*;

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

Release Information Statement introduced in Junos OS Release 9.0.

Description Set the boot file advertised to DHCP clients. After the client receives an IP address and the boot file location from the DHCP server, the client uses the boot image stored in the boot file to complete DHCP setup. This is equivalent to DHCP option 67.

Options *filename*—Location of the boot file on the boot server. The filename can include a pathname.

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

Related Documentation
- Configuring Address-Assignment Pools
- boot-server on page 64

boot-server

Syntax boot-server (*address* | *hostname*);

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup. This is equivalent to DHCP option 66.

Options ***address***—IPv4 address of a boot server.

hostname—Fully qualified hostname of a boot server.

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

Related Documentation
- Configuring Address-Assignment Pools
- boot-file on page 63

cell-overhead

Syntax cell-overhead;

Hierarchy Level [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

Release Information Statement introduced in Junos OS Release 8.3.

Description Configure the session to use Asynchronous Transfer Mode (ATM)-aware egress shaping on the IQ2 PIC.

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

Related Documentation
- Configuring the PPP Attributes for a Group Profile on page 17
- Configuring PPP Properties for a Client-Specific Profile on page 30

chap-secret

Syntax chap-secret *chap-secret*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the CHAP secret key associated with a peer.

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

Options ***chap-secret***—The secret key associated with a peer.

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

Related Documentation
- Configuring the CHAP Secret for an L2TP Profile on page 25

circuit-id (Address-Assignment Pools)

Syntax circuit-id *value* range *named-range*;

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes option-match option-82]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure the address-assignment pool named-range to use for a particular option 82 Agent Circuit ID value.

Options ***value***—String for the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82) in DHCP packets.

range *named-range*—Name of the address-assignment pool range to use.

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

Related Documentation
- Configuring Address-Assignment Pools

circuit-type (DHCP Local Server)

Syntax circuit-type;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify that the circuit type is concatenated with the username during the subscriber authentication process.

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

Related Documentation
- Using External AAA Authentication Services with DHCP

client

Syntax

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

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

Release Information Statement introduced before Junos OS Release 7.4.
Support for MX Series routers introduced in Junos OS Release 11.4. Not all subordinate statements are supported for L2TP LNS on MX Series routers.

Description Configure the peer identity.

Options ***client-name***—A peer identity. For L2TP clients, you can use a special name to configure a default client. This client enables the LNS to accept any LAC to establish the

session. On M Series routers, use * for the default client configuration. On MX Series routers, use **default**.

The remaining statements are explained separately.

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

Related Documentation
- (For M Series routers) Configuring the L2TP Client on page 23
- (For M Series routers) Configuring Access Profiles for L2TP or PPP Parameters on page 19
- (For MX Series routers) Configuring an L2TP Access Profile on the LNS

client-authentication-algorithm

Syntax client-authentication-algorithm (direct | round-robin);

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

Release Information Statement introduced in Junos OS Release 10.0.

Description Configure the access method the router uses to access RADIUS authentication servers.

Default direct

Options **direct**—Use the direct method.

round-robin—Use the round-robin method.

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

Related Documentation
- Configuring RADIUS Server Parameters for Subscriber Access
- Configuring RADIUS Server Options for Subscriber Access

dhcp-attributes (Address-Assignment Pools)

Syntax

```
dhcp-attributes {
  boot-file filename;
  boot-server (address | hostname);
  dns-server [ ipv6-address ];
  domain-name domain-name;
  grace-period seconds;
  maximum-lease-time seconds;
  name-server [ server-list ];
  netbios-node-type node-type;
  option {
    [ (id-number option-type option-value)
    (id-number array option-type option-value) ];
  }
  option-match {
    option-82 {
      circuit-id value range named-range;
      remote-id value range named-range;
    }
  }
  router [ router-address ];
  server-identifier ip4-address;
  sip-server-address [ ipv6-address ];
  sip-server-domain-name domain-name;
  tftp-server address;
  wins-server [ servers ];
}
```

Hierarchy Level [edit access address-assignment pool *pool-name* family *family*]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure address pools that can be used by different client applications.

The remaining statements are explained separately.

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

Related Documentation

- Address-Assignment Pools Overview
- Configuring Address-Assignment Pools
- Configuring DHCP Client-Specific Attributes

domain-name (Address-Assignment Pools)

Syntax domain-name *domain-name*;

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure the name of the domain in which clients search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.

Options ***domain-name***—Name of the domain.

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

Related Documentation
- Configuring Address-Assignment Pools

drop-timeout

Syntax drop-timeout *milliseconds*;

Hierarchy Level [edit access profile *profile-name* client *client-name* l2tp multilink]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the drop timeout for a multilink bundle.

Options ***milliseconds***—Number of milliseconds for the timeout that is 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 OS 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.)

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

Related Documentation
- Configuring L2TP Properties for a Client-Specific Profile on page 26

encapsulation-overhead

Syntax encapsulation-overhead *bytes*;

Hierarchy Level [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

Release Information Statement introduced in Junos OS Release 8.3.

Description Configure the encapsulation overhead for class-of-service calculations.

Options ***bytes***—The number of bytes used as encapsulation overhead for the session.

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

Related Documentation
- Configuring the PPP Attributes for a Group Profile on page 17
- Configuring PPP Properties for a Client-Specific Profile on page 30

ethernet-port-type-virtual

Syntax ethernet-port-type-virtual;

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Specify the physical port type the router or switch uses to authenticate clients. The router or switch passes a port type of **ethernet** in RADIUS attribute 61 (NAS-Port-Type) by default. This statement specifies a port type of **virtual**.

NOTE: **This statement takes precedence over the nas-port-type statement if you include both statements in the same access profile.**

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

Related Documentation
- Configuring RADIUS Server Options for Subscriber Access
- Configuring RADIUS Server Parameters for Subscriber Access

exclude (RADIUS)

Syntax

```
exclude {
  accounting-authentic [ accounting-on | accounting-off ];
  accounting-delay-time [ accounting-on | accounting-off ];
  accounting-session-id [ access-request | accounting-on | accounting-off | accounting-stop
    ];
  accounting-terminate-cause [ accounting-off ];
  called-station-id [ access-request | accounting-start | accounting-stop ];
  calling-station-id [ access-request | accounting-start | accounting-stop ];
  class [ accounting-start | accounting-stop ];
  dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
  dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
  dhcp-options [ access-request | accounting-start | accounting-stop ];
  downstream-calculated-qos-rate [ access-request | accounting-start | accounting-stop
    ]
  dsl-forum-attributes [ access-request | accounting-start | accounting-stop ]
  event-timestamp [ accounting-on | accounting-off | accounting-start | accounting-stop
    ];
  framed-ip-address [ accounting-start | accounting-stop ];
  framed-ip-netmask [ accounting-start | accounting-stop ];
  input-filter [ accounting-start | accounting-stop ];
  input-gigapackets [ accounting-stop ];
  input-gigawords [ accounting-stop ];
  interface-description [ access-request | accounting-start | accounting-stop ];
  nas-identifier [ access-request | accounting-on | accounting-off | accounting-start |
    accounting-stop ];
  nas-port [ access-request | accounting-start | accounting-stop ];
  nas-port-id [ access-request | accounting-start | accounting-stop ];
  nas-port-type [ access-request | accounting-start | accounting-stop ];
  output-filter [ accounting-start | accounting-stop ];
  output-gigapackets [ accounting-stop ];
  output-gigawords [ accounting-stop ];
  upstream-calculated-qos-rate [ access-request | accounting-start | accounting-stop ];
}
```

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Options **downstream-calculated-qos-rate**, **dsl-forum-attributes**, and **upstream-calculated-qos-rate** introduced in Junos OS Release 11.4.

Description Configure the router or switch to exclude the specified attributes from the specified type of RADIUS message.

Not all attributes are available in all types of RADIUS messages. By default, the router or switch includes the specified attributes in RADIUS Access-Request, Acct-On, Acct-Off, Acct-Start, and Acct-Stop messages.

Options RADIUS attribute type—RADIUS attribute or Juniper Networks VSA number and name.

- **accounting-authentic**—RADIUS attribute 45, Acct-Authentic.

- **accounting-delay-time**—RADIUS attribute 41, Acct-Delay-Time.
- **accounting-session-id**—RADIUS attribute 44, Acct-Session-Id.
- **accounting-terminate-cause**—RADIUS attribute 49, Acct-Terminate-Cause.
- **called-station-id**—RADIUS attribute 30, Called-Station-Id.
- **calling-station-id**—RADIUS attribute 31, Calling-Station-Id.
- **class**—RADIUS attribute 25, Class.
- **dhcp-gi-address**—Juniper VSA 26-57, DHCP-GI-Address.
- **dhcp-mac-address**—Juniper VSA 26-56, DHCP-MAC-Address.
- **dhcp-options**—Juniper VSA 26-55, DHCP-Options.
- **downstream-calculated-qos-rate**—Juniper VSA 26-141
- **dsl-forum-attributes**—DSL Forum VSA as described in RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*
- **event-timestamp**—RADIUS attribute 55, Event-Timestamp.
- **framed-ip-address**—RADIUS attribute 8, Framed-IP-Address.
- **framed-ip-netmask**—RADIUS attribute 9, Framed-IP-Netmask.
- **input-filter**—Juniper VSA 26-10, Ingress-Policy-Name.
- **input-gigapackets**—Juniper VSA 26-42, Acct-Input-Gigapackets.
- **input-gigawords**—RADIUS attribute 52, Acct-Input-Gigawords.
- **interface-description**—Juniper VSA 26-53, Interface-Desc.
- **nas-identifier**—RADIUS attribute 32, NAS-Identifier.
- **nas-port**—RADIUS attribute 5, NAS-Port.
- **nas-port-id**—RADIUS attribute 87, NAS-Port-Id.
- **nas-port-type**—RADIUS attribute 61, NAS-Port-Type.
- **output-filter**—Juniper VSA 26-11, Egress-Policy-Name.
- **output-gigapackets**—Juniper VSA 25-43, Acct-Output-Gigapackets.
- **output-gigawords**—RADIUS attribute 53, Acct-Output-Gigawords.
- **upstream-calculated-qos-rate**—Juniper VSA 26-142

RADIUS message type

- **access-request**—RADIUS Access-Accept messages.
- **accounting-off**—RADIUS Accounting-Off messages.
- **accounting-on**—RADIUS Accounting-On messages.
- **accounting-start**—RADIUS Accounting-Start messages.
- **accounting-stop**—RADIUS Accounting-Stop messages.

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

Related Documentation
- Configuring RADIUS Server Parameters for Subscriber Access

fragment-threshold

Syntax
fragment-threshold *bytes*;

Hierarchy Level
[edit access profile *profile-name* client *client-name* l2tp multilink]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure the fragmentation threshold for a multilink bundle.

Options
bytes—The maximum number of bytes in a packet. If a packet exceeds the fragmentation threshold, the Junos OS fragments it into two or more multilink fragments.

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

Related Documentation
- Configuring L2TP Properties for a Client-Specific Profile on page 26
- multilink on page 92

framed-ip-address

Syntax
framed-ip-address *address*;

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Specify a framed IP address.

Options
address—The IP version 4 (IPv4) prefix.

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

Related Documentation
- Configuring PPP Properties for a Client-Specific Profile on page 30

framed-pool

Syntax framed-pool *framed-pool*;

Hierarchy Level [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the address pool.

Options ***framed-pool***—References a configured address pool.

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

Related Documentation
- Configuring the PPP Attributes for a Group Profile on page 17
- Configuring PPP Properties for a Client-Specific Profile on page 30

grace-period

Syntax grace-period *seconds*;

Hierarchy Level [edit access address-assignment pool *pool-name* family (inet | inet6) dhcp-attributes]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure the amount of time that the client retains the address lease after the lease expires. The address cannot be reassigned to another client during the grace period.

Options ***seconds***—Number of seconds the lease is retained.

Range: 0 through 4,294,967,295 seconds

Default: 0 (no grace period)

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

Related Documentation
- Configuring Address-Assignment Pools

group-profile (Associating with Client)

Syntax group-profile *profile-name*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Associate a group profile with a client.

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

Options ***profile-name***—Name assigned to the group profile.

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

Related Documentation

- Referencing the Group Profile from the L2TP Profile on page 26

group-profile (Group Profile)

Syntax

```
group-profile profile-name {
  l2tp {
    interface-id interface-id;
    lcp-renegotiation;
    local-chap;
    maximum-sessions-per-tunnel number;
  }
  ppp {
    cell-overhead;
    encapsulation-overhead bytes;
    framed-pool pool-id;
    idle-timeout seconds;
    interface-id interface-id;
    keepalive seconds;
    ppp-options {
      chap;
      pap;
    }
    primary-dns primary-dns;
    primary-wins primary-wins;
    secondary-dns secondary-dns;
    secondary-wins secondary-wins;
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS Release 7.4.
(MX Series routers only) The **ppp-options** stanza introduced in Junos OS Release 11.4.

Description Configure the group profile.

Only the **idle-timeout** statement, the **keepalive** statement, and the **ppp-options** stanza are supported for L2TP LNS on MX Series routers.

Options *profile-name*—Name assigned to the group profile.

The remaining statements are explained separately.

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

Related Documentation

- (M Series routers) Configuring the Group Profile for Defining L2TP Attributes on page 16
- (MX Series routers) Configuring a User Group Profile for L2TP LNS

hardware-address

Syntax hardware-address *mac-address*;

Hierarchy Level [edit access address-assignment pool *pool-name* family (inet | inet6) host *hostname*]

Release Information Statement introduced in Junos OS Release 9.0.

Description Specify the MAC address of the client. This is the hardware address that identifies the client on the network.

Options ***mac-address***—MAC address of the client.

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

Related Documentation
- Configuring Address-Assignment Pools

host (Address-Assignment Pools)

Syntax
```
host hostname {
    hardware-address mac-address;
    ip-address ip-address;
}
```

Hierarchy Level [edit access address-assignment pool *pool-name* family (inet | inet6)]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure a static binding for the specified client.

Options ***hostname***—Name of the client.

The remaining statements are explained separately.

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

Related Documentation
- Address-Assignment Pools Overview
- Configuring Address-Assignment Pools

idle-timeout

Syntax idle-timeout *seconds*;

Hierarchy Level [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Support for L2TP LNS on MX Series routers introduced in Junos OS Release 11.4.

Description Configure the idle timeout for a user. The router might consider a PPP session to be idle because of the following reasons:

- There is no ingress traffic on the PPP session.
- There is no egress traffic.
- There is neither ingress or egress traffic on the PPP session.
- There is no ingress or egress PPP control traffic. This is applicable only if keepalives are enabled.

Options ***seconds***—Number of seconds a user can remain idle before the session is terminated.

Range: 0 through 4,294,967,295 seconds

Default: 0

NOTE: **The edit access hierarchy is not available on QFabric switches.**

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

Related Documentation

- (M Series routers) Configuring the PPP Attributes for a Group Profile on page 17
- (M Series routers) Configuring PPP Properties for a Client-Specific Profile on page 30
- (MX Series routers) Configuring a User Group Profile for L2TP LNS

ignore

Syntax

```
ignore {
  framed-ip-netmask;
  input-filter;
  logical-system-routing-instance;
  output-filter;
}
```

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the router or switch to ignore the specified attributes in RADIUS Access-Accept messages. By default, the router or switch processes the attributes it receives from the external server.

Options

framed-ip-netmask—Ignore Framed-IP-Netmask (RADIUS attribute 9).

input-filter—Ignore Ingress-Policy-Name (VSA 26-10).

logical-system-routing-instance—Ignore Virtual-Router (VSA 26-1).

output-filter—Ignore Egress-Policy-Name (VSA 26-11).

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

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access

ike

Syntax

```
ike {
  allowed-proxy-pair {
    remote remote-proxy-address local local-proxy-address;
  }
  pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
  ike-policy policy-name;
  interface-id string-value;
}
```

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

Release Information Statement introduced in Junos OS Release 7.4.
ike-policy statement introduced in Junos OS Release 8.2.

Description Configure an IKE access profile.

The remaining statements are explained separately.

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

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

Related Documentation

- Configuring an IKE Access Profile on page 22

ike-policy

Syntax ike-policy *policy-name*;

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

Release Information Statement introduced in Junos OS Release 8.2.

Description Specify the IKE policy used to authenticate dynamic peers during IKE negotiation.

Options ***policy-name***—The name of an IKE policy configured at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level. The IKE policy defines either the local digital certificate or the pre-shared key used for IKE authentication with dynamic peers. For more information about how to configure the IKE policy, see the *Junos OS Services Interfaces Configuration Guide*.

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

Related Documentation

- Configuring an IKE Access Profile on page 22
- *Junos IPsec Feature Guide*
- *Junos OS Services Interfaces Configuration Guide*

immediate-update

Syntax immediate-update;

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the router or switch to send an Acct-Update message to the RADIUS accounting server on receipt of a response (for example, an ACK or timeout) to the Acct-Start message.

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

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access
- Configuring Per-Subscriber Session Accounting

initiate-dead-peer-detection

Syntax initiate-dead-peer-detection;

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

Release Information Statement introduced in Junos OS Release 8.3.

Description Detect inactive peers on dynamic IPsec tunnels.

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

Related Documentation
- Configuring an IKE Access Profile on page 22

interface-description-format

Syntax
```
interface-description-format {
  exclude-adapter;
  exclude-sub-interface;
}
```

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Options **exclude-adapter** and **exclude-sub-interface** introduced in Junos OS Release 10.4.

Description Specify the information that is excluded from the interface description that the device passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). By default, the device includes both the subinterface and the adapter in the interface description.

Options **exclude-adapter**—Exclude the adapter from the interface description.

exclude-sub-interface—Exclude the subinterface from the interface description.

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

Related Documentation
- Configuring RADIUS Server Options for Subscriber Access
- RADIUS Server Options for Subscriber Access

interface-id

Syntax interface-id *interface-id*;

Hierarchy Level [edit access group-profile *profile-name* l2tp],
[edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ike],
[edit access profile *profile-name* client *client-name* l2tp],
[edit access profile *profile-name* client *client-name* ppp]

Release Information Statement introduced before Junos OS Release 7.4.
(MX Series routers only) Support at the **[edit ... l2tp]** hierarchy levels for L2TP LNS introduced in Junos OS Release 11.4.

Description Configure the interface identifier.

Options *interface-id*—The identifier for the interface representing a Layer 2 Tunneling Protocol (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 OS Services Interfaces Configuration Guide*.

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

Related Documentation

- (M Series routers) Configuring L2TP for a Group Profile on page 17
- (M Series routers) Configuring the PPP Attributes for a Group Profile on page 17
- (M Series routers) Configuring L2TP Properties for a Client-Specific Profile on page 26
- (M Series routers) Configuring PPP Properties for a Client-Specific Profile on page 30
- (M Series routers) Configuring an IKE Access Profile on page 22
- (MX Series routers) Configuring an L2TP Access Profile on the LNS

ip-address

Syntax ip-address *ip-address*;

Hierarchy Level [edit access address-assignment pool *pool-name* family inet host *hostname*]

Release Information Statement introduced in Junos OS Release 9.0.

Description Specify the reserved IP address assigned to the client.

Options ***ip-address***—IP version 4 (IPv4) address.

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

Related Documentation
- Configuring Address-Assignment Pools
- Configuring Static Address Assignment

keepalive

Syntax keepalive *seconds*;

Hierarchy Level [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

Release Information Statement introduced before Junos OS Release 7.4.
Support for L2TP LNS on MX Series routers introduced in Junos OS Release 11.4.

Description Configure the keepalive interval for an L2TP tunnel.

Options ***seconds***—The time period that must elapse before the Junos OS checks the status of the Point-to-Point Protocol (PPP) session by sending an echo request to the peer.

For L2TP on MX Series routers, the minimum recommended interval is 30 seconds. A value of 0 disables generation of keepalive messages from the LNS.

Range: 0 through 32,767 seconds

Default: 30 seconds

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

Related Documentation
- (M Series routers) Configuring the PPP Attributes for a Group Profile on page 17
- (M Series routers) Configuring PPP Properties for a Client-Specific Profile on page 30
- (MX Series routers) Configuring a User Group Profile for L2TP LNS

keepalive-retries

Syntax keepalive-retries *number-of-retries*;

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

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure the number of retry attempts for checking the keepalive status of a Point-to-Point (PPP) protocol session. Configure this setting to reduce the detection time for PPP client session timeouts or failures if you have configured the keepalive timeout interval (using the **keepalive** statement).

Options *number-of-retries*—The maximum number of retries the L2TP network server (LNS) attempts by sending LCP echo requests to the peer to check the keepalive status of the PPP session. If there is no response from the PPP client within the specified number of retries, the PPP session is considered to have timed out.

Range: 3 through 32,767 times

Default: 10 times

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

Related Documentation

- Configuring PPP Properties for a Client-Specific Profile on page 30
- keepalive on page 85

l2tp (Group Profile)

Syntax

```
l2tp {
  interface-id interface-id;
  lcp-renegotiation;
  local-chap;
  maximum-sessions-per-tunnel number;
}
```

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the Layer 2 Tunneling Protocol for a group profile.

The remaining statements are explained separately.

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

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

Related Documentation

- Configuring L2TP for a Group Profile on page 17

l2tp (Profile)

Syntax

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

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the L2TP properties for a profile.

The remaining statements are explained separately.

NOTE: Only the interface-id, lcp-renegotiation, maximum-sessions-per-tunnel, and shared-secret statements are supported for L2TP LNS on MX Series routers.

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

Related Documentation

- Configuring L2TP Properties for a Client-Specific Profile on page 26

lcp-renegotiation

Syntax lcp-renegotiation;

Hierarchy Level [edit access group-profile *profile-name* l2tp],
[edit access profile *profile-name* client *client-name* l2tp]

Release Information Statement introduced before Junos OS Release 7.4.
(MX Series routers only) Support at the **[edit access profile *profile-name* client *client-name* l2tp]** hierarchy level for L2TP LNS introduced in Junos OS Release 11.4.

Description Configure the L2TP network server (LNS) so it renegotiates the link control protocol (LCP) with the PPP client. When LCP renegotiation is disabled, LNS uses the pre-negotiated LCP parameters between the L2TP access concentrator (LAC) and PPP client to set up the session. When LCP renegotiation is enabled, authentication is also renegotiated.

NOTE: **This statement is not supported at the [edit access group-profile l2tp] hierarchy level for L2TP LNS on MX Series routers.**

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

Related Documentation

- (M Series routers)Configuring L2TP for a Group Profile on page 17
- (M Series routers)Configuring L2TP Properties for a Client-Specific Profile on page 26
- (MX Series routers) Configuring an L2TP Access Profile on the LNS

local-chap

Syntax local-chap;

Hierarchy Level [edit access group-profile *profile-name* l2tp],
[edit access profile *profile-name* client *client-name* l2tp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the Junos OS so that the LNS ignores proxy authentication attribute-value pairs (AVPs) from the L2TP access concentrator (LAC) and reauthenticates the PPP client using a Challenge Handshake Authentication Protocol (CHAP) challenge. When you do this, the LNS directly authenticates the PPP client.

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

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

Related Documentation
- Configuring L2TP for a Group Profile on page 17
- Configuring L2TP Properties for a Client-Specific Profile on page 26

maximum-lease-time

Syntax maximum-lease-time *seconds*;

Hierarchy Level [edit access address-assignment pool *pool-name* family (inet | inet6) dhcp-attributes]

Release Information Statement introduced in Junos OS Release 9.0.

Description Specify the maximum length of time, in seconds, that the lease is held for a client if the client does not renew the lease. This is equivalent to DHCP option 51.

Options ***seconds***—Maximum number of seconds the lease can be held.
Range: 30 through 4,294,967,295 seconds
Default: 86,400 (24 hours)

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

Related Documentation
- Configuring Address-Assignment Pools

maximum-sessions-per-tunnel

Syntax maximum-sessions-per-tunnel *number*;

Hierarchy Level [edit access group-profile l2tp],
[edit access profile *profile-name* client *client-name* l2tp]

Release Information Statement introduced before Junos OS Release 7.4.
Support at the **[edit access profile *profile-name* client *client-name* l2tp]** hierarchy level for L2TP LNS on MX Series routers introduced in Junos OS Release 11.4.

Description Configure the maximum sessions for a Layer 2 tunnel.

NOTE: **This statement is not supported at the [edit access group-profile l2tp] hierarchy level for L2TP LNS on MX Series routers.**

Options ***number***—Maximum number of sessions for a Layer 2 tunnel.

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

Related Documentation

- (M Series routers) Configuring L2TP for a Group Profile on page 17
- (M Series routers) Configuring L2TP Properties for a Client-Specific Profile on page 26
- (MX Series routers) Configuring an L2TP Access Profile on the LNS

multilink

Syntax

```
multilink {
  drop-timeout milliseconds;
  fragment-threshold bytes;
}
```

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure Multilink PPP for Layer 2 Tunneling Protocol (L2TP).

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

Options The 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 Properties for a Client-Specific Profile on page 26

name-server

Syntax name-server [*server-names*];

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure one or more Domain Name System (DNS) name servers available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

Options ***server-names***—IP addresses of the domain name servers, listed in order of preference.

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

Related Documentation

- Configuring Address-Assignment Pools

nas-identifier

Syntax nas-identifier *identifier-value*;

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests.

Options ***identifier-value***—String to use for authentication and accounting requests.

Range: 1 through 64 characters

Required Privilege Level admin—To view this statement in the configuration.
admin–control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access
- Configuring RADIUS Server Parameters for Subscriber Access

nas-port-extended-format

Syntax

```
nas-port-extended-format {
  adapter-width width;
  port-width width;
  slot-width width;
  stacked-vlan-width width;
  vlan-width width;
}
```

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute.

Options

adapter-width *width*—Number of bits in the adapter field.

port-width *width*—Number of bits in the port field.

slot-width *width*—Number of bits in the slot field.

stacked-vlan-width *width*—Number of bits in the SVLAN ID field.

vlan-width *width*—Number of bits in the VLAN ID field.

NOTE: The total of the widths must not exceed 32 bits, or the configuration will fail.

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

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access
- Configuring RADIUS Server Parameters for Subscriber Access

netbios-node-type

Syntax netbios-node-type *node-type*;

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

Release Information Statement introduced in Junos OS Release 9.0.

Description Specify the NetBIOS node type. This is equivalent to DHCP option 46.

Options ***node-type***—One of the following node types:

- **b-node**—Broadcast node
- **h-node**—Hybrid node
- **m-node**—Mixed node
- **p-node**—Peer-to-peer node

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

Related Documentation

- Configuring Address-Assignment Pools

network

Syntax network *ip-prefix</prefix-length>*;

Hierarchy Level [edit access address-assignment pool *pool-name* family inet]

Release Information Statement introduced in Junos OS Release 9.0.
Support for LNS on MX Series routers introduced in Junos OS Release 11.4.

Description Configure subnet information for an IPv4 address-assignment pool.

Options

- ***ip-prefix***—IP version 4 address or prefix value.
- ***prefix-length***—(Optional) Subnet mask.

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

Related Documentation

- Configuring Address-Assignment Pools

option

Syntax

```
option {
  [ (id-number option-type option-value)
  (id-number array option-type option-value) ];
}
```

Hierarchy Level [edit access address-assignment pool *pool-name* family (inet | inet6) dhcp-attributes]

Release Information Statement introduced in Junos OS Release 9.0.

Description Specify user-defined options that are added to client packets.

Options

array—An option can include an array of option types.

id-number—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.

option-type—Any of the following types: byte, byte-stream, flag, integer, ip-address, short, string, unsigned-integer, or unsigned-short.

option-value—Value associated with an option. The option value must be compatible with the option type (for example, an On or Off value for a flag type).

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

Related Documentation

- Configuring Address-Assignment Pools

option-82 (Address-Assignment Pools)

Syntax

```
option-82 {
  circuit-id value range named-range;
  remote-id value range named-range;
}
```

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes option-match]

Release Information Statement introduced in Junos OS Release 9.0.

Description Specify the list of option 82 suboption match criteria used to select the named address range used for the client. The server matches the option 82 value in the user PDU to the specified option 82 match criteria and uses the named address range associated with the string.

The remaining statements are explained separately.

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

Related Documentation
- Configuring Address-Assignment Pools

option-match

Syntax

```
option-match {
  option-82 {
    circuit-id value range named-range;
    remote-id value range named-range;
  }
}
```

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

Release Information Statement introduced in Junos OS Release 9.0.

Description Specify a list of match criteria used to determine which named address range in the address-assignment pool to use. The extended DHCP local server matches this information to the match criteria specified in the client PDUs. For example, for option 82 match criteria, the server matches the option 82 value in the user PDU to the specified option 82 string and uses the named range associated with the string.

The remaining statements are explained separately.

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

Related Documentation
- Configuring Address-Assignment Pools

options

Syntax

```
options {
  accounting-session-id-format (decimal | description);
  client-accounting-algorithm (direct | round-robin);
  client-authentication-algorithm (direct | round-robin);
  ethernet-port-type-virtual;
  interface-description-format {
    exclude-adapter;
    exclude-sub-interface;
  }
  juniper-dsl-attributes;
  nas-identifier identifier-value;
  nas-port-extended-format {
    adapter-width width;
    port-width width;
    slot-width width;
    stacked-vlan-width width;
    vlan-width width;
  }
  nas-port-id-delimiter delimiter-character;
  nas-port-id-format {
    agent-circuit-id;
    agent-remote-id;
    interface-description;
    nas-identifier;
  }
  nas-port-type {
    ethernet {
      port-type;
    }
  }
  revert-interval interval;
  vlan-nas-port-stacked-format;
}
```

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the options used by RADIUS authentication and accounting servers.

The remaining statements are explained separately.

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

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access
- RADIUS Server Options for Subscriber Access

order

Syntax order [*accounting-method*];

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Set the order in which the Junos OS tries different accounting methods for client activity. When a client logs in, the software tries the accounting methods in the specified order.

Options ***accounting-method***—One or more accounting methods. When a client logs in, the software tries the accounting methods in the following order, from first to last. The only valid value is **radius** for RADIUS accounting.

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

Related Documentation
- Configuring Authentication and Accounting Parameters for Subscriber Access

pap-password

Syntax pap-password *password*;

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

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the Password Authentication Protocol (PAP) password.

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

Options ***password***—PAP password.

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

Related Documentation
- Configuring the PAP Password for an L2TP Profile on page 29

pool (Address-Assignment Pools)

Syntax

```
pool pool-name {
  family family {
    dhcp-attributes {
      [ protocol-specific attributes ]
    }
    host hostname {
      hardware-address mac-address;
      ip-address ip-address;
    }
    network ip-prefix/<prefix-length>;
    prefix ipv6-prefix;
    range range-name {
      high upper-limit;
      low lower-limit;
      prefix-length prefix-length;
    }
  }
  link pool-name;
}
```

Hierarchy Level [edit access address-assignment]

Release Information Statement introduced in Junos OS Release 9.0.
Support for LNS on MX Series routers introduced in Junos OS Release 11.4. Not all subordinate statements are supported for L2TP LNS on MX Series routers.

Description Configure the name of an address-assignment pool.

Options ***pool-name***—Name assigned to the address-assignment pool.

The remaining statements are explained separately.

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

Related Documentation

- Address-Assignment Pools Overview
- Configuring Address-Assignment Pools

port

Syntax port *port-number*;

Hierarchy Level [edit access radius-server*server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the port number on which to contact the RADIUS server.

Options ***port-number***—Port number on which to contact the RADIUS server.

Default: 1812 (as specified in RFC 2865)

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

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers
- Configuring Authentication and Accounting Parameters for Subscriber Access

ppp (Group Profile)

Syntax

```
ppp {
  cell-overhead;
  encapsulation-overhead bytes;
  framed-pool framed-pool;
  idle-timeout seconds;
  interface-id interface-id;
  keepalive seconds;
  ppp-options {
    chap;
    pap;
  }
  primary-dns primary-dns;
  primary-wins primary-wins;
  secondary-dns secondary-dns;
  secondary-wins secondary-wins;
}
```

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

Release Information Statement introduced before Junos OS Release 7.4.
ppp-options statement introduced in Junos OS Release 11.4.

Description Configure PPP properties for a group profile.

The remaining statements are explained separately.

NOTE: Only the **idle-timeout** statement, the **keepalive** statement, and the **ppp-options** stanza are supported for L2TP LNS on MX Series routers.

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

Related Documentation

- (M Series routers) Configuring the PPP Attributes for a Group Profile on page 17
- (MX Series routers) Configuring a User Group Profile for L2TP LNS

ppp (Profile)

Syntax

```
ppp {
  cell-overhead;
  encapsulation-overhead bytes;
  framed-ip-address address;
  framed-pool framed-pool;
  idle-timeout seconds;
  interface-id interface-id;
  keepalive seconds;
  primary-dns primary-dns;
  primary-wins primary-wins;
  secondary-dns secondary-dns;
  secondary-wins secondary-wins;
}
```

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure PPP properties for a client profile.

The remaining statements are explained separately.

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

Related Documentation

- Configuring PPP Properties for a Client-Specific Profile on page 30

ppp-authentication

Syntax ppp-authentication (chap | pap);

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure PPP authentication.

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

Options
- **chap**—Challenge Handshake Authentication Protocol.
- **pap**—Password Authentication Protocol.

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

Related Documentation
- Configuring L2TP Properties for a Client-Specific Profile on page 26

ppp-profile

Syntax ppp-profile *profile-name*;

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

Release Information Statement introduced in Junos OS Release 7.4.

Description Specify the profile used to validate PPP session requests through L2TP tunnels.

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

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

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

Related Documentation
- Configuring RADIUS Authentication for an L2TP Client and Profile on page 44

pre-shared-key

Syntax pre-shared-key (ascii-text *character-string* | hexadecimal *hexadecimal-digits*);

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

Release Information Statement introduced in Junos OS Release 7.4.

Description Configure the key used to authenticate a dynamic peer during IKE phase 1 negotiation. Specify the key in either ASCII or hexadecimal format.

Options **ascii-text *character-string***—Authentication key in ASCII format.

hexadecimal *hexadecimal-digits*—Authentication key in hexadecimal format.

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

Related Documentation
- Configuring an IKE Access Profile on page 22

primary-dns

Syntax primary-dns *primary-dns*;

Hierarchy Level [edit access group-profile *profile-name* client *client-name* ppp],
[edit access profile *profile-name* ppp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the primary Domain Name System (DNS) server.

Options ***primary-dns***—An IPv4 address.

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

Related Documentation
- Configuring the PPP Attributes for a Group Profile on page 17
- Configuring PPP Properties for a Client-Specific Profile on page 30

primary-wins

Syntax primary-wins *primary-wins*;

Hierarchy Level [edit access group-profile *profile-name* client *client-name* ppp],
[edit access profile *profile-name* ppp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the primary Windows Internet name server.

Options ***primary-wins***—An IPv4 address.

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

Related Documentation

- Configuring the PPP Attributes for a Group Profile on page 17
- Configuring PPP Properties for a Client-Specific Profile on page 30

profile

Syntax

```
profile profile-name {
  accounting {
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    coa-immediate-update;
    coa-no-override service-class-attribute;
    duplication;
    immediate-update;
    order [ accounting-method ];
    statistics (time | volume-time);
    update-interval minutes;
    }
  authentication-order [ authentication-methods ];
  client client-name {
    chap-secret chap-secret;
    group-profile profile-name;
    ike {
      allowed-proxy-pair {
        remote remote-proxy-address local local-proxy-address;
      }
      pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
      ike-policy policy-name;
      interface-id string-value;
    }
    l2tp {
      interface-id interface-id;
      lcp-renegotiation;
      local-chap;
      maximum-sessions-per-tunnel number;
      multilink {
        drop-timeout milliseconds;
        fragment-threshold bytes;
      }
      ppp-authentication (chap | pap);
      ppp-profile profile-name;
      shared-secret shared-secret;
    }
    pap-password pap-password;
    ppp {
      cell-overhead;
      encapsulation-overhead bytes;
      framed-ip-address ip-address;
      framed-pool framed-pool;
      idle-timeout seconds;
      interface-id interface-id;
      keepalive seconds;
      primary-dns primary-dns;
      primary-wins primary-wins;
      secondary-dns secondary-dns;
      secondary-wins secondary-wins;
    }
    user-group-profile profile-name;
```

```
}
radius {
    accounting-server [ ip-address ];
    authentication-server [ ip-address ];
    options {
        accounting-session-id-format (decimal | description);
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        ethernet-port-type-virtual;
        interface-description-format {
            exclude-adapter;
            exclude-sub-interface;
        }
        juniper-dsl-attributes;
        nas-identifier identifier-value;
        nas-port-extended-format {
            adapter-width width;
            port-width width;
            slot-width width;
            stacked-vlan-width width;
            vlan-width width;
        }
        nas-port-id-delimiter delimiter-character;
        nas-port-id-format {
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            nas-identifier;
        }
        nas-port-type {
            ethernet {
                port-type;
            }
        }
        revert-interval interval;
        vlan-nas-port-stacked-format;
    }
    attributes {
        exclude {
            ...
        }
        ignore {
            framed-ip-netmask;
            input-filter;
            logical-system:routing-instance;
            output-filter;
        }
    }
}
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
    max-outstanding-requests value;
```

```
    source-address source-address;
    timeout seconds;
  }
  service {
    accounting-order (activation-protocol | radius);
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure PPP CHAP, or a profile and its subscriber access, L2TP, or PPP properties.

Options *profile-name*—Name of the profile.

For CHAP, the name serves as the mapping between peer identifiers and CHAP secret keys. This entity is queried for the secret key whenever a CHAP challenge or response is received.

The remaining statements are explained separately.

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

Related Documentation

- Configuring the PPP Authentication Protocol on page 8
- Configuring Access Profiles for L2TP or PPP Parameters on page 19
- Configuring L2TP Properties for a Client-Specific Profile on page 26
- Configuring PPP Properties for a Client-Specific Profile on page 30
- Configuring Service Accounting with JSRC
- AAA Service Framework Overview
- show network-access aaa statistics
- clear network-access aaa statistics on page 128

radius (Access Profile)

Syntax

```
radius {
    accounting-server [ ip-address ];
    attributes {
        exclude
            ...
        }
        ignore {
            framed-ip-netmask;
            input-filter;
            logical-system-routing-instance;
            output-filter;
        }
    }
    authentication-server [ ip-address ];
    options {
        accounting-session-id-format (decimal | description);
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        ethernet-port-type-virtual;
        interface-description-format {
            exclude-adapter;
            exclude-sub-interface;
        }
        juniper-dsl-attributes;
        nas-identifier identifier-value;
        nas-port-extended-format {
            adapter-width width;
            port-width width;
            slot-width width;
            stacked-vlan-width width;
            vlan-width width;
        }
        nas-port-id-delimiter delimiter-character;
        nas-port-id-format {
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            nas-identifier;
        }
        nas-port-type {
            ethernet {
                port-type;
            }
        }
        revert-interval interval;
        vlan-nas-port-stacked-format;
    }
}
```

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

Release Information Statement introduced in Junos OS Release 9.1.

Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.

The remaining statements are explained separately.

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

Related Documentation
- Configuring RADIUS Server Parameters for Subscriber Access
- RADIUS Server Options for Subscriber Access

radius-disconnect

Syntax

```
radius-disconnect {
  client-address {
    secret password;
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure a disconnect server that listens on a configured User Datagram Protocol (UDP) port for disconnect messages from a configured client and processes these disconnect messages.

Options ***client-address***—A valid IP address configured on one of the router interfaces.

The remaining statements are explained separately.

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

Related Documentation
- Configuring the RADIUS Disconnect Server for L2TP on page 43

radius-disconnect-port

Syntax radius-disconnect-port *port-number*;

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify a port number on which to contact the RADIUS disconnect server. Most RADIUS servers use port number 1700.

Options ***port-number***—The server port to which disconnect requests from the RADIUS client are sent. The L2TP network server, which accepts these disconnect requests, is the server.

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

The remaining statements are explained separately.

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

Related Documentation

- Configuring the RADIUS Disconnect Server for L2TP on page 43

radius-server

Syntax

```
radius-server server-address {
  accounting-port port-number;
  port port-number;
  retry attempts;
  routing-instance routing-instance-name;
  secret password;
  max-outstanding-requests value;
  source-address source-address;
  timeout seconds;
}
```

Hierarchy Level

[edit access],
[edit access profile *profile-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure RADIUS for subscriber access management, L2TP, or PPP.

To configure multiple RADIUS servers, include multiple **radius-server** statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

Options

server-address—Address of the RADIUS authentication server.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring RADIUS Authentication for L2TP on page 37
- Configuring the PPP Authentication Protocol on page 8
- Configuring RADIUS Authentication
- Configuring Authentication and Accounting Parameters for Subscriber Access
- show network-access aaa statistics
- clear network-access aaa statistics on page 128

range (Address-Assignment Pools)

Syntax

```
range range-name {
    high upper-limit;
    low lower-limit;
    prefix-length prefix-length;
}
```

Hierarchy Level [edit access address-assignment pool *pool-name* family (inet | inet6)]

Release Information
Statement introduced in Junos OS Release 9.0.
IPv6 support introduced in Junos OS Release 10.0.
Support for LNS on MX Series routers introduced in Junos OS Release 11.4.

Description Configure a named range of IPv4 addresses or IPv6 prefixes, used within an address-assignment pool.

Options

high *upper-limit*—Upper limit of an address range or IPv6 prefix range.

low *lower-limit*—Lower limit of an address range or IPv6 prefix range.

prefix-length *prefix-length*—Assigned length of the IPv6 prefix.

range-name—Name assigned to the range of IPv4 addresses or IPv6 prefixes.

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

Related Documentation

- Address-Assignment Pools Overview
- Configuring Address-Assignment Pools

remote-id

Syntax remote-id *value* range *named-range*;

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes option-match option-82]

Release Information Statement introduced in Junos OS Release 9.0.

Description Specify the address-assignment pool named range to use based on the particular option 82 Agent Remote ID value.

Options range ***named-range***—Name of the address-assignment pool range to use.

value—String for Agent Remote ID suboption (suboption 2) of the DHCP relay agent information option (option 82) in DHCP packets.

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

Related Documentation

- Configuring Address-Assignment Pools

retry

Syntax retry *attempts*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the number of times that the router or switch is allowed to attempt to contact a RADIUS authentication or accounting server.

Options ***attempts***—Number of times that the router is allowed to attempt to contact a RADIUS server.

Range: 1 through 10

Default: 3

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

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access
- Configuring Router or Switch Interaction with RADIUS Servers
- Example: Configuring CHAP Authentication with RADIUS on page 9
- Configuring RADIUS Authentication for L2TP on page 37
- timeout on page 122

revert-interval

Syntax revert-interval *interval*;

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the amount of time the router or switch waits after a server has become unreachable. The router or switch rechecks the connection to the server when the specified interval expires. If the server is then reachable, it is used in accordance with the order of the server list.

Options ***interval***—Amount of time to wait.

Range: 0 through 4294967295 seconds

Default: 60 seconds

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

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access
- Configuring Authentication and Accounting Parameters for Subscriber Access

router (Address-Assignment Pools)

Syntax router [*router-address*];

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

Release Information Statement introduced in Junos OS Release 9.0.

Description Specify one or more routers located on the client's subnet. This statement is the equivalent of DHCP option 3.

Options ***router-address***—IP address of one or more routers.

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

Related Documentation

- Configuring Address-Assignment Pools

routing-instance

Syntax routing-instance *routing-instance-name*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the routing instance used to send RADIUS packets to the RADIUS server.

Options ***routing-instance-name***—Routing instance name.

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

Related Documentation
- Configuring the PPP Authentication Protocol on page 8
- Configuring Authentication and Accounting Parameters for Subscriber Access

secondary-dns

Syntax secondary-dns *secondary-dns*;

Hierarchy Level [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the secondary DNS server.

Options ***secondary-dns***—An IPv4 address.

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

Related Documentation
- Configuring the PPP Attributes for a Group Profile on page 17
- Configuring PPP Properties for a Client-Specific Profile on page 30

secondary-wins

Syntax secondary-wins *secondary-wins*;

Hierarchy Level [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the secondary Windows Internet name server.

Options ***secondary-wins***—An IPv4 address.

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

Related Documentation

- Configuring the PPP Attributes for a Group Profile on page 17
- Configuring PPP Properties for a Client-Specific Profile on page 30

secret

Syntax secret *password*;

Hierarchy Level [edit access profile *profile-name* radius-server *server-address*],
[edit access radius-disconnect *client-address*],
[edit access radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the password to use with the RADIUS server. The secret password used by the local router or switch must match that used by the server.

Options ***password***—Password to use; it can include spaces if the character string is enclosed in quotation marks.

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

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access
- Configuring Router or Switch Interaction with RADIUS Servers
- Example: Configuring CHAP Authentication with RADIUS on page 9
- Configuring RADIUS Authentication for L2TP on page 37
- Configuring the RADIUS Disconnect Server for L2TP on page 43

shared-secret

Syntax shared-secret *shared-secret*;

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

Release Information Statement introduced in Junos OS Release 7.4.
Support for MX Series routers introduced in Junos OS Release 11.4.

Description Configure the shared secret.

Options ***shared-secret***—The shared secret key for authenticating the peer.

Required Privilege Level admin—To view this statement in the configuration.
admin–control—To add this statement to the configuration.

Related Documentation
- (M Series routers) Configuring L2TP Properties for a Client-Specific Profile on page 26
- (MX Series routers) Configuring an L2TP Access Profile on the LNS

source-address

Syntax source-address *source-address*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address.

Options ***source-address***—Valid IPv4 address configured on one of the router or switch interfaces. On M Series routers only, the source address can be an IPv6 address and the UDP source port is 514.

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

Related Documentation
- Configuring Router or Switch Interaction with RADIUS Servers
- Configuring Authentication and Accounting Parameters for Subscriber Access
- Example: Configuring CHAP Authentication with RADIUS on page 9
- Configuring RADIUS Authentication for L2TP on page 37

statistics

Syntax statistics (time | volume-time);

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Option **volume-time** introduced in Junos OS Release 9.4.

Description Configure the router or switch to collect time statistics, or both volume and time statistics, for the sessions being managed by AAA.

Options **time**—Collect uptime statistics only.

volume-time—Collect both volume and uptime statistics. This option is not available for Mobile IP.

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

Related Documentation
- Mobile IP Home Agent Elements and Behavior
- Configuring Authentication and Accounting Parameters for Subscriber Access

tftp-server

Syntax tftp-server *ip-address*;

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

Release Information Statement introduced in Junos OS Release 9.0.

Description Specify the Trivial File Transfer Protocol (TFTP) server that the client uses to obtain the client configuration file. This is equivalent to DHCP option 150.

Options *ip-address*—IP address of the TFTP server.

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

Related Documentation
- Configuring Address-Assignment Pools

timeout (RADIUS)

Syntax timeout *seconds*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the amount of time that the local router or switch waits to receive a response from a RADIUS server.

Options *seconds*—Amount of time to wait.

Range: 1 through 90 seconds

Default: 3 seconds

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

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers
- Configuring Authentication and Accounting Parameters for Subscriber Access
- Example: Configuring CHAP Authentication with RADIUS on page 9
- Configuring RADIUS Authentication for L2TP on page 37

update-interval

Syntax update-interval *minutes*;

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the amount of time that the router or switch waits before sending a new accounting update.

Default No updates

Options ***minutes***—Amount of time between updates, in minutes.

Range: 10 through 1440 minutes

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

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access

user-group-profile

Syntax user-group-profile *profile-name*;

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

Release Information (M7i and M10i routers only) Statement introduced before Junos OS Release 7.4.
Support for MX Series routers introduced in Junos OS Release 11.4.

Description Apply a configured PPP group profile to PPP users.

Options ***profile-name***—Name of a PPP group profile configured at the **[edit access group-profile *profile-name*]** hierarchy level.

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

Related Documentation

- (M Series routers) Applying a Configured PPP Group Profile to a Tunnel on page 32
- (MX Series routers) Configuring an L2TP Access Profile on the LNS

vlan-nas-port-stacked-format

Syntax vlan-nas-port-stacked-format;

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

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

Related Documentation
- Configuring RADIUS Server Options for Subscriber Access
- Configuring Authentication and Accounting Parameters for Subscriber Access

wins-server

Syntax
```
wins-server {
  ipv4-address;
}
```

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

Release Information Statement introduced in Junos OS Release 9.0.

Description Specify one or more NetBIOS name servers (NBNS) that the client uses to resolve NetBIOS names. This is equivalent to DHCP option 44.

Options ***ipv4-address***—IP address of each NetBIOS name server; add them to the configuration in order of preference.

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

Related Documentation
- Configuring Address-Assignment Pools

PART 3

Administration

CHAPTER 5

Administrative Commands

clear network-access aaa statistics

Syntax
clear network-access aaa statistics
<accounting>
<address-assignment (client | pool *pool-name*)>
<authentication>
<dynamic-requests>
<radius>
<re-authentication>
<terminate-code>

Release Information
Command introduced in Junos OS Release 10.0.
Option **radius** introduced in Junos OS Release 11.4
Option **terminate-code** introduced in Junos OS Release 11.4.

Description
Clear AAA statistics.

Options
accounting—(Optional) Clear AAA accounting statistics.

address-assignment client—(Optional) Clear AAA address-assignment statistics for the client.

address-assignment pool *pool-name*—(Optional) Clear AAA address-assignment pool statistics.

authentication—(Optional) Clear AAA authentication statistics.

dynamic-requests—(Optional) Clear AAA dynamic-request statistics.

radius—(Optional) Clears the values in the **Peak** and **Exceeded** columns only.

re-authentication—(Optional) Clear AAA reauthentication statistics.

terminate-code—(Optional) Clear AAA termination code statistics.

Required Privilege Level
maintenance

List of Sample Output
clear network-access aaa statistics accounting on page 128
clear network-access aaa statistics address-assignment pool on page 128
clear network-access aaa statistics radius on page 129

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

Sample Output

clear network-access aaa statistics accounting

```
user@host> clear network-access aaa statistics accounting
```

clear network-access aaa statistics

```
user@host> clear network-access aaa statistics address-assignment pool isp_1
```

address-assignment pool

clear network-access aaa statistics radius

`user@host>` clear network-access aaa statistics radius

clear network-access aaa subscriber

Syntax clear network-access aaa subscriber
<statistics username *username*>
<username *username*>

Release Information Command introduced in Junos OS Release 9.1.

Description Clear AAA subscriber statistics and log out subscribers.

Options statistics username *username*—Clear AAA subscriber statistics and log out the subscriber.

username *username*—Log out the AAA subscriber.

Required Privilege Level maintenance

List of Sample Output clear network-access aaa subscriber statistics username on page 130
clear network-access aaa subscriber username on page 130

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

Sample Output

clear network-access aaa subscriber statistics username

```
user@host> clear network-access aaa subscriber statistics username dsmith@isp5555.com
```

clear network-access aaa subscriber username

```
user@host> clear network-access aaa subscriber username dsmith@isp5555.com
```

clear services l2tp session

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

Release Information Command introduced before Junos OS Release 7.4.
Support for LAC on MX Series routers introduced in Junos OS Release 10.4.
Support for LNS on MX Series routers introduced in Junos OS Release 11.4.

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

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 140

List of Sample Output clear services l2tp session on page 132

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
```

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

List of Sample Output

clear services l2tp tunnel statistics all on page 134

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 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 136
show services l2tp radius statistics on page 137

Output Fields Table 5 on page 135 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
```

CHAPTER 6

Monitoring Commands

show services l2tp session

Syntax

show services l2tp session
<brief | detail | extensive | statistics>
<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.
Support for LAC on MX Series routers introduced in Junos OS Release 10.4.
Support for LNS on MX Series routers introduced in Junos OS Release 11.4.

Description

(M10i and M7i routers: LNS only. MX Series routers: LAC and LNS.) Display a list of active L2TP sessions.

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 *interface-name*—(Optional) Display L2TP session information for only the specified adaptive services or inline services interface. The interface type depends on the line card as follows:

- **si-*fpc/pic/port***— MPCs on MX Series routers only. This option is not available for L2TP on M Series routers.
- **sp-*fpc/pic/port***—AS or Multiservices PICs on M7i, M10i, and M120 routers only. This option is not available for L2TP on MX Series routers.

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

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

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

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

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

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

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 131

List of Sample Output
show services l2tp session (LNS on M Series Routers) on page 144
show services l2tp session (LNS on MX Series Routers) on page 144
show services l2tp session (LAC) on page 144
show services l2tp session detail (LAC) on page 144
show services l2tp session extensive (LAC) on page 144
show services l2tp session extensive (LNS on M Series Routers) on page 145
show services l2tp session extensive (LNS on MX Series Routers) on page 145

Output Fields Table 6 on page 141 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

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

Field Name	Field Description	Level of Output
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
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**

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

Field Name	Field Description	Level of Output
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
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**

Table 6: show services l2tp session 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.	**extensive**

Sample Output

show services l2tp session (LNS on M Series Routers)

```
user@host> show services l2tp session
Interface: sp-1/2/0, Tunnel group: group1, Tunnel local ID:  8802
  Local Remote Interface State               Bundle Username
  ID    ID     unit
  37966      5         2 Established
```

show services l2tp session (LNS on MX Series Routers)

```
user@host> show services l2tp session
Tunnel local ID: 40553
  Local  Remote   State                Interface         Interface
  ID     ID                            unit              Name
  17967  1        Established          1073749824        si-5/2/0
```

show services l2tp session (LAC)

```
user@host> show services l2tp session
Tunnel local ID: 31889
  Local  Remote   State                Interface         Interface
  ID     ID                            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 on M Series Routers)

```
user@host> show services l2tp session extensive
Interface: sp-1/2/0, Tunnel group: group1, Tunnel local ID: 62746
  Session local ID: 56793, Session remote ID: 53304
    State: Established, Bundle ID: 5, Mode: shared
    Local IP: 10.128.1.1:1701, Remote IP: 10.128.1.2:1701
    Username: usr1@juniper_1.net, Assigned IP address: 10.50.2.1/32
    Local MRU: 4000, Remote MRU: 1500, Tx speed: 64000, Rx speed: 64000
    Bearer type: 2, Framing type: 1
    LCP renegotiation: Off, Authentication: CHAP, Interface ID: unit_20
    Interface unit: 20, Call serial number: 4137941434
    Policer bandwidth: 64000, Policer burst size: 51200
    Firewall filter: f1
    Session encapsulation overhead: 16, Session cell overhead: 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
```

show services l2tp session extensive (LNS on MX Series Routers)

```
user@host> show services l2tp session extensive
Tunnel local ID: 40553
  Session local ID: 17967, Session remote ID: 1
    Interface unit: 1073749824
    State: Established
    Interface: si-5/2/0
    Mode: Dedicated
    Local IP: 11.1.1.2:1701, Remote IP: 11.1.1.3:1701
    Local name: lns-mx960, Remote name: testlac
    Tx speed: 56000, Rx speed: 0
    Bearer type: 2, Framing type: 1
    LCP renegotiation: Off, Authentication: None
    Call serial number: 1
```

```
Create time: Mon Apr 25 20:27:50 2011, Up time: 00:01:48
Idle time: N/A
Statistics since: Mon Apr 25 20:27:50 2011
                    Packets        Bytes
  Control Tx              4          219
  Control Rx              4          221
  Data Tx                 0            0
  Data Rx                10          228
  Errors Tx               0
  Errors Rx               0
```

show services l2tp 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 148
show services l2tp radius statistics on page 149

Output Fields Table 5 on page 135 lists the output fields for the **show services l2tp radius** command. Output fields are listed in the approximate order in which they appear.

Table 7: 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 7: 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 summary

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

Release Information
Command introduced before Junos OS Release 7.4.
Support for LAC on MX Series routers introduced in Junos OS Release 10.4.
Support for LNS on MX Series routers introduced in Junos OS Release 11.4.

Description
(M10i and M7i routers: LNS only. MX Series routers: LAC and LNS.) Display Layer 2 Tunneling Protocol (L2TP) summary information.

Options
none—Display complete L2TP summary information. For LNS on M Series routers, display L2TP summary information for all adaptive services interfaces. For LNS on MX Series routers, display L2TP summary information for all inline services interfaces.

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 152
show services l2tp summary (LNS on MX Series routers) on page 153
show services l2tp summary (LNS on M Series routers) on page 153

Output Fields
Table 8 on page 151 lists the output fields for the **show services l2tp summary** command. Output fields are listed in the approximate order in which they appear.

Table 8: 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 8: 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. On M Series router 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.
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 (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
```

PART 4

Index

Index

W