



Junos[®] OS

Layer 2 Network Access Protocols Feature Guide for Routing Devices

Release

14.1



Published: 2014-05-08

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

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos[®] OS Layer 2 Network Access Protocols Feature Guide for Routing Devices

14.1

Copyright © 2014, Juniper Networks, Inc.
All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

	About the Documentation	xi
	Documentation and Release Notes	xi
	Supported Platforms	xi
	Using the Examples in This Manual	xi
	Merging a Full Example	xii
	Merging a Snippet	xii
	Documentation Conventions	xiii
	Documentation Feedback	xv
	Requesting Technical Support	xv
	Self-Help Online Tools and Resources	xv
	Opening a Case with JTAC	xvi
Part 1	Overview	
Chapter 1	Network Access Configuration Overview	3
	Network Access Configuration Overview	3
Part 2	Configuration	
Chapter 2	Configuring PPP and L2TP	7
	Configuring the PPP Authentication Protocol	8
	Example: Configuring PPP CHAP	8
	Example: Configuring CHAP Authentication with RADIUS	9
	Configuring L2TP for Enabling PPP Tunneling Within a Network	12
	Defining the Minimum L2TP Configuration	13
	Configuring the Address Pool for L2TP Network Server IP Address Allocation	14
	Example: Configuring an Address-Assignment Pool	15
	Configuring the Group Profile for Defining L2TP Attributes	16
	Configuring L2TP for a Group Profile	17
	Configuring the PPP Attributes for a Group Profile	17
	Example: Group Profile Configuration	18
	Configuring Access Profiles for L2TP or PPP Parameters	19
	Configuring the Access Profile	19
	Configuring the L2TP Properties for a Profile	20
	Configuring the PPP Properties for a Profile	20
	Configuring the Authentication Order	21
	Configuring the Accounting Order	21
	Example: Access Profile Configuration	22
	Configuring an IKE Access Profile	23
	Configuring the L2TP Client	24
	Example: Defining the Default Tunnel Client	25

	Example: Defining the User Group Profile	25
	Configuring the CHAP Secret for an L2TP Profile	26
	Example: Configuring L2TP PPP CHAP	27
	Referencing the Group Profile from the L2TP Profile	27
	Configuring L2TP Properties for a Client-Specific Profile	27
	Example: PPP MP for L2TP	29
	Example: L2TP Multilink PPP Support on Shared Interfaces	29
	Configuring the PAP Password for an L2TP Profile	30
	Example: Configuring PAP for an L2TP Profile	31
	Configuring PPP Properties for a Client-Specific Profile	31
	Applying a Configured PPP Group Profile to a Tunnel	33
	Example: Applying a User Group Profile on the M7i or M10i Router	33
	Example: Configuring L2TP	34
Chapter 3	Configuring RADIUS Authentication for L2TP	37
	Configuring RADIUS Authentication for L2TP	37
	RADIUS Attributes for L2TP	39
	RADIUS Local Loopback Interface Attribute for L2TP Overview	42
	Example: Configuring RADIUS Authentication for L2TP	43
	Configuring the RADIUS Disconnect Server for L2TP	44
	Configuring RADIUS Authentication for an L2TP Client and Profile	45
	Example: Configuring RADIUS Authentication for an L2TP Profile	46
	Example: Configuring RADIUS-Based Subscriber Authentication and Accounting	46
	Understanding Session Options for Subscriber Access	48
	Configuring Subscriber Session Options	50
Chapter 4	Configuration Statements	53
	Access Configuration Statements	56
	accounting (Access Profile)	60
	accounting-order	61
	accounting-port	61
	accounting-server	62
	accounting-session-id-format	62
	accounting-stop-on-access-deny	63
	accounting-stop-on-failure	63
	address (Access Address Pool)	64
	address-assignment (Address-Assignment Pools)	65
	address-pool	66
	address-range	67
	allowed-proxy-pair	67
	attributes	68
	authentication-order	69
	authentication-server	70
	boot-file	70
	boot-server	71
	cell-overhead	71
	chap-secret	72
	circuit-id (Address-Assignment Pools)	73
	circuit-type (DHCP Local Server)	74

client	75
client-authentication-algorithm	76
client-idle-timeout	77
client-group	78
client-session-timeout	79
dead-peer-detection	80
dhcp-attributes (Address-Assignment Pools)	81
domain-name (Address-Assignment Pools)	82
drop-timeout	82
encapsulation-overhead	83
ethernet-port-type-virtual	83
exclude (RADIUS)	84
fragment-threshold (Access)	88
framed-ip-address	88
framed-pool	89
grace-period	89
group-profile (Associating with Client)	90
group-profile (Group Profile)	91
hardware-address	92
host (Address-Assignment Pools)	92
idle-timeout (Access)	93
ignore	94
ike (Access Profile)	95
ike-policy	96
immediate-update	96
initiate-dead-peer-detection (IPsec)	97
interface-description-format	97
interface-id	98
ip-address	98
keepalive	99
keepalive-retries	100
l2tp (Group Profile)	101
l2tp (Profile)	102
lcp-renegotiation	103
local-chap	104
maximum-lease-time	105
maximum-sessions-per-tunnel	106
multilink	107
name-server	107
nas-identifier	108
nas-port-extended-format (Access Profile)	109
netbios-node-type	110
network	111
option	111
option-82 (Address-Assignment Pools)	112
option-match	112
options (Access Profile)	113
order	114
pap-password	115

pool (Address-Assignment Pools)	116
port	117
ppp (Group Profile)	118
ppp (Profile)	119
ppp-authentication	120
ppp-profile	120
pre-shared-key (Access Profile)	121
primary-dns	121
primary-wins	122
profile (Access)	123
radius (Access Profile)	127
radius-disconnect	129
radius-disconnect-port	130
radius-server	131
range (Address-Assignment Pools)	132
remote-id	133
retry	134
reverse-route	134
revert-interval	135
router (Address-Assignment Pools)	135
routing-instance	136
secondary-dns	136
secondary-wins	137
secret	137
session-options	138
shared-secret	138
source-address	139
statistics (Access Profile)	140
tftp-server	140
timeout (RADIUS)	141
update-interval	142
user-group-profile	143
vlan-nas-port-stacked-format	143
wins-server (Access)	144

Part 3

Administration

Chapter 5

Administrative Commands 147

clear network-access aaa statistics	148
clear network-access aaa subscriber	150
clear services l2tp session	151
clear services l2tp tunnel statistics	153
show services l2tp radius	155

Chapter 6

Monitoring Commands 159

show services l2tp session	160
show services l2tp radius	168
show services l2tp summary	172

Part 4

Index

Index	179
-------------	-----

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xiii
	Table 2: Text and Syntax Conventions	xiv
Part 2	Configuration	
Chapter 3	Configuring RADIUS Authentication for L2TP	37
	Table 3: Juniper Networks Vendor-Specific RADIUS Attributes for L2TP	39
	Table 4: Supported IETF RADIUS Attributes for L2TP	39
	Table 5: Supported RADIUS Accounting Start Attributes for L2TP	40
	Table 6: Supported RADIUS Accounting Stop Attributes for L2TP	41
Part 3	Administration	
Chapter 5	Administrative Commands	147
	Table 7: show services l2tp radius Output Fields	155
Chapter 6	Monitoring Commands	159
	Table 8: show services l2tp session Output Fields	161
	Table 9: show services l2tp radius Output Fields	168
	Table 10: show services l2tp summary Output Fields	172

About the Documentation

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

Documentation and Release Notes

To obtain the most current version of all Juniper Networks[®] technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

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

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

Supported Platforms

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

- M Series
- MX Series
- T Series
- J Series

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

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

Table 2: Text and Syntax Conventions

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

GUI Conventions

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

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

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>

- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes:
<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications:
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

- [Network Access Configuration Overview on page 3](#)

CHAPTER 1

Network Access Configuration Overview

- [Network Access Configuration Overview on page 3](#)

Network Access Configuration Overview

The Junos operating system (Junos OS) enables you to configure network access features for the device at the **[edit access]** hierarchy level. This includes Layer 2 Tunneling Protocol (L2TP), Point-to-Point Protocol (PPP), and Subscriber Access configuration.

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

The L2TP protocol allows PPP to be tunneled within a network.

For a complete hierarchy of access configuration statements, see [“Access Configuration Statements” on page 56](#).

For information about configuring Subscriber Access, see:

- *AAA Service Framework Feature Guide for Subscriber Management*
- *Address Assignment Pools Feature Guide for Subscriber Management*
- *DHCP Local Server Feature Guide for Subscriber Management*
- *PPP Feature Guide for Subscriber Management*

Related Documentation

- [Access Configuration Statements on page 56](#)
- [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

- [Configuring PPP and L2TP on page 7](#)
- [Configuring RADIUS Authentication for L2TP on page 37](#)
- [Configuration Statements on page 53](#)

CHAPTER 2

Configuring PPP and L2TP

- [Configuring the PPP Authentication Protocol on page 8](#)
- [Example: Configuring PPP CHAP 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](#)
- [Example: Configuring an Address-Assignment Pool on page 15](#)
- [Configuring the Group Profile for Defining L2TP Attributes on page 16](#)
- [Example: Group Profile Configuration on page 18](#)
- [Configuring Access Profiles for L2TP or PPP Parameters on page 19](#)
- [Configuring an IKE Access Profile on page 23](#)
- [Configuring the L2TP Client on page 24](#)
- [Example: Defining the Default Tunnel Client on page 25](#)
- [Example: Defining the User Group Profile on page 25](#)
- [Configuring the CHAP Secret for an L2TP Profile on page 26](#)
- [Example: Configuring L2TP PPP CHAP on page 27](#)
- [Referencing the Group Profile from the L2TP Profile on page 27](#)
- [Configuring L2TP Properties for a Client-Specific Profile on page 27](#)
- [Example: PPP MP for L2TP on page 29](#)
- [Example: L2TP Multilink PPP Support on Shared Interfaces on page 29](#)
- [Configuring the PAP Password for an L2TP Profile on page 30](#)
- [Example: Configuring PAP for an L2TP Profile on page 31](#)
- [Configuring PPP Properties for a Client-Specific Profile on page 31](#)
- [Applying a Configured PPP Group Profile to a Tunnel on page 33](#)
- [Example: Applying a User Group Profile on the M7i or M10i Router on page 33](#)
- [Example: Configuring L2TP on page 34](#)

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 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.

Definitions:

- **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 "$1$kdAsfaDAfkjDsASxfafdKdFKJ";
        # 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 Library for Routing Devices* and the *Junos OS Network Interfaces Library for Routing Devices*.

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 31.



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 33.

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 27](#)

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](#)
6. [Example: Access Profile Configuration on page 22](#)

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 33](#).

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;
  }
}
```

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 L2TP 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.

Example: Access Profile Configuration

The following example shows a configuration of an access profile:

```
[edit access]
profile westcoast_bldg_1 {
  client white {
    chap-secret "$9$3s2690leK8X7VKM7VwgaJn/Ctu1hclv87Ct87";
    # SECRET-DATA
    ppp {
      idle-timeout 22;
      primary-dns 192.120.65.10;
      framed-ip-address 12.12.12.12/32;
    }
    group-profile westcoast_users;
  }
  client blue {
    chap-secret "$9$eq1KWxbwgZUHNdjmqmTF3uO1Rhr-dsoJDNd";
    # SECRET-DATA
    group-profile sunnyvale_users;
  }
  authentication-order password;
}
profile westcoast_bldg_1_tunnel {
  client test {
    l2tp {
      shared-secret "$9$r3HKvLg4ZUDkX7JGjif5pOBIRS8LN";
      # 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;
  }
}

```

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;
      }
      dead-peer-detection {
        interval seconds
        threshold number
      }
      ike-policy policy-name;
      initiate-dead-peer-detection;
      interface-id string-value;
      ipsec-policy ipsec-policy;
      pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
      reverse-route
    }
  }
}

```

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.

- **dead-peer-detection**—Enable the device to use dead peer detection (DPD). DPD is a method used by devices to verify the current existence and availability of IPsec peer devices. A device performs this verification by sending encrypted IKE Phase 1 notification payloads (R-U-THERE) to peers and waiting for DPD acknowledgements (R-U-THERE-ACK). Use the option **interval** to specify the seconds between which messages should be sent. Use the **threshold** option to specify the maximum number of messages (1-10) to be sent.
- **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.
- **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.
- **reverse-route** —(M Series and MX Series routers with an AS or MultiServices PIC only) Configure a reverse route for dynamic endpoint IPsec tunnels.

**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 25](#)

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 24](#)
- [Example: Defining the User Group Profile on page 25](#)

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 33.](#)

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 27](#)

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 26](#)

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 25](#)
- [Configuring Access Profiles for L2TP or PPP Parameters on page 19](#)
- [Configuring L2TP Properties for a Client-Specific Profile on page 27](#)

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 31](#)
 - [Example: PPP MP for L2TP on page 29](#)
 - [Example: L2TP Multilink PPP Support on Shared Interfaces on page 29](#)

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 27](#)
 - [Example: L2TP Multilink PPP Support on Shared Interfaces on page 29](#)

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 27](#)

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 26](#).

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 31](#)

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 30](#)

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 27](#)

Applying a Configured PPP Group Profile to a Tunnel

On M7 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 33](#)
- [Example: Defining the User Group Profile on page 25](#)

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

**Related
Documentation**

- [Applying a Configured PPP Group Profile to a Tunnel on page 33](#)

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$3s2690leK8X7VKM7VwgaJn/Ctu1hclv87Ct87";
        # SECRET-DATA
        ppp {
            idle-timeout 22;
            primary-dns 192.120.65.10;
            framed-ip-address 12.12.12.12/32;
        }
        group-profile westcoast_users;
    }
    client blue {
        chap-secret "$9$eq1KWxbwgZUHNdjqmTF3uO1Rhr-dsoJDNd";
        # SECRET-DATA
        group-profile sunnyvale_users;
    }
    authentication-order password;
}
profile west-coast_bldg_2 {
    client red {
        pap-password "$9$3s2690leK8X7VKM8888Ctu1hclv87Ct87";
        # 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

```

```
        rXxbs2aJDHqf3nCP5"; # SECRET-DATA
        ppp-authentication chap;
    }
    group-profile westcoast_tunnel;
}
}
profile westcoast_bldg_2_tunnel {
    client black {
        l2tp {
            shared-secret "$9$R2QErV8X-goGylVwg4jiTz36/t0BEleWFnRh
            rXxbs2aJDHqf3nCP5";
            # 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 on page 37](#)
- [RADIUS Attributes for L2TP on page 39](#)
- [RADIUS Local Loopback Interface Attribute for L2TP Overview on page 42](#)
- [Example: Configuring RADIUS Authentication for L2TP on page 43](#)
- [Configuring the RADIUS Disconnect Server for L2TP on page 44](#)
- [Configuring RADIUS Authentication for an L2TP Client and Profile on page 45](#)
- [Example: Configuring RADIUS Authentication for an L2TP Profile on page 46](#)
- [Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 46](#)
- [Understanding Session Options for Subscriber Access on page 48](#)
- [Configuring Subscriber Session Options on page 50](#)

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 30 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 44](#).



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 44](#)

RADIUS Attributes for L2TP

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

- Juniper Networks vendor-specific attributes (VSAs)
- 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 3 on page 39](#) lists the Juniper Networks VSAs you can configure for L2TP.

Table 3: 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 4 on page 39](#) lists the IETF RADIUS AVPs supported for L2TP.

Table 4: 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

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

Attribute Name	Standard Number	Value
NAS-Port	5	Integer
Service-Type	6	Integer
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 5 on page 40](#) lists the supported RADIUS accounting start AVPs for L2TP.

Table 5: 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

Table 5: Supported RADIUS Accounting Start Attributes for L2TP (continued)

Attribute Name	Standard Number	Value
Calling-Station-ID	31	String
Acct-Status-Type	40	Integer
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 6 on page 41](#) lists the supported RADIUS accounting stop AVPs for L2TP.

Table 6: Supported RADIUS Accounting Stop Attributes for L2TP

Attribute Name	Standard Number	Value
User-Name	1	String
Local-Loopback-Interface	3	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

Table 6: Supported RADIUS Accounting Stop Attributes for L2TP (continued)

Attribute Name	Standard Number	Value
Acct-Status-Type	40	Integer
Acct-Delay-Time	41	Integer
Acct-Input-Octets	42	Integer
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 43](#)

RADIUS Local Loopback Interface Attribute for L2TP Overview

You can configure the Local-Loopback-Interface attribute on a RADIUS server to manage multiple LAC devices. This attribute is used as the LAC source address on an LNS tunnel for PPPoE subscribers tunneled over L2TP.

When you use the Tunnel-Client-Endpoint attribute as the LAC source address, you must configure the Tunnel-Client-Endpoint attribute for each MX Series router that uses the same RADIUS server. Starting with this release you can use the Local-Loopback-Interface attribute, which needs to be configured only once. When the LAC initiates an Access-Request message to RADIUS for authentication, RADIUS returns the Local-Loopback-Interface attribute in the Access-Accept message. This attribute contains the name of the loopback interface, either as a generic interface name such as "lo0" or as a specific name like "lo0.0". The MX Series router then uses the configured loopback interface IP address as the source address during tunnel negotiation with the LNS.



NOTE: An MX Series router can act as the LAC and use any interface address on it as an L2TP tunnel source address. The source address can be dynamically assigned by RADIUS through the Tunnel-Client-Endpoint or Local-Loopback-Interface attribute. The tunnel source address can be statically configured on the MX Series router by using the L2TP tunnel profile. If RADIUS does not return the Tunnel-Client-Endpoint or Local-Loopback-Interface attribute, and if there is no corresponding L2TP tunnel profile configured on the MX Series router, then the L2TP tunnel fails to initiate because the router does not have a proper tunnel source address. In this case, the router can use the locally configured loopback address as the source address to successfully establish the L2TP tunnel.

Related Documentation

- [RADIUS Attributes for L2TP on page 39](#)

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/A0z30lhr8Lbs24GDHqmTFn";
    # SECRET-DATA
    192.168.64.157 secret "$9$Hk5FCA0lhruOrv87sYGDikfTFn/t0B";
    # SECRET-DATA
    192.168.64.173 secret "$9$Hk5FCA0lhruOrv87sYGDikfTFn/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 46](#)

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 45](#)

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;
    accounting-retry 6;
    accounting-timeout 20;
    retry 3;
    secret &tIUEI*7688+;
    source-address 192.168.1.100;
    timeout 45;
  }
}
```

```
192.168.1.251 {
  port 1812;
  accounting-port 1813;
  accounting-retry 6;
  accounting-timeout 20;
  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;
  accounting {
    order radius;
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    immediate-update;
    statistics time;
    update-interval 12;
    wait-for-acct-on-ack;
    send-acct-status-on-config-change;
  }
  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*

Understanding Session Options for Subscriber Access

You can limit subscriber access by configuring a session timeout or an idle timeout. Use a session timeout to specify a fixed period of time that the subscriber is permitted to have access. Use an idle timeout to specify a maximum period of time that the subscriber can be idle. You can use these timeouts separately or together. By default, neither timeout is present.



NOTE: For all subscriber types other than DHCP (such as L2TP-tunneled and PPP-terminated subscribers), the session timeout value limits the subscriber session. For DHCP subscribers, the session timeout value is used to limit the lease. The lease expires when the timeout value expires. If this value is not supplied by either the CLI or RADIUS, the DHCP lease does not expire.

The idle timeout is based on accounting statistics for the subscriber. The router determines subscriber inactivity by monitoring data traffic, both upstream from the user and downstream to the user. Control traffic is ignored. The subscriber is not considered idle as long as data traffic is detected in either direction.

When either timeout period expires, the non-DHCP subscribers are gracefully logged out, similarly to a RADIUS-initiated disconnect or a CLI-initiated logout. DHCP subscribers are disconnected. The Acct-Terminate-Cause [RADIUS attribute 49] value includes a reason code of 5 for a session timeout and a code of 4 for an idle timeout.

You can configure these limitations to subscriber access on a per-subscriber basis by using the RADIUS attributes Session-Timeout [27] and Idle-Timeout [28]. RADIUS returns these attributes in Access-Accept messages in response to Access-Request messages from the access server.

Service providers often choose to apply the same limitations to large numbers of subscribers. You can reduce the RADIUS provisioning effort for this scenario by defining the limitations for subscribers in an access profile on a per-routing-instance basis. If you do so, RADIUS attributes subsequently returned for a particular subscriber logged in with the profile override the per-routing-instance values.

The available range for setting a timeout is the same whether you configure it in the CLI or through the RADIUS attributes. Session timeouts can be set for 1 minute through 527,040 minutes in the CLI and the corresponding number of seconds (60 through 31,622,400) in the Session-Timeout attribute [27]. Idle timeouts can be set for 10 minutes through 1440 minutes in the CLI and the corresponding number of seconds (600 through 86,400) in the Idle-Timeout attribute [28].

The router interprets the values in the attributes to conform to the supported ranges. For example, for Session-Timeout [27]:

- A value of zero is treated as no timeout.
- A value in the range 1 through 59 is raised to 60 seconds.
- A value that exceeds 31,622,400 is reduced to 31,622,400 seconds.

For Idle-Timeout [28]:

- A value of zero is treated as no timeout.
- A value in the range 1 through 599 is raised to 600 seconds.
- A value that exceeds 86,400 is reduced to 86,400 seconds.

In configurations using dynamically created subscriber VLANs, the idle timeout also deletes the inactive subscriber VLANs when the inactivity threshold has been reached. In addition to deleting inactive dynamic subscriber VLANs, the idle timeout also removes dynamic VLANs when no client sessions were ever created (for example, in the event no client sessions are created on the dynamic VLAN or following the occurrence of an error during session creation or client authentication where no client sessions are created on the dynamic VLAN).

When using the idle timeout for dynamic VLAN removal, keep the following in mind:

- The idle timeout period begins after a dynamic subscriber VLAN interface is created or traffic activity stops on a dynamic subscriber VLAN interface.

- If a new client session is created or a client session is reactivated successfully, the client idle timeout resets.
- The removal of inactive subscriber VLANs functions only with VLANs that have been authenticated.

**Related
Documentation**

- *RADIUS IETF Attributes Supported by the AAA Service Framework*
- [Configuring Subscriber Session Options on page 50](#)
- *Removing Inactive Dynamic Subscriber VLANs*

Configuring Subscriber Session Options

Subscriber session timeouts enable you to place limits on subscriber access based on how long the session has been up, how long the user has been inactive, or both. The subscriber session timeouts apply to both L2TP-tunneled and PPP-terminated subscriber sessions.



NOTE: To configure the timeout attributes in RADIUS, refer to the documentation for your RADIUS server.

To configure limitations on subscriber sessions:

1. Edit session options for the router access profile.

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

2. Configure the maximum period a subscriber session can be active.

```
[edit access profile profile-name session-options]
user@host# set client-session-timeout minutes
```

3. Configure the maximum period a subscriber session can be idle.

```
[edit access profile profile-name session-options]
user@host# set client-idle-timeout minutes
```

For example, to configure a client session timeout of 2 hours and an idle timeout of 15 minutes in the **acc-prof** profile:

```
[edit]
access {
  profile {
    acc-prof {
      session-options {
        client-session-timeout 120;
        client-idle-timeout 15;
      }
    }
  }
}
```

- Related Documentation**
- [Understanding Session Options for Subscriber Access on page 48](#)
 - [client-idle-timeout on page 77](#)
 - [client-session-timeout on page 79](#)

CHAPTER 4

Configuration Statements

- [Access Configuration Statements on page 56](#)
- [accounting \(Access Profile\) on page 60](#)
- [accounting-order on page 61](#)
- [accounting-port on page 61](#)
- [accounting-server on page 62](#)
- [accounting-session-id-format on page 62](#)
- [accounting-stop-on-access-deny on page 63](#)
- [accounting-stop-on-failure on page 63](#)
- [address \(Access Address Pool\) on page 64](#)
- [address-assignment \(Address-Assignment Pools\) on page 65](#)
- [address-pool on page 66](#)
- [address-range on page 67](#)
- [allowed-proxy-pair on page 67](#)
- [attributes on page 68](#)
- [authentication-order on page 69](#)
- [authentication-server on page 70](#)
- [boot-file on page 70](#)
- [boot-server on page 71](#)
- [cell-overhead on page 71](#)
- [chap-secret on page 72](#)
- [circuit-id \(Address-Assignment Pools\) on page 73](#)
- [circuit-type \(DHCP Local Server\) on page 74](#)
- [client on page 75](#)
- [client-authentication-algorithm on page 76](#)
- [client-idle-timeout on page 77](#)
- [client-group on page 78](#)
- [client-session-timeout on page 79](#)
- [dead-peer-detection on page 80](#)

- [dhcp-attributes \(Address-Assignment Pools\) on page 81](#)
- [domain-name \(Address-Assignment Pools\) on page 82](#)
- [drop-timeout on page 82](#)
- [encapsulation-overhead on page 83](#)
- [ethernet-port-type-virtual on page 83](#)
- [exclude \(RADIUS\) on page 84](#)
- [fragment-threshold \(Access\) on page 88](#)
- [framed-ip-address on page 88](#)
- [framed-pool on page 89](#)
- [grace-period on page 89](#)
- [group-profile \(Associating with Client\) on page 90](#)
- [group-profile \(Group Profile\) on page 91](#)
- [hardware-address on page 92](#)
- [host \(Address-Assignment Pools\) on page 92](#)
- [idle-timeout \(Access\) on page 93](#)
- [ignore on page 94](#)
- [ike \(Access Profile\) on page 95](#)
- [ike-policy on page 96](#)
- [immediate-update on page 96](#)
- [initiate-dead-peer-detection \(IPsec\) on page 97](#)
- [interface-description-format on page 97](#)
- [interface-id on page 98](#)
- [ip-address on page 98](#)
- [keepalive on page 99](#)
- [keepalive-retries on page 100](#)
- [l2tp \(Group Profile\) on page 101](#)
- [l2tp \(Profile\) on page 102](#)
- [lcp-renegotiation on page 103](#)
- [local-chap on page 104](#)
- [maximum-lease-time on page 105](#)
- [maximum-sessions-per-tunnel on page 106](#)
- [multilink on page 107](#)
- [name-server on page 107](#)
- [nas-identifier on page 108](#)
- [nas-port-extended-format \(Access Profile\) on page 109](#)
- [netbios-node-type on page 110](#)
- [network on page 111](#)

- [option](#) on page 111
- [option-82 \(Address-Assignment Pools\)](#) on page 112
- [option-match](#) on page 112
- [options \(Access Profile\)](#) on page 113
- [order](#) on page 114
- [pap-password](#) on page 115
- [pool \(Address-Assignment Pools\)](#) on page 116
- [port](#) on page 117
- [ppp \(Group Profile\)](#) on page 118
- [ppp \(Profile\)](#) on page 119
- [ppp-authentication](#) on page 120
- [ppp-profile](#) on page 120
- [pre-shared-key \(Access Profile\)](#) on page 121
- [primary-dns](#) on page 121
- [primary-wins](#) on page 122
- [profile \(Access\)](#) on page 123
- [radius \(Access Profile\)](#) on page 127
- [radius-disconnect](#) on page 129
- [radius-disconnect-port](#) on page 130
- [radius-server](#) on page 131
- [range \(Address-Assignment Pools\)](#) on page 132
- [remote-id](#) on page 133
- [retry](#) on page 134
- [reverse-route](#) on page 134
- [revert-interval](#) on page 135
- [router \(Address-Assignment Pools\)](#) on page 135
- [routing-instance](#) on page 136
- [secondary-dns](#) on page 136
- [secondary-wins](#) on page 137
- [secret](#) on page 137
- [session-options](#) on page 138
- [shared-secret](#) on page 138
- [source-address](#) on page 139
- [statistics \(Access Profile\)](#) on page 140
- [tftp-server](#) on page 140
- [timeout \(RADIUS\)](#) on page 141
- [update-interval](#) on page 142

- [user-group-profile](#) on page 143
- [vlan-nas-port-stacked-format](#) on page 143
- [wins-server \(Access\)](#) on page 144

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;
    duplication;
    immediate-update;
    order [ accounting-method ];
    statistics (time | volume-time);
    update-interval minutes;
  }
  accounting-order radius;
  authentication-order [ authentication-methods ];
  authorization-order jsr;
  client client-name {
    chap-secret chap-secret;
    client-group [ group-names ];
    firewall-user {
      password password;
    }
    group-profile profile-name;
    ike {
      allowed-proxy-pair {
        local local-proxy-address remote remote-proxy-address;
      }
      ike-policy policy-name;
      initiate-dead-peer-detection;
      interface-id interface-id;
      ipsec-policy policy-name;
      pre-shared-key (ascii-text character-key-string | hexadecimal
        hexadecimal-digits-key-string);
    }
    l2tp {
      interface-id interface-identifier;
      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;
}
provisioning-order jsr;
user-group-profile profile-name;
}
radius {
  accounting-server [ ip-address ];
  attributes {
    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 ];
    }
  }
  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 [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;
}
}
radius-options {
    revert-interval interval;
}
radius-disconnect {
    client-address {
        secret password;
    }
}
radius-disconnect-port port-number;
radius-options {
    revert-interval interval;
}
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
    source-address address;
    timeout seconds;
}
session-options {
    client-group [ group-names ];
    client-idle-timeout minutes;
    client-session-timeout minutes;
}

```

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](#);
 address-change-immediate-update;
 coa-immediate-update;
 coa-no-override service-class-attribute;
 duplication;
 duplication-vrf {
 access-profile-name *profile-name*;
 vrf-name *vrf-name*;
 }
 [immediate-update](#);
 order [*accounting-method*];
 send-acct-status-on-config-change
 [statistics](#) (time | volume-time);
 [update-interval](#) *minutes*;
 wait-for-acct-on-ack;
 }

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 [<i>accounting-order-data-list</i>]);
Hierarchy Level	[edit access profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 8.0. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Enable RADIUS accounting for an L2TP profile.
Options	<p>radius—Use the RADIUS accounting method.</p> <p>[<i>accounting-order-data-list</i>]—Set of data listing the accounting order to be used, enclosed by brackets. This can be any combination of accounting methods, up to and including and entire list of the entire accounting order.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Accounting Order on page 21

accounting-port

Syntax	accounting-port <i>port-number</i> ;
Hierarchy Level	<p>[edit access radius-server <i>server-address</i>],</p> <p>[edit access profile <i>profile-name</i> radius-server <i>server-address</i>]</p>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Configure the port number on which to contact the accounting server.
Options	<i>port-number</i> —Port number on which to contact the accounting server. Most RADIUS servers use port number 1813 (as specified in RFC 2866).
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • 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	<code>accounting-server [<i>ip-address</i>];</code>
Hierarchy Level	<code>[edit access profile <i>profile-name</i> radius radius]</code>
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	<i>ip-address</i> —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	<ul style="list-style-type: none">• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

accounting-session-id-format

Syntax	<code>accounting-session-id-format (decimal description);</code>
Hierarchy Level	<code>[edit access profile <i>profile-name</i> radius radius options]</code>
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	<code>decimal</code>
Options	<code>decimal</code> —Use the decimal format. <code>description</code> —Use the generic format, in the form: <code>jnpr <i>interface-specifier:subscriber-session-id</i></code> .
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Options for Subscriber Access</i>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

accounting-stop-on-access-deny

Syntax	accounting-stop-on-access-deny;
Hierarchy Level	[edit access profile <i>profile-name</i> 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	<ul style="list-style-type: none"> • <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

accounting-stop-on-failure

Syntax	accounting-stop-on-failure;
Hierarchy Level	[edit access profile <i>profile-name</i> 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	<ul style="list-style-type: none"> • <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

address (Access Address Pool)

Syntax	<code>address <i>address-or-prefix</i>;</code>
Hierarchy Level	[edit access address-pool <i>pool-name</i>]
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	<i>address-or-prefix</i> —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	<ul style="list-style-type: none">• Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 14

address-assignment (Address-Assignment Pools)

```
Syntax address-assignment {
    abated-utilization percentage;
    abated-utilization-v6 percentage;
    high-utilization percentage;
    high-utilization-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.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

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



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

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](#)
- [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)

address-pool

Syntax	<pre>address-pool <i>pool-name</i> { address <i>address-or-prefix</i>; address-range <low <i>lower-limit</i>> <high <i>upper-limit</i>>; }</pre>
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	<p><i>pool-name</i>—Name assigned to an address pool.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 14

address-range

Syntax	<code>address-range <low <i>lower-limit</i>> <high <i>upper-limit</i>>;</code>
Hierarchy Level	<code>[edit access address-pool <i>pool-name</i>]</code>
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	<ul style="list-style-type: none"> • high <i>upper-limit</i>—Upper limit of an address range. • low <i>lower-limit</i>—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	<ul style="list-style-type: none"> • Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 14


allowed-proxy-pair

Syntax	<pre>allowed-proxy-pair { remote <i>remote-proxy-address</i> local <i>local-proxy-address</i>; }</pre>
Hierarchy Level	<code>[edit access profile <i>profile-name</i> client <i>client-name</i> ike]</code>
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	<p>local <i>local-proxy-address</i>—Network address of the local peer. Default: 0.0.0.0</p> <p>remote <i>remote-proxy-address</i>—Network address of the remote peer. Default: 0.0.0.0</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring an IKE Access Profile on page 23

attributes

Syntax	<pre>attributes { exclude { ... } ignore { framed-ip-netmask; input-filter; logical-system-routing-instance; output-filter; } }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i> 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	<ul style="list-style-type: none">• <i>Configuring How RADIUS Attributes Are Used for Subscriber Access</i>

authentication-order

Syntax	<code>authentication-order [<i>authentication-methods</i>];</code>
Hierarchy Level	<code>[edit access <i>profile</i> <i>profile-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Option none 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	<code>password</code>
Options	<p><i>authentication-methods</i></p> <ul style="list-style-type: none"> • 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 <code>[edit access profile <i>profile-name</i> client <i>client-name</i>]</code> hierarchy level. • radius—Verify the client using RADIUS authentication services.
<div>  <p>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.</p> </div>	
Required Privilege Level	<p><code>admin</code>—To view this statement in the configuration.</p> <p><code>admin-control</code>—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • 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	<code>authentication-server [<i>ip-address</i>];</code>
Hierarchy Level	[edit access profile <i>profile-name</i> 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	<i>ip-address</i> —IPv4 address.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Parameters for Subscriber Access</i>

boot-file

Syntax	<code>boot-file <i>filename</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> 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	<i>filename</i> —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	<ul style="list-style-type: none">• <i>Configuring Address-Assignment Pools</i>• boot-server on page 71


boot-server

Syntax	<code>boot-server (address hostname);</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> 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	<p>address—IPv4 address of a boot server.</p> <p>hostname—Fully qualified hostname of a boot server.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Address-Assignment Pools • boot-file on page 70

cell-overhead

Syntax	<code>cell-overhead;</code>
Hierarchy Level	<p>[edit access group-profile <i>profile-name</i> ppp],</p> <p>[edit access profile <i>profile-name</i> client <i>client-name</i> ppp]</p>
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	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the PPP Attributes for a Group Profile on page 17 • Configuring PPP Properties for a Client-Specific Profile on page 31

chap-secret

Syntax	<code>chap-secret <i>chap-secret</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> client <i>client-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	For interfaces with PPP encapsulation on which the PPP Challenge Handshake Authentication Protocol (CHAP) is configured, configure the shared secret (the CHAP secret key associated with a peer), as defined in RFC 1994.
<div> NOTE: This statement is not supported for L2TP LNS on MX Series routers.</div>	
Options	<i>chap-secret</i> —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	<ul style="list-style-type: none">• Configuring the CHAP Secret for an L2TP Profile on page 26• Configuring PPP CHAP Authentication• pap-password on page 115• Junos OS Administration Library for Routing Devices

circuit-id (Address-Assignment Pools)

Syntax	<code>circuit-id <i>value</i> range <i>named-range</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes option-match option-82]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Configure the address-assignment pool <i>named-range</i> to use for a particular option 82 Agent Circuit ID value.
Options	<p><i>value</i>—String for the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82) in DHCP packets.</p> <p><i>range named-range</i>—Name of the address-assignment pool range to use.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Address-Assignment Pools</i>

circuit-type (DHCP Local Server)

Syntax	circuit-type;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the circuit type is concatenated with the username during the subscriber authentication or client authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Using External AAA Authentication Services with DHCP</i>

client

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

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the peer identity.



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

Options *client-name*—A peer identity. For L2TP clients, you can use a special name to configure a default client. This client enables the LNS to accept any LAC to establish the session. On M Series routers, use * for the default client configuration. On MX Series routers, use **default**.

The remaining statements are explained separately.

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

Related Documentation

- [Configuring the L2TP Client on page 24](#)
- [Configuring Access Profiles for L2TP or PPP Parameters on page 19](#)
- [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.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

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](#)


client-idle-timeout

Syntax	<code>client-idle-timeout <i>minutes</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> session-options]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	(J Series, MX Series, and SRX Series devices) Specify the grace period that begins after an authenticated user terminates all sessions and connections. Authentication is not required if a new connection is initiated during the grace period by the same user.
Default	The timeout is not configured.
Options	<i>minutes</i> —Number of minutes of idle time that elapse before the session is terminated. Range: 10 through 1440 minutes
Required Privilege Level	access —To view this statement in the configuration. access-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Session Options for Subscriber Access on page 48• Configuring Subscriber Session Options on page 50• <i>Removing Inactive Dynamic Subscriber VLANs</i>

client-group

Syntax	client-group [<i>group-names</i>];
Hierarchy Level	[edit access profile <i>profile-name</i> client <i>client-name</i>] [edit access profile <i>profile-name</i> session-options]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify a list of client groups that the client belongs to. If the group list is not defined as part of the client profile, the client group configured at the [edit access profile <i>profile-name</i> session-options] hierarchy level is used.
<div> NOTE: This statement is not supported on MX Series routers.</div>	
Options	<i>group-names</i> —Names of one or more groups the client belongs to, enclosed in brackets and separated by spaces—for example [g1 g2 g3] . The total length of the group name string cannot exceed 256 characters.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Session Options for Subscriber Access on page 48

client-session-timeout

Syntax	client-session-timeout <i>minutes</i> ;
Hierarchy Level	[edit access profile <i>profile-name</i> session-options]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	(J Series, MX Series, and SRX Series devices) Specify the amount of time after which user sessions are terminated, regardless of user activity (also known as a forced or hard authentication timeout).
<div style="display: flex; align-items: center;">  <div> <p>NOTE: For all subscriber types other than DHCP (such as L2TP-tunneled and PPP-terminated subscribers), the client-session-timeout value limits the subscriber session. For DHCP subscribers, the client-session-timeout value is used to limit the lease. The lease expires when the timeout value expires. If this value is not supplied by either the CLI or RADIUS, the DHCP lease does not expire.</p> </div> </div>	
Default	The timeout is not configured.
Options	<i>minutes</i> —Number of minutes after which user sessions are terminated. Range: 1 through 527040 minutes
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Understanding Session Options for Subscriber Access on page 48 • Configuring Subscriber Session Options on page 50

dead-peer-detection

Syntax	<pre>dead-peer-detection { always-send; interval <i>seconds</i>; threshold <i>number</i>; }</pre>
Hierarchy Level	[edit security ike gateway <i>gateway-name</i>]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Enable the device to use dead peer detection (DPD). DPD is a method used by devices to verify the current existence and availability of IPsec peer devices. A device performs this verification by sending encrypted IKE Phase 1 notification payloads (R-U-THERE) to peers and waiting for DPD acknowledgements (R-U-THERE-ACK).
Options	The remaining statements are explained separately.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Junos OS Security Configuration Guide</i>

dhcp-attributes (Address-Assignment Pools)

Syntax	<pre> 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; } } preferred-lifetime seconds; router [router-address]; server-identifier ip4-address; sip-server-address [ipv6-address]; sip-server-domain-name domain-name; t1-percentage percentage; t2-percentage percentage; tftp-server address; valid-lifetime seconds; wins-server [servers]; } </pre>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family <i>family</i>]
Release Information	<p>Statement introduced in Junos OS Release 9.0.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p>
Description	<p>Configure address pools that can be used by different client applications.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Address-Assignment Pools Overview</i> • <i>DHCP Attributes for Address-Assignment Pools</i> • <i>Configuring Address-Assignment Pools</i> • <i>Configuring DHCP Client-Specific Attributes</i> • <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>

domain-name (Address-Assignment Pools)

Syntax	<code>domain-name <i>domain-name</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> 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	<i>domain-name</i> —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	<ul style="list-style-type: none">• Configuring Address-Assignment Pools


drop-timeout

Syntax	<code>drop-timeout <i>milliseconds</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> client <i>client-name</i> l2tp multilink]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the drop timeout for a multilink bundle.
Options	<i>milliseconds</i> —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	<ul style="list-style-type: none">• Configuring L2TP Properties for a Client-Specific Profile on page 27

encapsulation-overhead

Syntax	<code>encapsulation-overhead bytes;</code>
Hierarchy Level	[edit access group-profile <i>profile-name</i> ppp], [edit access profile <i>profile-name</i> client <i>client-name</i> 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	<ul style="list-style-type: none"> • Configuring the PPP Attributes for a Group Profile on page 17 • Configuring PPP Properties for a Client-Specific Profile on page 31

ethernet-port-type-virtual

Syntax	<code>ethernet-port-type-virtual;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> 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 .
<div style="display: flex; align-items: center;">  <div> <p>NOTE: This statement takes precedence over the <code>nas-port-type</code> statement if you include both statements in the same access profile.</p> </div> </div>	
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring RADIUS Server Options for Subscriber Access • Configuring RADIUS Server Parameters for Subscriber Access

exclude (RADIUS)

Syntax `exclude {`

```
    acc-aggr-cir-id-asc [ access-request | accounting-start | accounting-stop ];
    acc-aggr-cir-id-bin [ access-request | accounting-start | accounting-stop ];
    acc-loop-cir-id [ access-request | accounting-start | accounting-stop ];
    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 ];
    act-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    act-data-rate-up [ access-request | accounting-start | accounting-stop ];
    act-interlv-delay-dn [ access-request | accounting-start | accounting-stop ];
    act-interlv-delay-up [ access-request | accounting-start | accounting-stop ];
    att-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    att-data-rate-up [ access-request | accounting-start | accounting-stop ];
    called-station-id [ access-request | accounting-start | accounting-stop ];
    calling-station-id [ access-request | accounting-start | accounting-stop ];
    class [ accounting-start | accounting-stop ];
    cos-shaping-rate [ 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 ];
    dsl-line-state [ access-request | accounting-start | accounting-stop ];
    dsl-type [ access-request | accounting-start | accounting-stop ];
    event-timestamp [ accounting-on | accounting-off | accounting-start | accounting-stop
    ];
    filter-id [ 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 ];
    max-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    max-data-rate-up [ access-request | accounting-start | accounting-stop ];
    max-interlv-delay-dn [ access-request | accounting-start | accounting-stop ];
    max-interlv-delay-up [ access-request | accounting-start | accounting-stop ];
    min-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    min-data-rate-up [ access-request | accounting-start | accounting-stop ];
    min-lp-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    min-lp-data-rate-up [ 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.
Options **cos-shaping-rate** and **filter-id** introduced in Junos OS Release 13.2.

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, Juniper Networks (vendor ID 4874) VSA number and name, or DSL Forum (vendor ID 3561) VSA number and name.
- **acc-aggr-cir-id-asc**—Juniper Networks VSA 26-112, Acc-Aggr-Cir-Id-Asc.
 - **acc-aggr-cir-id-bin**—Juniper Networks VSA 26-111, Acc-Aggr-Cir-Id-Bin.
 - **acc-loop-cir-id**—Juniper Networks VSA 26-110, Acc-Loop-Cir-Id.
 - **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.
 - **act-data-rate-dn**—Juniper Networks VSA 26-114, Act-Data-Rate-Dn
 - **act-data-rate-up**—Juniper Networks VSA 26-113, Act-Data-Rate-Up
 - **act-interlv-delay-dn**—Juniper Networks VSA 26-126, Act-Interlv-Delay-Dn
 - **act-interlv-delay-up**—Juniper Networks VSA 26-124, Act-Interlv-Delay-Up
 - **att-data-rate-dn**—Juniper Networks VSA 26-118, Att-Data-Rate-Dn
 - **att-data-rate-up**—Juniper Networks VSA 26-117, Att-Data-Rate-Up
 - **called-station-id**—RADIUS attribute 30, Called-Station-Id.
 - **calling-station-id**—RADIUS attribute 31, Calling-Station-Id.
 - **class**—RADIUS attribute 25, Class.
 - **cos-shaping-rate**—Juniper Networks VSA 26-177, Cos-Shaping-Rate.
 - **dhcp-gi-address**—Juniper Networks VSA 26-57, DHCP-GI-Address.
 - **dhcp-mac-address**—Juniper Networks VSA 26-56, DHCP-MAC-Address.
 - **dhcp-options**—Juniper Networks VSA 26-55, DHCP-Options.
 - **downstream-calculated-qos-rate**—Juniper Networks VSA 26-141
 - **dsl-forum-attributes**—DSL Forum VSA (vendor ID 3561) as described in RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*
 - **dsl-line-state**—Juniper Networks VSA 26-127, DSL-Line-State
 - **dsl-type**—Juniper Networks VSA 26-128, DSL-Type
 - **event-timestamp**—RADIUS attribute 55, Event-Timestamp.
 - **filter-id**—RADIUS attribute 11, Filter-Id.
 - **framed-ip-address**—RADIUS attribute 8, Framed-IP-Address.
 - **framed-ip-netmask**—RADIUS attribute 9, Framed-IP-Netmask.
 - **input-filter**—Juniper Networks VSA 26-10, Ingress-Policy-Name.
 - **input-gigapackets**—Juniper Networks VSA 26-42, Acct-Input-Gigapackets.

- **input-gigawords**—RADIUS attribute 52, Acct-Input-Gigawords.
- **interface-description**—Juniper Networks VSA 26-53, Interface-Desc.
- **max-data-rate-dn**—Juniper Networks VSA 26-120, Max-Data-Rate-Dn
- **max-data-rate-up**—Juniper Networks VSA 26-119, Max-Data-Rate-Up
- **max-interlv-delay-dn**—Juniper Networks VSA 26-125, Max-Interlv-Delay-Dn
- **max-interlv-delay-up**—Juniper Networks VSA 26-123, Max-Interlv-Delay-Up
- **min-data-rate-dn**—Juniper Networks VSA 26-116, Min-Data-Rate-Dn
- **min-data-rate-up**—Juniper Networks VSA 26-115, Min-Data-Rate-Up
- **min-lp-data-rate-dn**—Juniper Networks VSA 26-122, Min-Lp-Data-Rate-Dn
- **min-lp-data-rate-up**—Juniper Networks VSA 26-121, Min-Lp-Data-Rate-Up
- **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 Networks VSA 26-11, Egress-Policy-Name.
- **output-gigapackets**—Juniper Networks VSA 26-43, Acct-Output-Gigapackets.
- **output-gigawords**—RADIUS attribute 53, Acct-Output-Gigawords.
- **upstream-calculated-qos-rate**—Juniper Networks 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 (Access)

Syntax	<code>fragment-threshold <i>bytes</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> client <i>client-name</i> l2tp multilink]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the fragmentation threshold for a multilink bundle.
Options	<i>bytes</i> —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	<ul style="list-style-type: none">• Configuring L2TP Properties for a Client-Specific Profile on page 27• multilink on page 107

framed-ip-address

Syntax	<code>framed-ip-address <i>address</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> client <i>client-name</i> ppp]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify a framed IP address.
Options	<i>address</i> —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	<ul style="list-style-type: none">• Configuring PPP Properties for a Client-Specific Profile on page 31

framed-pool

Syntax	<code>framed-pool <i>framed-pool</i>;</code>
Hierarchy Level	[edit access group-profile <i>profile-name</i> ppp], [edit access profile <i>profile-name</i> client <i>client-name</i> ppp]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the address pool.
Options	<i>framed-pool</i> —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	<ul style="list-style-type: none"> • Configuring the PPP Attributes for a Group Profile on page 17 • Configuring PPP Properties for a Client-Specific Profile on page 31

grace-period

Syntax	<code>grace-period <i>seconds</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> 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	<i>seconds</i> —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	<ul style="list-style-type: none"> • Configuring Address-Assignment Pools

group-profile (Associating with Client)

Syntax	<code>group-profile <i>profile-name</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> client <i>client-name</i>]
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	<i>profile-name</i> —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	<ul style="list-style-type: none">• Referencing the Group Profile from the L2TP Profile on page 27

group-profile (Group Profile)

Syntax

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

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the group profile.



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

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

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- [Configuring the Group Profile for Defining L2TP Attributes on page 16](#)
- [Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile](#)


hardware-address

Syntax	<code>hardware-address <i>mac-address</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family (inet inet6) host <i>hostname</i>]
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	<i>mac-address</i> —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	<ul style="list-style-type: none">• <i>Configuring Address-Assignment Pools</i>

host (Address-Assignment Pools)

Syntax	<pre>host <i>hostname</i> { hardware-address <i>mac-address</i>; ip-address <i>ip-address</i>; }</pre>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family (inet inet6)]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Configure a static binding for the specified client.
Options	<i>hostname</i> —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	<ul style="list-style-type: none">• <i>Address-Assignment Pools Overview</i>• <i>Configuring Address-Assignment Pools</i>

idle-timeout (Access)

Syntax	<code>idle-timeout seconds;</code>
Hierarchy Level	<code>[edit access group-profile <i>profile-name</i> ppp],</code> <code>[edit access profile <i>profile-name</i> client <i>client-name</i> ppp]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	<p>Configure the idle timeout for a user. The router might consider a PPP session to be idle because of the following reasons:</p> <ul style="list-style-type: none"> • 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	<p>seconds—Number of seconds a user can remain idle before the session is terminated.</p> <p>Range: 0 through 4,294,967,295 seconds</p> <p>Default: 0</p>
<div>  NOTE: The [edit access] hierarchy is not available on QFabric systems. </div>	
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the PPP Attributes for a Group Profile on page 17 • Configuring PPP Properties for a Client-Specific Profile on page 31 • Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile

ignore

Syntax	<pre>ignore { dynamic-iflset-name; framed-ip-netmask; input-filter; logical-system-routing-instance; output-filter; }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i> 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	<p>dynamic-iflset-name—Ignore Interface-Set/Dynamic-Ifset-Name (VSA 26-130).</p> <p>framed-ip-netmask—Ignore Framed-IP-Netmask (RADIUS attribute 9).</p> <p>input-filter—Ignore Ingress-Policy-Name (VSA 26-10).</p> <p>logical-system-routing-instance—Ignore Virtual-Router (VSA 26-1).</p> <p>output-filter—Ignore Egress-Policy-Name (VSA 26-11).</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Parameters for Subscriber Access</i>

ike (Access Profile)

Syntax

```
ike {
    allowed-proxy-pair {
        remote remote-proxy-address local local-proxy-address;
    }
    dead-peer-detection {
        interval seconds
        threshold number
    }
    ike-policy policy-name;
    initiate-dead-peer-detection;
    interface-id string-value;
    ipsec-policy ipsec-policy;
    pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
    reverse-route
}
```

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 23](#)

ike-policy

Syntax	<code>ike-policy <i>policy-name</i>;</code>
Hierarchy Level	<code>[edit access profile <i>profile-name</i> client <i>client-name</i> ike]</code>
Release Information	Statement introduced in Junos OS Release 8.2.
Description	Specify the IKE policy used to authenticate dynamic peers during IKE negotiation.
Options	<i>policy-name</i> —The name of an IKE policy configured at the <code>[edit services ipsec-vpn ike policy <i>policy-name</i>]</code> 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 <i>Junos OS Services Interfaces Library for Routing Devices</i> .
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an IKE Access Profile on page 23• <i>Junos IPsec Feature Guide</i>• <i>Junos OS Services Interfaces Library for Routing Devices</i>

immediate-update

Syntax	<code>immediate-update;</code>
Hierarchy Level	<code>[edit access profile <i>profile-name</i> accounting]</code>
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	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Parameters for Subscriber Access</i>• <i>Configuring Per-Subscriber Session Accounting</i>

initiate-dead-peer-detection (IPsec)

Syntax	<code>initiate-dead-peer-detection;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> client <i>client-name</i> 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	<ul style="list-style-type: none"> • Configuring an IKE Access Profile on page 23

interface-description-format

Syntax	<pre>interface-description-format { exclude-adapter; exclude-sub-interface; }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p> <p>Options exclude-adapter and exclude-sub-interface introduced in Junos OS Release 10.4.</p>
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	<p>exclude-adapter—Exclude the adapter from the interface description.</p> <p>exclude-sub-interface—Exclude the subinterface from the interface description.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring RADIUS Server Options for Subscriber Access • RADIUS Server Options for Subscriber Access

interface-id

Syntax	<code>interface-id <i>interface-id</i>;</code>
Hierarchy Level	[edit access group-profile <i>profile-name</i> l2tp], [edit access group-profile <i>profile-name</i> ppp], [edit access profile <i>profile-name</i> client <i>client-name</i> ike], [edit access profile <i>profile-name</i> client <i>client-name</i> l2tp], [edit access profile <i>profile-name</i> client <i>client-name</i> ppp]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the interface identifier.
Options	<i>interface-id</i> —Identifier for the interface representing a Layer 2 Tunneling Protocol (L2TP) session configured at the [edit interfaces <i>interface-name</i> unit <i>local-unit-number</i> dial-options] hierarchy level. For more information about the interface ID, see <i>Services Interface Naming Overview</i> .
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring L2TP for a Group Profile on page 17• Configuring the PPP Attributes for a Group Profile on page 17• Configuring L2TP Properties for a Client-Specific Profile on page 27• Configuring PPP Properties for a Client-Specific Profile on page 31• Configuring an IKE Access Profile on page 23• Configuring an L2TP Access Profile on the LNS

ip-address

Syntax	<code>ip-address <i>ip-address</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet host <i>hostname</i>]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Specify the reserved IP address assigned to the client.
Options	<i>ip-address</i> —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	<ul style="list-style-type: none">• Configuring Address-Assignment Pools• Configuring Static Address Assignment


keepalive

Syntax	<code>keepalive seconds;</code>
Hierarchy Level	[edit access group-profile <i>profile-name</i> ppp], [edit access profile <i>profile-name</i> client <i>client-name</i> ppp]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the keepalive interval for an L2TP tunnel.
Options	<p>seconds—Time period that must elapse before the Junos OS checks the status of the Point-to-Point Protocol (PPP) session by sending an echo request to the peer.</p> <p>For L2TP on MX Series routers, the minimum recommended interval is 30 seconds. A value of 0 disables generation of keepalive messages from the LNS.</p> <p>Range: 0 through 32,767 seconds</p> <p>Default: 30 seconds</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the PPP Attributes for a Group Profile on page 17 • Configuring PPP Properties for a Client-Specific Profile on page 31 • Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile

keepalive-retries

Syntax	<code>keepalive-retries <i>number-of-retries</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> client <i>client-name</i> 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	<p><i>number-of-retries</i>—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.</p> <p>Range: 3 through 32,767 times</p> <p>Default: 10 times</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring PPP Properties for a Client-Specific Profile on page 31• keepalive on page 99

l2tp (Group Profile)

Syntax	<pre>l2tp { interface-id <i>interface-id</i>; lcp-renegotiation; local-chap; maximum-sessions-per-tunnel <i>number</i>; }</pre>
Hierarchy Level	[edit access group-profile <i>profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure the Layer 2 Tunneling Protocol for a group profile.</p> <p>The remaining statements are explained separately.</p>
<div>  <p>NOTE: This statement is not supported for L2TP LNS on MX Series routers.</p> </div>	
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • 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 27](#)

lcp-renegotiation

Syntax	lcp-renegotiation;
Hierarchy Level	[edit access group-profile <i>profile-name</i> l2tp], [edit access profile <i>profile-name</i> client <i>client-name</i> l2tp]
Release Information	Statement introduced before Junos OS Release 7.4.
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.
<div>  NOTE: This statement is not supported at the [edit access group-profile l2tp] hierarchy level for L2TP LNS on MX Series routers. </div>	
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring L2TP for a Group Profile on page 17 • Configuring L2TP Properties for a Client-Specific Profile on page 27 • Configuring an L2TP Access Profile on the LNS

local-chap

Syntax	local-chap;
Hierarchy Level	[edit access group-profile <i>profile-name</i> l2tp], [edit access profile <i>profile-name</i> client <i>client-name</i> 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.
<div> NOTE: This statement is not supported for L2TP LNS on MX Series routers.</div>	
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring L2TP for a Group Profile on page 17• Configuring L2TP Properties for a Client-Specific Profile on page 27

maximum-lease-time

Syntax	<code>maximum-lease-time <i>seconds</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> 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. The maximum-lease-time is mutually exclusive with both the preferred-lifetime and the valid-lifetime , and cannot be configured with either timer.
Options	<p>seconds—Maximum number of seconds the lease can be held.</p> <p>Range: 30 through 4,294,967,295 seconds</p> <p>Default: 86,400 (24 hours)</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Address-Assignment Pools</i> • <i>DHCP Attributes for Address-Assignment Pools</i> • <i>preferred-lifetime (Address-Assignment Pools)</i> • <i>valid-lifetime (Address-Assignment Pools)</i>

maximum-sessions-per-tunnel

Syntax	<code>maximum-sessions-per-tunnel <i>number</i>;</code>
Hierarchy Level	<code>[edit access group-profile <i>l2tp</i>],</code> <code>[edit access profile <i>profile-name</i> client <i>client-name</i> <i>l2tp</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
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	<i>number</i> —Maximum number of sessions for a Layer 2 tunnel.
Required Privilege Level	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring L2TP for a Group Profile on page 17• Configuring L2TP Properties for a Client-Specific Profile on page 27• Configuring an L2TP Access Profile on the LNS

multilink

Syntax	<code>multilink { drop-timeout <i>milliseconds</i>; fragment-threshold <i>bytes</i>; }</code>
Hierarchy Level	[edit access <i>profile profile-name client client-name l2tp</i>]
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	<ul style="list-style-type: none"> • Configuring L2TP Properties for a Client-Specific Profile on page 27

name-server

Syntax	<code>name-server [<i>server-names</i>];</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet <i>dhcp-attributes</i>]
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	<i>server-names</i> —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	<ul style="list-style-type: none"> • Configuring Address-Assignment Pools

nas-identifier

Syntax	<code>nas-identifier <i>identifier-value</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> 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	<i>identifier-value</i> —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	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Options for Subscriber Access</i>• <i>Configuring RADIUS Server Parameters for Subscriber Access</i>

nas-port-extended-format (Access Profile)

Syntax

```
nas-port-extended-format {
  adapter-width width;
  ae-width width;
  port-width width;
  slot-width width;
  stacked-vlan-width width;
  vlan-width width;
  atm {
    adapter-width width;
    port-width width;
    slot-width width;
    vci-width width;
    vpi-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.
 Option **ae-width** introduced in Junos OS Release 12.1.
 Option **stacked** introduced in Junos OS Release 12.3.
 Option **atm** introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases.
 Option **atm** supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description In an access profile, 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. You can use the same access profile to configure the NAS-Port extended format for Ethernet subscribers and ATM subscribers.

Options

- adapter-width *width***—Number of bits in the adapter field.
- ae-width *width***—Number of bits in the aggregated Ethernet identifier field.
- port-width *width***—Number of bits in the port field.
- slot-width *width***—Number of bits in the slot field.
- stacked**—Include stacked VLAN IDs, in addition to VLAN IDs, in the NAS-Port extended format.
- stacked-vlan-width *width***—Number of bits in the SVLAN ID field.
- vlan-width *width***—Number of bits in the VLAN ID field.
- atm**—Configure the NAS-Port extended format for ATM subscribers; options include:
 - **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.
- **vci-width *width***—Number of bits in the ATM virtual circuit identifier (VCI) field.
- **vpi-width *width***—Number of bits in the ATM virtual path identifier (VPI) field.



NOTE: Each field can be 0 through 32 bits wide; however, the total of the widths of all fields must not exceed 32 bits, or the configuration fails.

The router may truncate the values of individual fields depending on the bit width you specify.

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring RADIUS Server Options for Subscriber Access</i> • <i>Configuring RADIUS Server Parameters for Subscriber Access</i>

netbios-node-type

Syntax	netbios-node-type <i>node-type</i> ;
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> 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	<p><i>node-type</i>—One of the following node types:</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • <i>Configuring Address-Assignment Pools</i>

network

Syntax	<code>network <i>ip-prefix</i> </<i>prefix-length</i>>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Configure subnet information for an IPv4 address-assignment pool.
Options	<p><i>ip-prefix</i>—IP version 4 address or prefix value.</p> <p><i>prefix-length</i>—(Optional) Subnet mask.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Address-Assignment Pools

option

Syntax	<pre>option { [(<i>id-number</i> <i>option-type</i> <i>option-value</i>) (<i>id-number</i> array <i>option-type</i> <i>option-value</i>)]; }</pre>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family (inet inet6) dhcp-attributes]
Release Information	<p>Statement introduced in Junos OS Release 9.0.</p> <p>hex-string option type introduced in Junos OS Release 13.3.</p>
Description	Specify user-defined options that are added to client packets.
Options	<p>array—An option can include an array of option types.</p> <p>id-number—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.</p> <p>option-type—Any of the following types: byte, byte-stream, flag, hex-string, integer, ip-address, short, string, unsigned-integer, or unsigned-short.</p> <p>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).</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Address-Assignment Pools

option-82 (Address-Assignment Pools)

Syntax	<pre>option-82 { circuit-id value range named-range; remote-id value range named-range; }</pre>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes option-match]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	<p>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.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Address-Assignment Pools</i>

option-match

Syntax	<pre>option-match { option-82 { circuit-id value range named-range; remote-id value range named-range; } }</pre>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	<p>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.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Address-Assignment Pools</i>

options (Access Profile)

```
Syntax  options {
    accounting-session-id-format (decimal | description);
    calling-station-id-delimiter delimiter-character;
    calling-station-id-format {
        agent-circuit-id;
        agent-remote-id;
        interface-description;
        nas-identifier;
    }
    client-accounting-algorithm (direct | round-robin);
    client-authentication-algorithm (direct | round-robin);
    coa-dynamic-variable-validation;
    ethernet-port-type-virtual;
    access-loop-id-local;
    interface-description-format {
        exclude-adapter;
        exclude-sub-interface;
    }
    ip-address-change-notify message;
    juniper-dsl-attributes;
    nas-identifier identifier-value;
    nas-port-extended-format {
        adapter-width width;
        ae-width width;
        port-width width;
        slot-width width;
        stacked-vlan-width width;
        vlan-width width;
        atm {
            adapter-width width;
            port-width width;
            slot-width width;
            vci-width width;
            vpi-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 <i>profile-name</i> 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	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Options for Subscriber Access</i>• <i>RADIUS Server Options for Subscriber Access</i>

order

Syntax	order [<i>accounting-method</i>];
Hierarchy Level	[edit access profile <i>profile-name</i> 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	<i>accounting-method</i> —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	<ul style="list-style-type: none">• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

pap-password

Syntax	<code>pap-password password;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> client <i>client-name</i>]
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	<code>password</code> —PAP password.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the PAP Password for an L2TP Profile on page 30

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.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Configure the name of an address-assignment pool.



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

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*
- *Configuring a DHCP Server on Switches (CLI Procedure)*

port

Syntax	<code>port <i>port-number</i>;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
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	<i>port-number</i> —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	<ul style="list-style-type: none">• <i>Configuring Router or Switch Interaction with RADIUS Servers</i>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

ppp (Group Profile)

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

Hierarchy Level [edit access [group-profile](#) *profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure PPP properties for a group profile.

The remaining statements are explained separately.



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

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

Related Documentation

- [Configuring the PPP Attributes for a Group Profile on page 17](#)
- [Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile](#)

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 31](#)

ppp-authentication

Syntax	<code>ppp-authentication (chap pap);</code>
Hierarchy Level	[edit access profile <i>profile-name</i> client <i>client-name</i> 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Configuring L2TP Properties for a Client-Specific Profile on page 27

ppp-profile

Syntax	<code>ppp-profile <i>profile-name</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> client <i>client-name</i> 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	<i>profile-name</i> —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	<ul style="list-style-type: none">• Configuring RADIUS Authentication for an L2TP Client and Profile on page 45

pre-shared-key (Access Profile)

Syntax	<code>pre-shared-key (ascii-text <i>character-string</i> hexadecimal <i>hexadecimal-digits</i>);</code>
Hierarchy Level	<code>[edit access profile <i>profile-name</i> client <i>client-name</i> ike]</code>
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	<p><code>ascii-text <i>character-string</i></code>—Authentication key in ASCII format.</p> <p><code>hexadecimal <i>hexadecimal-digits</i></code>—Authentication key in hexadecimal format.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring an IKE Access Profile on page 23

primary-dns

Syntax	<code>primary-dns <i>primary-dns</i>;</code>
Hierarchy Level	<p><code>[edit access group-profile <i>profile-name</i> client <i>client-name</i> ppp],</code></p> <p><code>[edit access profile <i>profile-name</i> ppp]</code></p>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the primary Domain Name System (DNS) server.
Options	<code><i>primary-dns</i></code> —An IPv4 address.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the PPP Attributes for a Group Profile on page 17 • Configuring PPP Properties for a Client-Specific Profile on page 31

primary-wins

Syntax	<code>primary-wins <i>primary-wins</i>;</code>
Hierarchy Level	[edit access group-profile <i>profile-name</i> client <i>client-name</i> ppp], [edit access profile <i>profile-name</i> ppp]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the primary Windows Internet name server.
Options	<i>primary-wins</i> —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	<ul style="list-style-type: none">• Configuring the PPP Attributes for a Group Profile on page 17• Configuring PPP Properties for a Client-Specific Profile on page 31

profile (Access)

```
Syntax  profile profile-name {
    accounting {
        address-change-immediate-update
        accounting-stop-on-access-deny;
        accounting-stop-on-failure;
        ancp-speed-change-immediate-update;
        coa-immediate-update;
        coa-no-override service-class-attribute;
        duplication;
        duplication-vrf {
            access-profile-name profile-name;
            vrf-name vrf-name;
        }
        immediate-update;
        order [ accounting-method ];
        send-acct-status-on-config-change;
        statistics (time | volume-time);
        update-interval minutes;
        wait-for-acct-on-ack;
    }
    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 {
            aaa-access-profile profile-name;
            interface-id interface-id;
            lcp-renegotiation;
            local-chap;
            maximum-sessions-per-tunnel number;
            multilink {
                drop-timeout milliseconds;
                fragment-threshold bytes;
            }
            ppp-authentication (chap | pap);
            ppp-profile profile-name;
            shared-secret shared-secret;
        }
        pap-password pap-password;
        ppp {
            cell-overhead;
            encapsulation-overhead bytes;
            framed-ip-address ip-address;
            framed-pool framed-pool;
        }
    }
}
```

```
    idle-timeout seconds;
    interface-id interface-id;
    keepalive seconds;
    primary-dns primary-dns;
    primary-wins primary-wins;
    secondary-dns secondary-dns;
    secondary-wins secondary-wins;
}
user-group-profile profile-name;
}
domain-name-server;
domain-name-server-inet;
domain-name-server-inet6;
preauthentication-order preauthentication-method;
provisioning-order (gx-plus | jsrc);
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);
    calling-station-id-delimiter delimiter-character;
    calling-station-id-format {
        agent-circuit-id;
        agent-remote-id;
        interface-description;
        nas-identifier;
    }
    client-accounting-algorithm (direct | round-robin);
    client-authentication-algorithm (direct | round-robin);
    coa-dynamic-variable-validation;
    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;
    ae-width width;
    port-width width;
    slot-width width;
    stacked-vlan-width width;
    vlan-width width;
    atm {
```

```

        adapter-width width;
        port-width width;
        slot-width width;
        vci-width width;
        vpi-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;
}
preauthentication-server ip-address;
}
radius-server server-address {
    accounting-port port-number;
    accounting-retry number;
    accounting-timeout seconds;
    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);
}
session-options {
    client-group [ group-names ];
    client-idle-timeout minutes;
    client-session-timeout minutes;
}
}

```

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 admin—To view this statement in the configuration.
Level 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 27](#)
- [Configuring an L2TP LNS with Inline Service Interfaces](#)
- [Configuring PPP Properties for a Client-Specific Profile on page 31](#)
- [Configuring Service Accounting with JSRC](#)
- [AAA Service Framework Overview](#)
- [show network-access aaa statistics](#)
- [clear network-access aaa statistics on page 148](#)

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);
    calling-station-id-delimiter delimiter-character;
    calling-station-id-format {
        agent-circuit-id;
        agent-remote-id;
        interface-description;
        nas-identifier;
    }
    client-accounting-algorithm (direct | round-robin);
    client-authentication-algorithm (direct | round-robin);
    coa-dynamic-variable-validation;
    ethernet-port-type-virtual;
    interface-description-format {
        exclude-adapter;
        exclude-sub-interface;
    }
    ip-address-change-notify message;
    juniper-dsl-attributes;
    nas-identifier identifier-value;
    nas-port-extended-format {
        adapter-width width;
        ae-width width;
        port-width width;
        slot-width width;
        stacked-vlan-width width;
        vlan-width width;
        atm {
            adapter-width width;
            port-width width;
            slot-width width;
            vci-width width;
            vpi-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;
}
preauthentication-server ip-address;
}
```

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	<pre>radius-disconnect { client-address { secret password; } }</pre>
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	<p><i>client-address</i>—A valid IP address configured on one of the router interfaces.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the RADIUS Disconnect Server for L2TP on page 44

radius-disconnect-port

Syntax	<code>radius-disconnect-port <i>port-number</i>;</code>
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	<i>port-number</i> —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	<ul style="list-style-type: none">• Configuring the RADIUS Disconnect Server for L2TP on page 44

radius-server

Syntax	<pre>radius-server server-address { accounting-port port-number; accounting-retry number; accounting-timeout seconds; port port-number; retry attempts; routing-instance routing-instance-name; secret password; max-outstanding-requests value; source-address source-address; timeout seconds; }</pre>
Hierarchy Level	<p>[edit access],</p> <p>[edit access profile profile-name]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	<p>Configure RADIUS for subscriber access management, L2TP, or PPP.</p> <p>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.</p>
Options	<p>server-address—Address of the RADIUS authentication server.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • 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 • Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) • show network-access aaa statistics • clear network-access aaa statistics on page 148

range (Address-Assignment Pools)

Syntax	<pre>range range-name { high upper-limit; low lower-limit; prefix-length prefix-length; }</pre>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family (inet inet6)]
Release Information	Statement introduced in Junos OS Release 9.0. IPv6 support introduced in Junos OS Release 10.0. Statement introduced in Junos OS Release 12.3 for EX Series switches.
Description	Configure a named range of IPv4 addresses or IPv6 prefixes, used within an address-assignment pool.
Options	<p>high upper-limit—Upper limit of an address range or IPv6 prefix range.</p> <p>low lower-limit—Lower limit of an address range or IPv6 prefix range.</p> <p>prefix-length prefix-length—Assigned length of the IPv6 prefix.</p> <p>range-name—Name assigned to the range of IPv4 addresses or IPv6 prefixes.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Address-Assignment Pools Overview</i>• <i>Configuring Address-Assignment Pools</i>• <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>

remote-id

Syntax	<code>remote-id value range <i>named-range</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> 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	<p>range <i>named-range</i>—Name of the address-assignment pool range to use.</p> <p>value—String for Agent Remote ID suboption (suboption 2) of the DHCP relay agent information option (option 82) in DHCP packets.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Address-Assignment Pools</i>

retry

Syntax	<code>retry attempts;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
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 30 Default: 3
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>• <i>Configuring Router or Switch Interaction with RADIUS Servers</i>• Example: Configuring CHAP Authentication with RADIUS on page 9• Configuring RADIUS Authentication for L2TP on page 37• timeout on page 141

reverse-route

Syntax	<code>reverse-route { preference <i>metric-value</i>; }</code>
Hierarchy Level	[edit access profile <i>profile-name</i> client <i>client-name</i> ike]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	(M Series and MX Series routers with an AS or MultiServices PIC only) Configure a reverse route for dynamic endpoint IPsec tunnels. 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.

revert-interval

Syntax	<code>revert-interval <i>interval</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius options], [edit access 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	<i>interval</i> —Amount of time to wait. Range: 0 through 604800 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	<ul style="list-style-type: none"> • <i>Configuring RADIUS Server Options for Subscriber Access</i> • <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

router (Address-Assignment Pools)

Syntax	<code>router [<i>router-address</i>];</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> 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	<i>router-address</i> —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	<ul style="list-style-type: none"> • <i>Configuring Address-Assignment Pools</i>

routing-instance

Syntax	<code>routing-instance <i>routing-instance-name</i>;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
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	<i>routing-instance-name</i> —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	<ul style="list-style-type: none">• Configuring the PPP Authentication Protocol on page 8• Configuring Authentication and Accounting Parameters for Subscriber Access

secondary-dns

Syntax	<code>secondary-dns <i>secondary-dns</i>;</code>
Hierarchy Level	[edit access group-profile <i>profile-name</i> ppp], [edit access profile <i>profile-name</i> client <i>client-name</i> ppp]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the secondary DNS server.
Options	<i>secondary-dns</i> —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	<ul style="list-style-type: none">• Configuring the PPP Attributes for a Group Profile on page 17• Configuring PPP Properties for a Client-Specific Profile on page 31

secondary-wins

Syntax	<code>secondary-wins secondary-wins;</code>
Hierarchy Level	[edit access group-profile <i>profile-name</i> ppp], [edit access profile <i>profile-name</i> client <i>client-name</i> ppp]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the secondary Windows Internet name server.
Options	<i>secondary-wins</i> —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	<ul style="list-style-type: none"> • Configuring the PPP Attributes for a Group Profile on page 17 • Configuring PPP Properties for a Client-Specific Profile on page 31

secret

Syntax	<code>secret password;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius-server <i>server-address</i>], [edit access radius-disconnect <i>client-address</i>], [edit access radius-server <i>server-address</i>]
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	<i>password</i> —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	<ul style="list-style-type: none"> • 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 44 • Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)

session-options

Syntax	<pre>session-options { client-group [<i>group-names</i>]; client-idle-timeout <i>minutes</i>; client-session-timeout <i>minutes</i>; }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	<p>(J Series, MX Series, and SRX Series devices) Define options that control a user's session after successful authentication.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Understanding Session Options for Subscriber Access on page 48• Configuring Subscriber Session Options on page 50

shared-secret

Syntax	<pre>shared-secret <i>shared-secret</i>;</pre>
Hierarchy Level	[edit access profile <i>profile-name</i> client <i>client-name</i> l2tp]
Release Information	Statement introduced in Junos OS Release 7.4.
Description	Configure the shared secret.
Options	<i>shared-secret</i> —Shared secret key for authenticating the peer.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring L2TP Properties for a Client-Specific Profile on page 27• Configuring an L2TP Access Profile on the LNS

source-address

Syntax	<code>source-address source-address;</code>
Hierarchy Level	<code>[edit access radius-server server-address],</code> <code>[edit access profile <i>profile-name</i> radius-server server-address]</code>
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	<i>source-address</i> —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	<ul style="list-style-type: none">• <i>Configuring Router or Switch Interaction with RADIUS Servers</i>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>• Example: Configuring CHAP Authentication with RADIUS on page 9• Configuring RADIUS Authentication for L2TP on page 37

statistics (Access Profile)

Syntax	statistics (time volume-time);
Hierarchy Level	[edit access profile <i>profile-name</i> 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	<ul style="list-style-type: none">• <i>Mobile IP Home Agent Elements and Behavior</i>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

tftp-server

Syntax	tftp-server <i>ip-address</i> ;
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> 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	<ul style="list-style-type: none">• <i>Configuring Address-Assignment Pools</i>


timeout (RADIUS)

Syntax	<code>timeout seconds;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
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	<ul style="list-style-type: none">• <i>Configuring Router or Switch Interaction with RADIUS Servers</i>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>• Example: Configuring CHAP Authentication with RADIUS on page 9• Configuring RADIUS Authentication for L2TP on page 37

update-interval

Syntax	update-interval <i>minutes</i> ;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Enable interim accounting updates and 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. All values are rounded up to the next higher multiple of 10. For example, the values 811 through 819 are all accepted by the CLI, but are all rounded up to 820. 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	<ul style="list-style-type: none">• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

user-group-profile

Syntax	<code>user-group-profile <i>profile-name</i>;</code>
Hierarchy Level	<code>[edit access profile <i>profile-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Apply a configured PPP group profile to PPP users.
<div>  <p>NOTE: If <code><user-group-profile></code> is modified or deleted, the existing LNS subscribers, which were using this Layer 2 Tunneling Protocol client configuration, will go down.</p> </div>	
Options	<i>profile-name</i> —Name of a PPP group profile configured at the <code>[edit access group-profile <i>profile-name</i>]</code> hierarchy level.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Applying a Configured PPP Group Profile to a Tunnel on page 33 • Configuring an L2TP Access Profile on the LNS

vlan-nas-port-stacked-format

Syntax	<code>vlan-nas-port-stacked-format;</code>
Hierarchy Level	<code>[edit access profile <i>profile-name</i> radius options]</code>
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	<ul style="list-style-type: none"> • Configuring RADIUS Server Options for Subscriber Access • Configuring Authentication and Accounting Parameters for Subscriber Access

wins-server (Access)

Syntax	<code>wins-server { <code>ipv4-address</code>; }</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> 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	<i>ipv4-address</i> —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	<ul style="list-style-type: none">• <i>Configuring Address-Assignment Pools</i>

PART 3

Administration

- [Administrative Commands on page 147](#)
- [Monitoring Commands on page 159](#)

CHAPTER 5

Administrative Commands

- `clear network-access aaa statistics`
- `clear network-access aaa subscriber`
- `clear services l2tp session`
- `clear services l2tp tunnel statistics`
- `show services l2tp radius`

clear network-access aaa statistics

Syntax	<code>clear network-access aaa statistics</code> <code><accounting></code> <code><address-assignment (client pool <i>pool-name</i>)></code> <code><authentication></code> <code><dynamic-requests></code> <code><radius></code> <code><re-authentication></code> <code><terminate-code></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 <i>pool-name</i> —(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
Related Documentation	<ul style="list-style-type: none">• <i>Verifying and Managing Subscriber AAA Information</i>
List of Sample Output	clear network-access aaa statistics accounting on page 148 clear network-access aaa statistics address-assignment pool on page 149 clear network-access aaa statistics radius on page 149
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 address-assignment pool`

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

`clear network-access aaa statistics radius`

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

clear network-access aaa subscriber

Syntax	<code>clear network-access aaa subscriber</code> <code><statistics username <i>username</i>></code> <code><username <i>username</i>></code>
Release Information	Command introduced in Junos OS Release 9.1.
Description	Clear AAA subscriber statistics and log out subscribers.
Options	statistics username <i>username</i> —Clear AAA subscriber statistics and log out the subscriber. username <i>username</i> —Log out the AAA subscriber.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• <i>Verifying and Managing Subscriber AAA Information</i>
List of Sample Output	clear network-access aaa subscriber statistics username on page 150 clear network-access aaa subscriber username on page 150
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 <i>interface-name</i> local-gateway <i>gateway-address</i> local-gateway-name <i>gateway-name</i> local-session-id <i>session-id</i> local-tunnel-id <i>tunnel-id</i> peer-gateway <i>gateway-address</i> peer-gateway-name <i>gateway-name</i> tunnel-group <i>group-name</i> user <i>username</i>)
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M10i and M7i routers only) Clear Layer 2 Tunneling Protocol (L2TP) sessions on LNS. (MX Series routers only) Clear L2TP sessions on LAC and LNS.
Options	<p>all—Close all L2TP sessions.</p> <p>interface <i>interface-name</i>—Clear only the L2TP sessions using the specified adaptive services or inline services interface. The interface type depends on the line card as follows:</p> <ul style="list-style-type: none"> • si-<i>fpc/pic/port</i>—MPCs on MX Series routers only. This option is not available for L2TP on M Series routers. • sp-<i>fpc/pic/port</i>—AS or Multiservices PICs on M7i, M10i, and M120 routers only. This option is not available for L2TP on MX Series routers. <p>local-gateway <i>gateway-address</i>—Clear only the L2TP sessions associated with the specified local gateway address.</p> <p>local-gateway-name <i>gateway-name</i>—Clear only the L2TP sessions associated with the specified local gateway name.</p> <p>local-session-id <i>session-id</i>—Clear only the L2TP sessions with this identifier for the local endpoint of the L2TP session.</p> <p>local-tunnel-id <i>tunnel-id</i>—Clear only the L2TP sessions associated with the specified local tunnel identifier.</p> <p>peer-gateway <i>gateway-address</i>—Clear only the L2TP sessions associated with the peer gateway with the specified address.</p> <p>peer-gateway-name <i>gateway-name</i>—Clear only the L2TP sessions associated with the peer gateway with the specified name.</p> <p>tunnel-group <i>group-name</i>—Clear only the L2TP sessions associated with the specified tunnel group. This option is not available for L2TP LAC on MX Series routers.</p> <p>user <i>username</i>—(M Series routers only) Clear only the L2TP sessions for the specified username.</p>
Required Privilege Level	clear

- Related Documentation**
- [L2TP Services Configuration Overview](#)
 - [L2TP Minimum Configuration](#)
 - [clear services l2tp session statistics](#)
 - [show services l2tp session on page 160](#)

List of Sample Output [clear services l2tp session on page 152](#)
[clear services l2tp session interface on page 152](#)

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

Sample Output

[clear services l2tp session](#)

```
user@host> clear services l2tp session 31694

Session 31694 closed
```

Sample Output

[clear services l2tp session interface](#)

```
user@host> show services l2tp session Tunnel local ID: 17185
Local Remote State Interface Interface
ID ID unit Name
5117 1 Established 1073741828 si-2/0/0
34915 2 Established 1073741829 si-2/1/0
6454 3 Established 1073741830 si-2/0/0
46142 4 Established 1073741831 si-2/1/0

user@host> clear services l2tp session interface si-2/0/0
Session 5117 closed
Session 6454 closed

user@host> show services l2tp session Tunnel local ID: 17185
Local Remote State Interface Interface
ID ID unit Name
34915 2 Established 1073741829 si-2/1/0
46142 4 Established 1073741831 si-2/1/0
```


clear services l2tp tunnel statistics

Syntax	clear services l2tp tunnel statistics (all interface <i>sp-fpc/pic/port</i> local-gateway <i>gateway-address</i> local-gateway-name <i>gateway-name</i> local-tunnel-id <i>tunnel-id</i> peer-gateway <i>gateway-address</i> peer-gateway-name <i>gateway-name</i> tunnel-group <i>group-name</i>)
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	<p>all—Clear statistics for all L2TP tunnels.</p> <p>interface <i>sp-fpc/pic/port</i>—Clear statistics for only the L2TP tunnels using the specified adaptive services interface. This option is not available for L2TP LAC on MX Series routers.</p> <p>local-gateway <i>gateway-address</i>—Clear statistics for only the L2TP tunnels associated with the local gateway with the specified address.</p> <p>local-gateway-name <i>gateway-name</i>—Clear statistics for only the L2TP tunnels associated with the local gateway with the specified name.</p> <p>local-tunnel-id <i>tunnel-id</i>—Clear statistics for only the L2TP tunnels that have the specified local tunnel identifier.</p> <p>peer-gateway <i>gateway-address</i>—Clear statistics for only the L2TP tunnels associated with the peer gateway with the specified address.</p> <p>peer-gateway-name <i>gateway-name</i>—Clear statistics for only the L2TP tunnels associated with the peer gateway with the specified name.</p> <p>tunnel-group <i>group-name</i>—Clear statistics for only the L2TP tunnels in the specified tunnel group. This option is not available for L2TP LAC on MX Series routers.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • <i>L2TP Services Configuration Overview</i> • <i>L2TP Minimum Configuration</i> • <i>clear services l2tp tunnel</i> • <i>show services l2tp tunnel</i>
List of Sample Output	clear services l2tp tunnel statistics all on page 154
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	<pre>show services l2tp radius <accounting (servers statistics)> <authentication (servers statistics)> <servers> <statistics></pre>
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	<p>You must include one of the following keywords to provide a valid completion for the command:</p> <p>accounting (servers statistics)—(Optional) Display RADIUS servers or statistical accounting information only.</p> <p>authentication (servers statistics)—(Optional) Display RADIUS servers or statistical authentication information only.</p> <p>servers—(Optional) Display RADIUS authentication and accounting server information only.</p> <p>statistics—(Optional) Display RADIUS authentication and accounting statistics information only.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>L2TP Services Configuration Overview</i> • <i>L2TP Minimum Configuration</i>
List of Sample Output	show services l2tp radius servers on page 157 show services l2tp radius statistics on page 157
Output Fields	<p>Table 7 on page 155 lists the output fields for the show services l2tp radius command. Output fields are listed in the approximate order in which they appear.</p>

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.

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

Field Name	Field Description
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.
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

IP Address	State	UDP Port	Retry Count	Timeout	Pending Requests	Maximum Sessions	Dead Time	Secret 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

IP Address	State	UDP Port	Retry Count	Timeout	Pending Requests	Maximum Sessions	Dead Time	Secret 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`
- `show services l2tp radius`
- `show services l2tp summary`

show services l2tp session

Syntax show services l2tp session
<brief | detail | extensive>
<interface *interface-name*>
<local-gateway *gateway-address*>
<local-gateway-name *gateway-name*>
<local-session-id *session-id*>
<local-tunnel-id *tunnel-id*>
<peer-gateway *gateway-address*>
<peer-gateway-name *gateway-name*>
<statistics>
<tunnel-group *group-name*>
<user *username*>

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

Description (M10i and M7i routers only) Display information about active L2TP sessions for LNS.

(MX Series routers only) Display information about active L2TP sessions for LAC and LNS.

Options **none**—Display standard information about all active L2TP sessions.

brief | detail | extensive—(Optional) Display the specified level of output.

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

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

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

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

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

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

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

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

statistics—(Optional) Display the number of control packets and bytes transmitted and received for the session. You cannot include this option with any of the level options, **brief**, **detail**, or **extensive**.

tunnel-group group-name—(Optional) Display L2TP session information for only the specified tunnel group. To display information about L2TP CPU and memory usage, you can include the tunnel group name in the **show services service-sets memory-usage group-name** and **show services service-sets cpu-usage group-name** commands. This option is not available for L2TP LAC on MX Series routers.

user username—(M Series routers only) (Optional) Display L2TP session information for only the specified username.

Required Privilege Level view

Related Documentation

- [L2TP Services Configuration Overview](#)
- [L2TP Minimum Configuration](#)
- [clear services l2tp session on page 151](#)

List of Sample Output

- [show services l2tp session \(LNS on M Series Routers\) on page 164](#)
- [show services l2tp session \(LNS on MX Series Routers\) on page 164](#)
- [show services l2tp session \(LAC\) on page 164](#)
- [show services l2tp session detail \(LAC\) on page 164](#)
- [show services l2tp session extensive \(LAC\) on page 165](#)
- [show services l2tp session extensive \(LAC on MX Series Routers\) on page 165](#)
- [show services l2tp session extensive \(LNS on M Series Routers\) on page 165](#)
- [show services l2tp session extensive \(LNS on MX Series Routers\) on page 166](#)
- [show services l2tp session statistics \(MX Series Routers\) on page 166](#)

Output Fields [Table 8 on page 161](#) lists the output fields for the **show services l2tp session** command. Output fields are listed in the approximate order in which they appear.

Table 8: 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

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

Field Name	Field Description	Level of Output
Session remote ID	Identifier of the remote endpoint of the L2TP session, as assigned by the L2TP access concentrator (LAC).	All levels
State	<p>State of the L2TP session:</p> <ul style="list-style-type: none"> • Established—Session is operating. This is the only state supported for the LAC. • closed—Session is being closed. • destroyed—Session is being destroyed. • clean-up—Session is being cleaned up. • lns-ic-accept-new—New session is being accepted. • lns-ic-idle—Session has been created and is idle. • lns-ic-reject-new—New session is being rejected. • lns-ic-wait-connect—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	<p>(LNS) Mode of the interface representing the session: shared or exclusive.</p> <p>(LAC) Mode of the interface representing the session: shared or dedicated. Only dedicated is currently supported for the LAC.</p>	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	<p>Transmit speed of the session conveyed from the LAC to the LNS, in bits per second (bps).</p> <p>Both the initial (initial) and current (update) line speeds can be displayed on MX Series routers.</p>	extensive

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

Field Name	Field Description	Level of Output
Rx speed	Receive speed of the session conveyed from the LAC to the LNS, in bits per second (bps). Both the initial (initial) and current (update) line speeds can be displayed on MX Series routers.	extensive
Bearer type	Type of bearer enabled: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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

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

Field Name	Field Description	Level of Output
Idle time	Length of time elapsed since the call became idle, in hours, minutes, and seconds.	extensive
Statistics since	<p>Date and time when collection of the following statistics began:</p> <ul style="list-style-type: none"> • Control Tx—Amount of control information transmitted, in packets and bytes. • Control Rx—Amount of control information received, in packets and bytes. • Data Tx—Amount of data transmitted, in packets and bytes. • Data Rx—Amount of data received, in packets and bytes. • Errors Tx—Number of errors transmitted, in packets. • Errors Rx—Number of errors received, in packets. • LCP echo req Tx—Number of LCP echo requests transmitted, in packets. • LCP echo req Rx—Number of LCP echo requests received, in packets. • LCP echo rep Tx—Number of LCP echo responses transmitted, in packets. • LCP echo rep Rx—Number of LCP echo responses received, in packets. • LCP echo Req timeout—Number of LCP echo requests that timed out. • LCP echo Req error—Number of errors received for LCP echo packets. • LCP echo Rep error—Number of errors transmitted for LCP echo packets. 	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      State      unit          Name
  17967 1      Established  1073749824    si-5/2/0

```

show services l2tp session (LAC)

```

user@host> show services l2tp session
Tunnel local ID: 31889
  Local Remote State      Interface      Interface
  ID    ID      State      unit          Name
  31694 1      Established  311           pp0

```

show services l2tp session detail (LAC)

```

user@host> show services l2tp session detail
Tunnel local ID: 31889
  Session local ID: 31694, Session remote ID: 1, Interface unit: 311
  State: Established, Interface: pp0, Mode: Dedicated

```

Local IP: 10.1.1.2:1701, Remote IP: 10.1.1.1:1701
 Local name: ce-lac, Remote name: ce-lns

show services l2tp session extensive (LAC)

```
user@host> show services l2tp session extensive
Tunnel local ID: 31889
Session local ID: 31694, Session remote ID: 1
Interface unit: 311
State: Established, Mode: Dedicated
Local IP: 10.10.1.2:1701, Remote IP: 10.10.1.1:1701
Local name: ce-lac, Remote name: ce-lns
Tx speed: 0, Rx speed: 0
Bearer type: 1, Framing type: 1
LCP renegotiation: N/A, Authentication: None, Interface ID: N/A
Interface unit: 311, Call serial number: 0
Policer bandwidth: 0, Policer burst size: 0
Policer exclude bandwidth: 0, Firewall filter: 0
Session encapsulation overhead: 0, Session cell overhead: 0
Create time: Tue Aug 24 14:38:23 2010, Up time: 01:06:25
Idle time: N/A
```

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

```
user@host> show services l2tp session extensive
Tunnel local ID: 31889
Session local ID: 31694, Session remote ID: 1
Interface unit: 311
State: Established, Mode: Dedicated
Local IP: 10.10.1.2:1701, Remote IP: 10.10.1.1:1701
Local name: ce-lac, Remote name: ce-lns
Tx speed: initial 64000, Update 256000
Rx speed: initial 64000, Update 256000
Bearer type: 1, Framing type: 1
LCP renegotiation: N/A, Authentication: None, Interface ID: N/A
Interface unit: 311, Call serial number: 0
Policer bandwidth: 0, Policer burst size: 0
Policer exclude bandwidth: 0, Firewall filter: 0
Session encapsulation overhead: 0, Session cell overhead: 0
Create time: Tue Aug 24 14:38:23 2010, Up time: 01:06:25
Idle time: N/A
```

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

```
user@host> show services l2tp session extensive
Interface: sp-1/2/0, Tunnel group: group1, Tunnel local ID: 62746
Session local ID: 56793, Session remote ID: 53304
State: Established, Bundle ID: 5, Mode: shared
Local IP: 10.128.1.1:1701, Remote IP: 10.128.1.2:1701
Username: usr1@juniper_1.net, Assigned IP address: 10.50.2.1/32
Local MRU: 4000, Remote MRU: 1500, Tx speed: 64000, Rx speed: 64000
Bearer type: 2, Framing type: 1
LCP renegotiation: Off, Authentication: CHAP, Interface ID: unit_20
Interface unit: 20, Call serial number: 4137941434
Policer bandwidth: 64000, Policer burst size: 51200
Firewall filter: f1
Session encapsulation overhead: 16, Session cell overhead: 0n
Create time: Tue Mar 23 14:13:15 2004, Up time: 01:16:41
Idle time: 00:00:00
Statistics since: Tue Mar 23 14:13:13 2004
```

	Packets	Bytes
Control Tx	4	88

Control Rx	2	28
Data Tx	0	0
Data Rx	461	29.0k
Errors Tx	0	
Errors Rx	0	

Interface: sp-1/2/0, Tunnel group: group_company_dns, Tunnel local ID: 37266
 Session local ID: 39962, Session remote ID: 53303
 State: Established, Bundle ID: 5, Mode: shared
 Local IP: 10.128.11.1:1701, Remote IP: 10.128.11.2:1701
 Username: usr1@company.com, Assigned IP address: 10.46.2.3/24
 Local name: router-1, Remote name: router-2
 Local MRU: 4470, Remote MRU: 4470, Tx speed: 155000000, Rx speed: 155000000
 Bearer type: 2, Framing type: 1
 LCP renegotiation: Off, Authentication: CHAP, Interface ID: unit_31
 Interface unit: 31, Call serial number: 4137941433
 Policer bandwidth: 64000, Policer burst size: 51200
 Firewall filter: f1
 Create time: Tue Mar 23 14:13:17 2004, Up time: 01:16:39
 Idle time: 01:16:36
 Statistics since: Tue Mar 23 14:13:15 2004

	Packets	Bytes
Control Tx	6	196
Control Rx	4	150
Data Tx	0	0
Data Rx	1	80
Errors Tx	0	
Errors Rx	0	

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

```
user@host> show services l2tp session extensive
Tunnel local ID: 40553
  Session local ID: 17967, Session remote ID: 1
    Interface unit: 1073749824
    State: Established
    Interface: si-5/2/0
    Mode: Dedicated
    Local IP: 11.1.1.2:1701, Remote IP: 11.1.1.3:1701
    Local name: lns-mx960, Remote name: testlac
    Tx speed: 56000, Rx speed: 0
    Bearer type: 2, Framing type: 1
    LCP renegotiation: Off, Authentication: None
    Call serial number: 1
    Create time: Mon Apr 25 20:27:50 2011, Up time: 00:01:48
    Idle time: N/A
    Statistics since: Mon Apr 25 20:27:50 2011
```

	Packets	Bytes
Control Tx	4	219
Control Rx	4	221
Data Tx	0	0
Data Rx	10	228
Errors Tx	0	
Errors Rx	0	

show services l2tp session statistics (MX Series Routers)

```
user@host> show services l2tp session statistics local session-id 1
Tunnel local ID: 17185
Session local ID: 1, Session remote ID: 14444, Interface unit: 1073788352
State: Established
```

Statistics since: Mon Aug 1 13:27:47 2011

	Packets	Bytes
Data Tx	4	51
Data Rx	3	36

show services l2tp radius

Syntax	<pre>show services l2tp radius <accounting (servers statistics)> <authentication (servers statistics)> <servers> <statistics></pre>
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	<p>You must include one of the following keywords to provide a valid completion for the command:</p> <p>accounting (servers statistics)—(Optional) Display RADIUS servers or statistical accounting information only.</p> <p>authentication (servers statistics)—(Optional) Display RADIUS servers or statistical authentication information only.</p> <p>servers—(Optional) Display RADIUS authentication and accounting server information only.</p> <p>statistics—(Optional) Display RADIUS authentication and accounting statistics information only.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>L2TP Services Configuration Overview</i> • <i>L2TP Minimum Configuration</i>
List of Sample Output	show services l2tp radius servers on page 170 show services l2tp radius statistics on page 170
Output Fields	<p>Table 7 on page 155 lists the output fields for the show services l2tp radius command. Output fields are listed in the approximate order in which they appear.</p>

Table 9: 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.

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

Field Name	Field Description
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.
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

IP Address	State	UDP Port	Retry Count	Timeout	Pending Requests	Maximum Sessions	Dead Time	Secret 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

IP Address	State	UDP Port	Retry Count	Timeout	Pending Requests	Maximum Sessions	Dead Time	Secret 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 <statistics> <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. Support for statistics option introduced in Junos OS Release 13.1
Description	(M10i and M7i routers: LNS only. MX Series routers: LAC and LNS.) Display Layer 2 Tunneling Protocol (L2TP) summary information.
Options	<p>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.</p> <p>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.</p> <p>statistics—(Optional) Display a summary of control packets and bytes transmitted and received.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> L2TP Services Configuration Overview L2TP Minimum Configuration
List of Sample Output	show services l2tp summary (LAC on M Series routers) on page 175 show services l2tp summary (LAC on MX Series routers) on page 175 show services l2tp summary (LNS on MX Series routers) on page 175 show services l2tp summary (LNS on M Series routers) on page 175 show services l2tp summary statistics (MX Series routers) on page 176
Output Fields	Table 10 on page 172 lists the output fields for the show services l2tp summary command. Output fields are listed in the approximate order in which they appear.

Table 10: 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.

Table 10: show services l2tp summary Output Fields (*continued*)

Field Name	Field Description
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.
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 <i>failover-protocol-fall-back-to-silent-failover</i> 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.
Tx connect speed method	The connection speed method configured to send the speed values in the L2TP Tx Connect Speed (AVP 24) and L2TP Rx Connect Speed (AVP 38). Possible values are: <ul style="list-style-type: none"> • ancp • pppoe-ia-tag • static
Rx speed avp when equal	Indicates if the Rx connect speed when equal configuration is enabled or disabled .
Tunnel assignment id	Format of the tunnel name. Format of the tunnel name, based on RADIUS attributes returned from the AAA server: <ul style="list-style-type: none"> • 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.

Table 10: show services l2tp summary Output Fields (*continued*)

Field Name	Field Description
Tunnel Tx Address Change	<p>Action taken by LAC when it receives a request from a peer to change the destination IP address, UDP port, or both:</p> <ul style="list-style-type: none"> • accept—Accepts change requests for the IP address or UDP port. This is the default action. • ignore—Ignores all change requests. • ignore-ip-address—Ignores change requests for the IP address but accepts them for the UDP port. • ignore-udp-port—Ignores change requests for the UDP port but accepts them for the IP address.
Min Retransmission Timeout for control packets	Minimum number of seconds that the local peer waits for the initial response after transmitting an L2TP control packet. If no response has been received by the time the period expires, the local peer retransmits the packet.
Max Retransmissions for Established Tunnel	Maximum number of times control messages are retransmitted for established tunnels.
Max Retransmissions for Not Established Tunnel	Maximum number of times control messages are retransmitted for tunnels that are not established.
Tunnel Idle Timeout	Period that a tunnel can be inactive—that is, carrying no traffic—before it times out and is torn down.
Destruct Timeout	Period that the router attempts to maintain dynamic destinations, tunnels, and sessions after they have been destroyed.
Destination Lockout Timeout	Timeout period for which all future destinations are locked out, meaning that they are not considered for selection when a new tunnel is created.
Reassembly Service Set	Indicates active IP reassembly configured for the interface.
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.
Switched sessions	Number of L2TP tunnel-switched 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 on M Series routers)

```

user@host> show services l2tp summary
Failover within a preference level is Disabled
Weighted load balancing is Enabled
Tunnel authentication challenge is Enabled
Calling number avp is Enabled
Failover Protocol is Disabled
Tunnel assignment id format is authentication-id
Destinations: 1 Tunnels: 1, Sessions: 1
  Tx packets    Rx packets    Memory (bytes)
Control        260           144          11513856
Data           7.5k          16.9k          8.3k
Errors          0             0

```

show services l2tp summary (LAC on MX Series routers)

```

user@host> show services l2tp summary
Failover within a preference level is Disabled
  Weighted load balancing is Disabled
  Tunnel authentication challenge is Enabled
  Calling number avp is Enabled
  Failover Protocol is Disabled
  Tx Connect speed method is static
  Rx speed avp when equal is enabled
  Tunnel Tx Address Change is Accept
  Min Retransmissions Timeout for control packets is 2 seconds
  Max Retransmissions for Established Tunnel is 7
  Max Retransmissions for Not Established Tunnel is 5
  Tunnel Idle Timeout is 60 seconds
  Destruct Timeout is 300 seconds
  Destination Lockout Timeout is 300 seconds
Reassembly Service Set is ssnr3
Destinations: 0, Tunnels: 0, Sessions: 0, Switched sessions: 0

```

show services l2tp summary (LNS on MX Series routers)

```

user@host> show services l2tp summary
Failover within a preference level is Disabled
Weighted load balancing is Disabled
Tunnel authentication challenge is Enabled
Calling number avp is Enabled
Failover Protocol is Enabled
Tx Connect speed method is static

reassembly Service Set is ssnr3 Destinations: 4, Tunnels: 19, Sessions: 65,
Switched sessions: 2

```

show services l2tp summary (LNS on M Series routers)

```

user@host> show services l2tp summary
Tunnels: 2, Sessions: 2, Errors: 0
  Tx packets    Rx packets    Memory (bytes)
Control         6k           9k          688k
Data           70k          70k          3054

```

show services l2tp summary statistics (MX Series routers)

```
user@host>show services l2tp summary statistics
Failover within a preference level is Disabled
Weighted load balancing is Disabled
Tunnel authentication challenge is Enabled
Calling number avp is Enabled
Failover Protocol is Enabled
Tx Connect speed method is advisory
Tunnel assignment id format is assignment-id
Tunnel Tx Address Change is Accept
Min Retransmissions Timeout for control packets is 4 seconds
Max Retransmissions for Established Tunnel is 7
Max Retransmissions for Not Established Tunnel is 5
Tunnel Idle Timeout is 60 seconds
Destruct Timeout is 300 seconds
Destination Lockout Timeout is 300 secondsDestinations: 1, Tunnels: 1, Sessions:
31815, Switched sessions: 0
  Tx packets    Rx packets    Memory (bytes)
Control        90.4k         32.0k         245678080
Data          127.3k        100.8kk         0
Errors         0             0
```


PART 4

Index

- [Index on page 179](#)

Index

Symbols

#, comments in configuration statements.....	xiv
(), in syntax descriptions.....	xiv
< >, in syntax descriptions.....	xiv
[], in configuration statements.....	xiv
{ }, in configuration statements.....	xiv
(pipe), in syntax descriptions.....	xiv

A

AAA	
subscriber statistics	
clearing.....	148, 150
subscribers	
logging out.....	150
access profile	
session options.....	48
access profile statements	
session-options.....	138
update-interval.....	142
access-profile statements	
accounting.....	60
accounting	
order.....	21
accounting statement	
access profile.....	60
accounting-order statement.....	61
usage guidelines.....	21
accounting-port statement.....	61
usage guidelines.....	38
accounting-server statement.....	62
accounting-session-id-format statement.....	62
accounting-stop-on-access-deny statement.....	63
accounting-stop-on-failure statement.....	63
address statement.....	64
usage guidelines.....	15
address-assignment pools	
DHCPv6 attributes	
specifying the preferred-lifetime.....	81
specifying the t1-percentage.....	81
specifying the t2-percentage.....	81
specifying the valid-lifetime.....	81

address-assignment statement	
address-assignment pools.....	65
address-pool statement.....	66
usage guidelines.....	14
address-range statement.....	67
usage guidelines.....	15
allowed-proxy-pair statement.....	67
usage guidelines.....	23
attributes statement.....	68
authentication	
order.....	21
authentication-order statement	
access.....	69
usage guidelines.....	21
authentication-server statement.....	70

B

boot-file statement.....	70
boot-server statement.....	71
braces, in configuration statements.....	xiv
brackets	
angle, in syntax descriptions.....	xiv
square, in configuration statements.....	xiv

C

cell-overhead statement.....	71
usage guidelines	
client profile.....	32
group profile.....	18
chap-secret statement.....	72
usage guidelines.....	8
circuit-id statement	
address-assignment pools.....	73
circuit-type statement	
DHCP local server.....	74
clear network-access aaa statistics	
command.....	148
clear network-access aaa subscriber	
command.....	150
clear services l2tp session command.....	151
clear services l2tp tunnel statistics command.....	153
client address statement	
usage guidelines.....	44
client statement.....	75
usage guidelines.....	8, 24
client-authentication-algorithm statement	
RADIUS.....	76
client-group statement	
access profile session options.....	78

client-idle-timeout statement	
access profile session options.....	77
client-session-timeout statement	
access profile session options.....	79
comments, in configuration statements.....	xiv
conventions	
text and syntax.....	xiii
curly braces, in configuration statements.....	xiv
customer support.....	xv
contacting JTAC.....	xv

D

dead-peer-detection statement.....	80
DHCP local server	
lease timers.....	105
DHCP local server statements	
boot-file.....	70
boot-server.....	71
circuit-type.....	74
dhcp-attributes statement	
address-assignment pools.....	81
DHCPv6 local server	
lease timers.....	105
documentation	
comments on.....	xv
domain-name statement	
address-assignment pools.....	82
drop-timeout statement.....	82
usage guidelines.....	28

E

encapsulation-overhead statement.....	83
usage guidelines	
client profile.....	32
group profile.....	18
ethernet-port-type-virtual statement.....	83
exclude statement.....	84

F

font conventions.....	xiii
fragment-threshold statement.....	88
fragmentation-threshold statement	
usage guidelines.....	28
framed-ip-address statement.....	88
usage guidelines.....	32
framed-pool statement.....	89
usage guidelines.....	18
client profile.....	32
group profile.....	18

G

grace-period statement.....	89
group-profile statement	
associating with L2TP client.....	90
usage guidelines.....	16, 27

H

hardware-address statement.....	92
host statement	
address-assignment pools.....	92

I

idle timeout	
subscriber access.....	48
idle-timeout statement.....	93
usage guidelines	
group profile.....	18
ignore statement.....	94
ike statement.....	95
immediate-update statement	
accounting.....	96
initiate-dead-peer-detection statement.....	97
interface-description-format statement.....	97
interface-id statement.....	98
usage guidelines.....	18, 28
client profile.....	32
ip-address statement.....	98

J

Juniper-Interface-ID attribute (RADIUS for L2TP).....	39
Juniper-IP-Pool-Name attribute (RADIUS for L2TP).....	39
Juniper-Keep-Alive attribute (RADIUS for L2TP).....	39
Juniper-Primary-DNS attribute (RADIUS for L2TP).....	39
Juniper-Primary-WINS attribute (RADIUS for L2TP).....	39
Juniper-Secondary-DNS attribute (RADIUS for L2TP).....	39
Juniper-Secondary-WINS attribute (RADIUS for L2TP).....	39

K

keepalive statement.....	99
usage guidelines	
client profile.....	32

keepalive-retries statement.....	100
usage guidelines	
client profile.....	32

L

L2TP services	
RADIUS information.....	155, 168
sessions	
clearing.....	151
displaying.....	160
summary information, displaying.....	172
tunnel statistics, clearing.....	153
l2tp statement	
client profile.....	102
group profile.....	101
usage guidelines.....	17, 27
L2TP statements	
LNS	
shared-secret.....	138
lcp-negotiation statement	
usage guidelines.....	28
lcp-renegotiation statement.....	103
usage guidelines.....	17, 27
local-chap statement.....	104
usage guidelines.....	28

M

manuals	
comments on.....	xv
maximum-lease-time statement.....	105
maximum-sessions-per-tunnel statement.....	106
usage guidelines.....	28
Mobile IP statements	
statistics.....	140
multilink statement.....	107
usage guidelines.....	28

N

name-server statement.....	107
nas-identifier statement.....	108
nas-port-extended-format statement	
access profiles.....	109
netbios-node-type statement.....	110
network statement.....	111

O

option statement.....	111
option-82 statement	
address-assignment pools.....	112

option-match statement.....	112
options statement	
RADIUS.....	113
order statement	
accounting.....	114

P

pap-password statement.....	115
usage guidelines.....	30
parentheses, in syntax descriptions.....	xiv
pool statement	
address-assignment pools.....	116
port statement	
RADIUS servers.....	117
usage guidelines.....	38
ppp statement	
client profile.....	119
group profile.....	118
usage guidelines.....	31
ppp-authentication statement.....	120
usage guidelines.....	28, 30
ppp-profile statement.....	120
usage guidelines.....	45
pre-shared-key statement.....	121
primary-dns statement.....	121
usage guidelines.....	32
group profile.....	18
primary-wins statement.....	122
usage guidelines	
client profile.....	32
group profile.....	18
profile statement	
subscriber access.....	123
usage guidelines.....	8, 19

R

RADIUS authentication	
in a private network.....	9
L2TP.....	37, 45
RADIUS information	
displaying.....	155, 168
RADIUS servers	
configuration example.....	46
radius statement	
subscriber access.....	127
radius-disconnect statement.....	129
usage guidelines.....	44
radius-disconnect-port statement.....	130
usage guidelines.....	44

radius-server statement.....	131	support, technical See technical support	
usage guidelines.....	38	syntax conventions.....	xiii
range statement		T	
address-assignment pools.....	132	technical support	
remote-id statement.....	133	contacting JTAC.....	xv
retry statement.....	134	tftp-server statement.....	140
reverse-route statement.....	134	timeout statement	
revert-interval statement.....	135	access.....	141
router statement		usage guidelines.....	38
address-assignment pools.....	135	timeouts	
routing-instance statement		idle and session.....	48
RADIUS.....	136	U	
usage guidelines.....	9	update-interval statement	
S		access profile.....	142
secondary-dns statement.....	136	user-group-profile statement.....	143
usage guidelines		usage guidelines.....	33
client profile.....	32	V	
group profile.....	18	vlan-nas-port-stacked-format statement.....	143
secondary-wins statement.....	137	W	
usage guidelines		wins-server statement.....	144
client profile.....	32		
group profile.....	18		
secret statement			
access.....	137		
usage guidelines, RADIUS			
authentication.....	38		
usage guidelines, RADIUS disconnect.....	44		
session options			
subscriber access.....	48		
session options statements			
client-group.....	78		
client-idle-timeout.....	77		
client-session-timeout.....	79		
session timeout			
subscriber access.....	48		
session-options statement			
access profile.....	138		
shared-secret statement.....	138		
usage guidelines.....	28		
show services l2tp radius command.....	155, 168		
show services l2tp session command.....	160		
show services l2tp summary command.....	172		
source-address statement			
RADIUS.....	139		
statistics statement			
access.....	140		
subscriber session options			
configuration overview.....	50		