Junos® OS

User Access and Authentication Feature Guide

Modified: 2019-06-27

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS User Access and Authentication Feature Guide

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 https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

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 https://www.juniper.net/books.

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

Table 1 on page xlv 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 xlvi 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`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	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* **]**

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

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

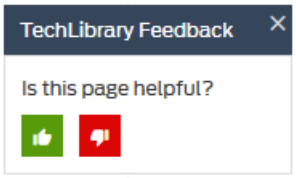
Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• 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 so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software 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 Juniper Care or Partner Support Services 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 https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://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: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- 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 https://support.juniper.net/support/requesting-support/.

CHAPTER 1

Login Classes and Login Settings

Junos OS Login Classes Overview

Junos OS login class allow you to define access privileges, permission for using CLI commands and statements, and session idle time for each login classes. You can apply login class to an individual user account, there by specifying certain privileges and permissions to the user. Read this topic for more information.

Junos OS Login Classes Overview

All users who can log in to the router or switch must be in a login class. With login classes, you define the following:

- Access privileges that users have when they are logged in to the router or switch
- Commands and statements that users can and cannot specify
- How long a login session can be idle before it times out and the user is logged out

You can define any number of login classes and then apply one login class to an individual user account.

The Junos operating system (Junos OS) contains a few predefined login classes, which are listed in Table 3 on page 49. The predefined login classes cannot be modified.

Table 3: Predefined System Login Classes

Login Class	Permission Flag Set
operator	clear, network, reset, trace, and view
read-only	view

Table 3: Predefined System Login Classes (continued)

Login Class	Permission Flag Set
superuser or **super-user**	all
unauthorized	None

NOTE:

- You cannot modify a predefined login class name. If you issue the **set** command on a predefined class name, the Junos OS appends **-local** to the login class name. The following message also appears:

  ```
  warning: '<class-name>' is a predefined class name; changing to
    '<class-name>-local'
  ```

- You cannot issue the **rename** or **copy** command on a predefined login class. Doing so results in the following error message:

  ```
  error: target '<class-name>' is a predefined class
  ```

Permission Bits

Each top-level CLI command and each configuration statement has an access privilege level associated with it. Users can execute only those commands and configure and view only those statements for which they have access privileges. The access privileges for each login class are defined by one or more permission bits (see Table 4 on page 50).

Two forms for the permissions control the individual parts of the configuration:

- "Plain" form—Provides read-only capability for that permission type. An example is **interface**.
- Form that ends in **-control**—Provides read and write capability for that permission type. An example is **interface-control**.

Table 4: Permission Bits for Login Classes

Permission Bit	Access
admin	Can view user account information in configuration mode and with the **show configuration** command.
admin-control	Can view user accounts and configure them (at the **[edit system login]** hierarchy level).
access	Can view the access configuration in configuration mode and with the **show configuration** operational mode command.
access-control	Can view and configure access information (at the **[edit access]** hierarchy level).

Table 4: Permission Bits for Login Classes (continued)

Permission Bit	Access
all	Has all permissions.
clear	Can clear (delete) information learned from the network that is stored in various network databases (using the **clear** commands).
configure	Can enter configuration mode (using the **configure** command) and commit configurations (using the **commit** command).
control	Can perform all control-level operations (all operations configured with the **-control** permission bits).
field	Reserved for field (debugging) support.
firewall	Can view the firewall filter configuration in configuration mode.
firewall-control	Can view and configure firewall filter information (at the **[edit firewall]** hierarchy level).
floppy	Can read from and write to the removable media.
interface	Can view the interface configuration in configuration mode and with the **show configuration** operational mode command.
interface-control	Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces (at the **[edit]** hierarchy).
maintenance	Can perform system maintenance, including starting a local shell on the device and becoming the superuser in the shell (by issuing the **su root** command), and can halt and reboot the device (using the **request system** commands).
network	Can access the network by entering the **ping**, **ssh**, **telnet**, and **traceroute** commands.
reset	Can restart software processes using the **restart** command and can configure whether software processes are enabled or disabled (at the **[edit system processes]** hierarchy level).
rollback	Can use the **rollback** command to return to a previously committed configuration other than the most recently committed one.
routing	Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.
routing-control	Can view general routing, routing protocol, and routing policy configuration information and configure general routing (at the **[edit routing-options]** hierarchy level), routing protocols (at the **[edit protocols]** hierarchy level), and routing policy (at the **[edit policy-options]** hierarchy level).
secret	Can view passwords and other authentication keys in the configuration.

Table 4: Permission Bits for Login Classes (continued)

Permission Bit	Access
secret-control	Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.
security	Can view security configuration in configuration mode and with the **show configuration** operational mode command.
security-control	Can view and configure security information (at the **[edit security]** hierarchy level).
shell	Can start a local shell on the device by entering the **start shell** command.
snmp	Can view SNMP configuration information in configuration and operational modes.
snmp-control	Can view SNMP configuration information and configure SNMP (at the **[edit snmp]** hierarchy level).
system	Can view system-level information in configuration and operational modes.
system-control	Can view system-level configuration information and configure it (at the **[edit system]** hierarchy level).
trace	Can view trace file settings in configuration and operational modes.
trace-control	Can view trace file settings and configure trace file properties.
view	Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics.

Denying or Allowing Individual Commands

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that are otherwise permitted or not allowed by a permission bit.

Defining Junos OS Login Classes

Login classes allow you to define the following:

- Access privileges that users have when they are logged in to the router or switch
- Commands and statements that users can and cannot specify
- How long a login session can be idle before it times out and the user is logged out

All users who can log in to the router or switch must be in a login class. Therefore, you must define a Junos OS login class for each user or class of users. You can define any number of login classes depending on the types of permissions the users need.

To define a login class and its access privileges, include the **class** statement at the **[edit system login]** hierarchy level:

```
[edit system login]
class class-name {
  access-end;
  access-start;
  allow-commands "regular-expression";
  ( allow-configuration | allow-configuration-regexps) “regular expression 1” “regular
    expression 2”;
  allowed-days;
  configuration-breadcrumbs;
  deny-commands "regular-expression";
  ( deny-configuration | deny-configuration-regexps )  “regular expression 1” “regular
    expression 2 ”;
  idle-timeout minutes;
  login-script filename;
  login-tip;
  no-scp-server;
  no-sftp-server;
  permissions [ permissions ];
}
```

Example: Creating Login Classes with Specific Privileges

Login classes are used to assign certain permissions or restrictions to groups of users, ensuring that sensitive commands are only accessible to the appropriate users. By default, Juniper Networks devices have four types of login classes with preset permissions: operator, read-only, superuser or super-user, and unauthorized.

You can create new custom login classes to make different combinations of permissions that are not found in the default login classes. The following example shows how to create three custom login classes, each with specific privileges and timers to disconnect the class members after a period of inactivity. Inactivity timers help protect network security by disconnecting a user from the network if the user is away from his computer for too long, preventing potential security risks created by leaving an unattended account logged in to a switch or router. The permissions and inactivity timers shown here are only examples and should be customized to your organization.

The first class of users is called **observation** and they can only view statistics and configuration. They are not allowed to modify any configuration. The second class of users is called **operation** and they can view and modify the configuration. The third class of users is called **engineering** and they have unlimited access and control. All three login classes use the same inactivity timer of 5 minutes.

```
[edit]
system {
  login {
    class observation {
      idle-timeout 5;
      permissions [ view ];
    }
    class operation {
      idle-timeout 5;
      permissions [ admin clear configure interface interface-control network
      reset routing routing-control snmp snmp-control trace-control
      firewall-control rollback ];
    }
    class engineering {
      idle-timeout 5;
      permissions all;
    }
  }
}
```

Related Documentation

- Junos OS User Accounts on page 67
- Junos OS Administrative Roles on page 79
- Junos OS User Access Privileges on page 90

Junos OS Login Settings

Junos OS allows you to specify various settings for the users after they have logged in. You can define what to notify for the users after they have logged in, display system alarms, provide login tips, or specify time-based user access, and limit the number of login attempts. Read this topic for more information.

- Configuring Junos OS to Display a System Login Announcement on page 55
- Configuring System Alarms to Appear Automatically Upon Login on page 56
- Configuring Login Tips on page 57
- Examples: Configuring Time-Based User Access on page 57
- Configuring the Timeout Value for Idle Login Sessions on page 58
- Login Retry Options on page 59
- Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 60
- Example: Configuring Login Retry Options on page 62

Configuring Junos OS to Display a System Login Announcement

Sometimes you want to make announcements only to authorized users after they have logged in. For example, you might want to announce an upcoming maintenance event.

You can format the announcement using the following special characters:

- \n—New line
- \t—Horizontal tab
- \'—Single quotation mark
- \"—Double quotation mark
- \\—Backslash

If the message text contains any spaces, enclose it in quotation marks.

By default, no login announcement is displayed.

To configure an announcement that can be seen only by authorized users:

1. Include the **announcement** statement in the **[edit system login]** configuration.

```
[edit system login]
user@host# set announcement text
```

   For example:

```
system {
   login {
      announcement "\tJuly 27th 1:00 AM to 8:00\n\nPlanned Network
         Maintenance\n\nAFFECTED LOCATIONS: Sunnyvale\n\nPLANNED ACTIVITY:
         Upgrade all 6200 switch firmware to the Enterprise TAC recommended firmware
         version\n\nPURPOSE: This activity will help to minimize the impact of unplanned
         power outages as well as address known issues within our currently installed
         firmware version(s)\n\nWHAT TO EXPECT: During the maintenance window for
         your site, the office network will not be available.\n\n";
      message "\n\n\n\tTP0 - M7i - iX Router Lab\n\n\tUNAUTHORIZED USE OF THIS
         ROUTER\n\tIS STRICTLY PROHIBITED!\n\n\tPlease contact
         \'astatti@juniper.net\' to gain\n\taccess to this equipment if you need
         authorization.\n\n\n"
   }
}
```

2. Commit the configuration.

```
[edit system login]
user@host# commit
```

3. Connect to the device in a new session to verify the presence of the new banner.

The preceding login message configuration example produces a login message similar to the following:

```
server% telnet host
Trying 203.0.113.0
Connected to host.example.net
Escape character is '^]'.



        TPO - M7i - iX Router Lab

        UNAUTHORIZED USE OF THIS ROUTER
        IS STRICTLY PROHIBITED!

        Please contact 'astatti@juniper.net' to gain
        access to this equipment if you need authorization



login: user
Password:

        July 27th 1:00 AM to 8:00

Planned Network Maintenance

AFFECTED  LOCATIONS:  Sunnyvale

PLANNED ACTIVITY: Upgrade all 6200 switch firmware to the Enterprise TAC
recommended firmware version

PURPOSE: This activity will help to minimize the impact of unplanned power
outages as well as address known issues within our currently installed firmware
 version(s)

WHAT TO EXPECT: During the maintenance window for your site, the office network
 will not be available.
```

If the announcement text contains any spaces, enclose the text in quotation marks.

A system login *announcement* appears after the user logs in. A system login *message* appears before the user logs in.

TIP: You can use the same special characters described to format your system login announcement.

Configuring System Alarms to Appear Automatically Upon Login

You can configure Juniper Networks routers and switches to run the **show system alarms** command whenever a user with the login class **admin** logs in to the router or switch. To do so, include the **login-alarms** statement at the **[edit system login class admin]** hierarchy level.

```
[edit system login class admin]
login-alarms;
```

For more information on the **show system alarms** command, see the CLI Explorer.

See Also
- *show system alarms*

Configuring Login Tips

The Junos OS CLI provides the option of configuring login tips for the user. By default, the **tip** command is not enabled when a user logs in.

- To enable tips, include the **login-tip** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]
login-tip;
```

Adding this statement enables the **tip** command for the class specified, provided the user logs in using the CLI.

Examples: Configuring Time-Based User Access

The following example shows how to configure user access for the **operator-round-the-clock-access** login class from Monday through Friday without any restriction on access time or duration of login:

```
[edit system]
login {
  class operator-round-the-clock-access {
    allowed-days [ monday tuesday wednesday thursday friday ];
  }
```

The following example shows how to configure user access for the **operator-day-shift** login class on Monday, Wednesday, and Friday from 8:30 AM to 4:30 PM:

```
[edit system]
login {
  class operator-day-shift {
    allowed-days [ monday wednesday friday ];
    access-start 0830;
    access-end 1630;
  }
}
```

Alternatively, you can also specify the login start time and end time for the **operator-day-shift** login class to be from 8:30 AM to 4:30 PM in the following format:

```
[edit system]
login {
  class operator-day-shift {
```

```
    allowed-days [ monday wednesday friday ];
    access-start 08:30am;
    access-end 04:30pm;
  }
}
```

The following example shows how to configure user access for the **operator-day-shift-all-days-of-the-week** login class to be on all days of the week from 8:30 AM to 4:30 PM:

```
[edit system]
login {
  class operator-day-shift-all-days-of-the-week {
    access-start 0830;
    access-end 1630;
  }
}
```

See Also

- *Configuring Time-Based User Access*

Configuring the Timeout Value for Idle Login Sessions

An idle login session is one in which the CLI operational mode prompt is displayed but there is no input from the keyboard. By default, a login session remains established until a user logs out of the router or switch, even if that session is idle. To close idle sessions automatically, you must configure a time limit for each login class. If a session established by a user in that class remains idle for the configured time limit, the session automatically closes. **Idle-timeout** can only be configured for user defined classes. Configuration won't work for the system predefined classes: **operator**, **read-only**, **super-user**. These classes' values and permissions are not editable.

To define the timeout value for idle login sessions, include the **idle-timeout** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]
idle-timeout minutes;
```

Specify the number of minutes that a session can be idle before it is automatically closed.

If you have configured a timeout value, the CLI displays messages similar to the following when timing out an idle user. It starts displaying these messages 5 minutes before timing out the user.

```
user@host# Session will be closed in 5 minutes if there is no activity.
Warning: session will be closed in 1 minute if there is no activity
Warning: session will be closed in 10 seconds if there is no activity
Idle timeout exceeded: closing session
```

If you configure a timeout value, the session closes after the specified time has elapsed, unless the user is running telnet or monitoring interfaces using the **monitor interface** or **monitor traffic** command.

See Also
- idle-timeout (System-Login) on page 1131

Login Retry Options

The security administrator can configure the number of times a user can try to log in to the device with invalid login credentials. The device can be locked after the specified number of unsuccessful authentication attempts. This helps to protect the device from malicious users attempting to access the system by guessing an account's password. The security administrator can unlock the user account or define a time period for the user account to remain locked.

The system **lockout-period** defines the amount of time the device can be locked for a user account after a specified number of unsuccessful login attempts.

The security administrator can configure a period of time after which an inactive session will be locked and require re-authentication to be unlocked. This helps to protect the device from being idle for a long period before the session times out.

The system **idle-timeout** defines length of time the CLI operational mode prompt remains active before the session times out.

The security administrator can configure a banner with an advisory notice to be displayed before the identification and authentication screen.

The system **message** defines the system login message. This message appears before a user logs in.

The number of reattempts the device allows is defined by the **tries-before-disconnect** option. The device allows 3 unsuccessful attempts by default or as configured by the administrator. The device prevents the locked users to perform activities that require authentication, until a security administrator manually clears the lock or the defined time period for the device to remain locked has elapsed. However, the existing locks are ignored when the user attempts to log in from the local console.

NOTE: To clear the console during an administrator-initiated logout, the administrator must configure the **set system login message "message string"** such that, the message-string contains newline (\n) characters and a login banner message at the end of the \n characters.

To ensure that configuration information is cleared completely, the administrator can enter 50 or more \n characters in the *message-string* of the command **set system login message "message string"**.

For example, **set system login message "\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n Welcome to Junos!!!"**

Limiting the Number of User Login Attempts for SSH and Telnet Sessions

You can limit the number of times a user can attempt to enter a password while logging in through SSH or Telnet. The connection is terminated if a user fails to log in after the number of attempts specified. You can also specify a delay, in seconds, before a user can try to enter a password after a failed attempt. In addition, you can specify the threshold for the number of failed attempts before the user experiences a delay in being able to enter a password again.

To specify the number of times a user can attempt to enter a password while logging in, include the **retry-options** statement at the **[edit system login]** hierarchy level:

```
[edit system login]
retry-options {
  tries-before-disconnect number;
  backoff-threshold number;
  backoff-factor seconds;
  maximum-time seconds
  minimum-time seconds;
}
```

You can configure the following options:

- **tries-before-disconnect**—Number of times a user can attempt to enter a password when logging in. The connection closes if a user fails to log in after the number specified. The range is from 1 through 10, and the default is 10.
- **backoff-threshold**—Threshold for the number of failed login attempts before the user experiences a delay in being able to enter a password again. Use the **backoff-factor** option to specify the length of the delay in seconds. The range is from 1 through 3, and the default is 2.
- **backoff-factor**—Length of time, in seconds, before a user can attempt to log in after a failed attempt. The delay increases by the value specified for each subsequent attempt after the threshold. The range is from 5 through 10, and the default is 5 seconds.
- **maximum-time *seconds***—Maximum length of time, in seconds, that the connection remains open for the user to enter a username and password to log in. If the user

remains idle and does not enter a username and password within the configured **maximum-time**, the connection is closed. The range is from 20 through 300 seconds, and the default is 120 seconds.

- **minimum-time**—Minimum length of time, in seconds, that a connection remains open while a user is attempting to enter a correct password. The range is from 20 through 60, and the default is 40.

The following example shows how to limit the user to four attempts when the user enters a password while logging in through SSH or Telnet:

Limiting the number of SSH and Telnet login attempts per user is one of the most effective methods of stopping brute force attacks from compromising your network security. Brute force attackers execute a large number of login attempts in a short period of time to illegitimately gain access to a private network. By configuring the **retry-options** command, you can create an increasing delay after each failed login attempt, eventually disconnecting any user who passes your set threshold of login attempts.

Set the **backoff-threshold** to 2, the **back-off-factor** to 5 seconds, and the **minimum-time** to 40 seconds. The user experiences a delay of 5 seconds after the second attempt to enter a correct password fails. After each subsequent failed attempt, the delay increases by 5 seconds. After the fourth and final failed attempt to enter a correct password, the user experiences an additional 10-second delay, and the connection closes after a total of 40 seconds.

The additional variables **maximum-time** and **lockout-period** are not set in this example.

```
[edit]
system {
   login {
      retry-options {
         backoff-threshold 2;
         backoff-factor 5;
         minimum-time 40;
         tries-before-disconnect 4;
      }
      password {
      }
   }
}
```

NOTE: This sample only shows the portion of the [edit system login] hierarchy level being modified.

Example: Configuring Login Retry Options

This example shows how to configure system retry options to protect the device from malicious users.

Requirements

Before you begin, you should understand "Login Retry Options" on page 59.

No special configuration beyond device initialization is required before configuring this feature.

Overview

Malicious users sometimes try to log in to a secure device by guessing an authorized user account's password. Locking out a user account after a number of failed authentication attempts helps protect the device from malicious users.

Device lockout allows you to configure the number of failed attempts before the user account is locked out of the device and configure the amount of time before the user can attempt to log in to the device again. You can configure the amount of time in-between failed login attempts of a user account and can manually lock and unlock user accounts.

NOTE:

This example includes the following settings:

- **backoff-factor** — Sets the length of delay in seconds after each failed login attempt. When a user incorrectly logs in to the device, the user must wait the configured amount of time before attempting to log in to the device again. The length of delay increases by this value for each subsequent login attempt after the value specified in the **backoff-threshold** statement. The default value for this statement is five seconds, with a range of five to ten seconds.
- **backoff-threshold** — Sets the threshold for the number of failed login attempts on the device before the user experiences a delay when attempting to reenter a password. When a user incorrectly logs in to the device and hits the threshold of failed login attempts, the user experiences a delay that is set in the **backoff-factor** statement before attempting to log in to the device again. The default value for this statement is two, with a range of one through three.
- **lockout-period** — Sets the amount of time in minutes before the user can attempt to log in to the device after being locked out due to the number of failed login attempts specified in the **tries-before-disconnect** statement. When a user fails to correctly login after the number of allowed attempts specified by the **tries-before-disconnect** statement, the user must wait the configured amount of minutes before attempting to log in to the device again. The lockout-period must be greater than zero. The range at which you can configure the lockout-period is one through 43,200 minutes.
- **tries-before-disconnect** — Sets the maximum number of times the user is allowed to enter a password to attempt to log in to the device through SSH or Telnet. When the user reaches the maximum number of failed login attempts, the user is locked out of the device. The user must wait the configured amount of minutes in the **lockout-period** statement before attempting to log back in to the device. The **tries-before-disconnect** statement must be set when the **lockout-period** statement is set; otherwise, the **lockout-period** statement is meaningless. The default number of attempts is ten, with a range of one through ten attempts.

Once a user is locked out of the device, if you are the security administrator, you can manually remove the user from this state using the **clear system login lockout** *<username>* command. You can also use the **show system login lockout** command to view which users are currently locked out, when the lockout period began for each user, and when the lockout period ends for each user.

If the security administrator is locked out of the device, he can log in to the device from the console port, which ignores any user locks. This provides a way for the administrator to remove the user lock on their own user account.

In this example the user waits for the **backoff-threshold** multiplied by the **backoff-factor** interval, in seconds, to get the login prompt. In this example, the user must wait 5 seconds after the first failed login attempt and 10 seconds after the second failed login attempt to get the login prompt. The user gets disconnected after 15 seconds after the third failed attempt because the **tries-before-disconnect** option is configured as 3.

The user cannot attempt anther login until 120 minutes has elapsed, unless a security administrator manually clears the lock sooner.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login retry-options backoff-factor 5
set system login retry-options backoff-threshold 1
set system login retry-options lockout-period 120
set system login retry-options tries-before-disconnect 3
```

Step-by-Step Procedure

To configure system retry-options:

1. Configure the backoff factor.

   ```
   [edit ]
   user@host# set system login retry-options backoff-factor 5
   ```

2. Configure the backoff threshold.

   ```
   [edit]
   user@host# set system login retry-options backoff-threshold 1
   ```

3. Configure the amount of time the device gets locked after failed attempts.

   ```
   [edit]
   user@host# set system login retry-options lockout-period 5
   ```

4. Configure the number of unsuccessful attempts during which, the device can remain unlocked.

   ```
   [edit]
   user@host# set system login retry-options tries-before-disconnect 3
   ```

Results

From configuration mode, confirm your configuration by entering the **show system login retry-options** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system login retry-options
backoff-factor 5;
backoff-threshold 1;
lockout-period 5;
tries-before-disconnect 3;
```

Confirm that the configuration is working properly.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Displaying the Locked User Logins

Purpose Verify that the login lockout configuration is enabled.

Action Attempt three unsuccessful logins for a particular username. The device will be locked for that username; then log in to the device with a different username. From operational mode, enter the **show system login lockout** command.

Meaning When you perform three unsuccessful login attempts with a particular username, the device is locked for that user for five minutes, as configured in the example. You can verify that the device is locked for that user by logging in to the device with a different username and entering the **show system login lockout** command.

Related Documentation

- Junos OS Login Classes Overview on page 49
- Junos OS User Accounts on page 67

CHAPTER 2

User Accounts

Junos OS User Accounts

Junos OS allows you to create accounts for router, switch, and security users. All users also belong one the system login classes.

Junos OS requires that all users have a predefined user account before they can log in to the device. For each user account, you define the login name for the user and, optionally, information that identifies the user. User accounts provide a way for users to access a router or switch or security device. Read this topic for more information.

Junos OS User Accounts Overview

User accounts provide one way for users to access the device. (Users can access the device without accounts if you configured RADIUS or TACACS+ servers, as described in "Junos OS User Authentication Methods" on page 161.) For each account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

For each user account, you can define the following:

- Username—Name that identifies the user. It must be unique within the device. Do not include spaces, colons, or commas in the username. The username can be up to 64 characters long.
- User's full name—(Optional) If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.

- User identifier (UID)—(Optional) Numeric identifier that is associated with the user account name. The identifier must be in the range from 100 through 64,000 and must be unique within the device. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.

You must ensure that the UID is unique. However, it is possible to assign the same UID to different users. If you do this, the CLI displays a warning when you commit the configuration and then assigns the duplicate UID.

- User's access privilege—(Required) One of the login classes you defined in the **class** statement at the **[edit system login]** hierarchy level, or one of the default classes listed in "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 99.
- Authentication method or methods and passwords that the user can use to access the device—(Optional) You can use SSH or a Message Digest 5 (MD5) password, or you can enter a plain-text password that the Junos OS encrypts using MD5-style encryption before entering it in the password database. For each method, you can specify the user's password. If you configure the **plain-text-password** option, you are prompted to enter and confirm the password:

  ```
  [edit system login user username]
  user@host# set authentication plain-text-password
  New password: type password here
  Retype new password: retype password here
  ```

  The default requirements for plain-text passwords are:

  - The password must be between 6 and 128 characters long.
  - You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
  - Valid passwords must contain at least one change of case or character class.

  Junos-FIPS and Common Criteria have special password requirements. FIPS and Common Criteria passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If Junos-FIPS is installed on the device, you cannot configure passwords unless they meet this standard.

For SSH authentication, you can copy the contents of an SSH key file into the configuration or directly configure SSH key information. Use the **load-key-file** *URL filename* command to load an SSH key file that was previously generated, e.g. by using **ssh-keygen**. The *URL filename* is the path to the file's location and name. This command loads RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys. The contents of the SSH key file are copied into the configuration immediately after you enter the **load-key-file** statement. Optionally, you can use the **ssh-dsa** *public key* **<from** *hostname*> and the **ssh-rsa** *public key* **<from** *hostname*> statements to directly configure SSH keys.

Starting in Junos OS Release 18.3R1, the **ssh-dss** and **ssh-dsa** hostkey algorithms are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

For each user account and for root logins, you can configure more than one public RSA or DSA key for user authentication. When a user logs in using a user account or as root, the configured public keys are referenced to determine whether the private key matches any of them.

To view the SSH keys entries, use the configuration mode **show** command. For example:

```
[edit system login user boojum]
user@host# set authentication load-key-file my-host:.ssh/id_dsa.pub
.file.19692 | 0 KB | 0.3 kB/s | ETA: 00:00:00 | 100%
[edit system]
user@host# show
root-authentication {
   ssh-rsa "$ABC123"; # SECRET-DATA
}
```

An account for the user **root** is always present in the configuration. You configure the password for **root** using the **root-authentication** statement, as described in "Configuring the Root Password" on page 140.

Junos-FIPS Crypto Officer and User Accounts Overview

Junos-FIPS defines a restricted set of user roles. Unlike the Junos OS, which enables a wide range of capabilities to users, FIPS 140-2 defines specific types of users (Crypto Officer, User, and Maintenance). Crypto Officers and FIPS Users perform all FIPS-related configuration tasks and issue all FIPS-related commands. Crypto Officer and FIPS User configurations must follow FIPS 140-2 guidelines. Typically, no user besides a Crypto Officer can perform FIPS-related tasks.

Crypto Officer User Configuration

Junos-FIPS offers finer control of user permissions than those mandated by FIPS 140-2. For FIPS 140-2 conformance, any Junos-FIPS user with the **secret**, **security**, and **maintenance** permission bits set is a Crypto Officer. In most cases, the **super-user** class should be reserved for a Crypto Officer. A FIPS User can be defined as any Junos-FIPS user that does not have the **secret**, **security**, and **maintenance** bits set.

FIPS User Configuration

A Crypto Officer sets up FIPS Users. FIPS Users can be granted permissions normally reserved for a Crypto Officer; for example, permission to zeroize the system and individual AS-II FIPS PICs.

Example: Configuring User Accounts

The following example shows how to create accounts for four router or switch users, and create an account for the template user **remote**. All users use one of the default system login classes. User **alexander** also has two digital signal algorithm (DSA) public keys configured for SSH authentication.

```
[edit]
system {
   login {
      user philip {
         full-name “Philip of Macedonia”;
         uid 1001;
         class super-user;
         authentication {
            encrypted-password “$ABC123”;
         }
      }
      user alexander {
         full-name “Alexander the Great”;
         uid 1002;
         class view;
         authentication {
            encrypted-password “$ABC123”;
            ssh-dsa “8924 37 5678 5678@gaugamela.per”;
            ssh-dsa “6273 94 9283@boojum.per”;
         }
      }
      user darius {
         full-name “Darius King of Persia”;
         uid 1003;
         class operator;
         authentication {
            ssh-rsa “1024 37 12341234@ecbatana.per”;
         }
      }
      user anonymous {
         class unauthorized;
      }
      user remote {
         full-name “All remote users”;
         uid 9999;
         class read-only;
      }
   }
}
```

Example: Configuring New Users

This example shows how to configure new users.

- Requirements on page 71
- Overview on page 71

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

You can add new users to the device's local database. For each account, you define a login name and password for the user and specify a login class for access privileges. The login password must meet the following criteria:

- The password must be at least six characters long.
- You can include most character classes in a password (alphabetic, numeric, and special characters), but not control characters.
- The password must contain at least one change of case or character class.

In this example, you create a login class named operator-and-boot and allow it to reboot the device. You can define any number of login classes. You then allow the operator-and-boot login class to use commands defined in the clear, network, reset, trace, and view permission bits.

Then you create user accounts. User accounts enable you to access the device. (You can access the device without accounts if you configured RADIUS or TACACS+ servers.) You set the username as cmartin and the login class as superuser. Finally, you define the encrypted password for the user.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login class operator-and-boot allow-commands “request system reboot”
set class system login operator-and-boot permissions [clear network reset trace view]
set system login user cmartin class superuser authentication encrypted-password
    $1$ABC123
```

GUI Step-by-Step Procedure

To configure new users:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Users** tab.

4. Click **Add** to add a new user. The Add User dialog box appears.

5. In the User name box, type a unique name for the user.

   Do not include spaces, colons, or commas in the username.

6. In the User ID box, type a unique ID for the user.

7. In the Full Name box, type the user's full name.

   If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.

8. In the Password and Confirm Password boxes, enter a login password for the user and verify your entry.

9. From the Login Class list, select the user's access privilege:

   - **operator**
   - **read-only**
   - **unauthorized**

   This list also includes any user-defined login classes.

10. Click **OK** in the Add User dialog box and Edit User Management dialog box.

11. Click **OK** to check your configuration and save it as a candidate configuration.

12. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure new users:

1. Set the name of the login class and allow the use of the reboot command.

```
[edit system login]
user@host# set class operator-and-boot allow-commands "request system reboot"
```

2. Set the permission bits for the login class.

```
[edit system login]
user@host# set class operator-and-boot permissions [clear network reset trace
    view]
```

3. Set the username, login class, and encrypted password for the user.

```
[edit system login]
user@host# set user cmartin class superuser authentication encrypted-password
  $1$ABC123
```

Results From configuration mode, confirm your configuration by entering the **show system login** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system login
  class operator-and-boot {
  permissions [ clear network reset trace view ];
  allow-commands "request system reboot";
}
user cmartin {
  class superuser;
    authentication {
    encrypted-password "$1$ABC123";
  }
}
```

The following example shows how to create accounts for four router or switch users, and create an account for the template user **remote**. All users use one of the default system login classes. User **alexander** also has two digital signal algorithm (DSA) public keys configured for SSH authentication.

```
[edit]
system {
  login {
    user philip {
      full-name “Philip of Macedonia”;
      uid 1001;
      class super-user;
      authentication {
        encrypted-password “$ABC123”;
      }
    }
    user alexander {
      full-name “Alexander the Great”;
      uid 1002;
      class view;
      authentication {
        encrypted-password “$ABC123”;
        ssh-dsa “8924 37 5678 5678@gaugamela.per”;
        ssh-dsa “6273 94 9283@boojum.per”;
      }
    }
    user darius {
      full-name “Darius King of Persia”;
      uid 1003;
```



```
        class operator;
        authentication {
          ssh-rsa “1024 37 12341234@ecbatana.per”;
        }
      }
      user anonymous {
        class unauthorized;
      }
      user remote {
        full-name “All remote users”;
        uid 9999;
        class read-only;
      }
    }
}
```

The following example shows how to create accounts for four router or switch users, and create an account for the template user **remote**. All users use one of the default system login classes. User **alexander** also has two digital signal algorithm (DSA) public keys configured for SSH authentication.

```
[edit]
system {
  login {
    user philip {
      full-name “Philip of Macedonia”;
      uid 1001;
      class super-user;
      authentication {
        encrypted-password “$ABC123”;
      }
    }
    user alexander {
      full-name “Alexander the Great”;
      uid 1002;
      class view;
      authentication {
        encrypted-password “$ABC123”;
        ssh-dsa “8924 37 5678 5678@gaugamela.per”;
        ssh-dsa “6273 94 9283@boojum.per”;
      }
    }
    user darius {
      full-name “Darius King of Persia”;
      uid 1003;
      class operator;
      authentication {
        ssh-rsa “1024 37 12341234@ecbatana.per”;
      }
    }
    user anonymous {
      class unauthorized;
    }
    user remote {
```

```
        full-name “All remote users”;
        uid 9999;
        class read-only;
      }
    }
}
```

The following example shows how to create accounts for four router or switch users, and create an account for the template user **remote**. All users use one of the default system login classes. User **alexander** also has two digital signal algorithm (DSA) public keys configured for SSH authentication.

```
[edit]
system {
  login {
    user philip {
      full-name “Philip of Macedonia”;
      uid 1001;
      class super-user;
      authentication {
        encrypted-password “$ABC123”;
      }
    }
    user alexander {
      full-name “Alexander the Great”;
      uid 1002;
      class view;
      authentication {
        encrypted-password “$ABC123”;
        ssh-dsa “8924 37 5678 5678@gaugamela.per”;
        ssh-dsa “6273 94 9283@boojum.per”;
      }
    }
    user darius {
      full-name “Darius King of Persia”;
      uid 1003;
      class operator;
      authentication {
        ssh-rsa “1024 37 12341234@ecbatana.per”;
      }
    }
    user anonymous {
      class unauthorized;
    }
    user remote {
      full-name “All remote users”;
      uid 9999;
      class read-only;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and specify a user template account. Do one of the following tasks:

- Configure a RADIUS server. See "Example: Configuring a RADIUS Server for System Authentication" on page 187.
- Configure a TACACS+ server. See "Example: Configuring a TACACS+ Server for System Authentication" on page 210.
- Configure a user. See "Example: Configuring New Users" on page 70.
- Configure template accounts. See "Example: Creating Template Accounts" on page 165.

Verification

Confirm that the configuration is working properly.

Verifying the New Users Configuration

Purpose Verify that the new users have been configured.

Action From operational mode, enter the **show system login** command.

Configuring Junos OS User Accounts by Using a Configuration Group

User accounts provide a way for users to access a router or switch. Junos OS requires that all users have a predefined user account before they can log in to the device. For each user account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

It is a common practice to use remote authentication servers to centrally store information about users. Even so, it is also a good practice to configure at least one nonroot user directly on each device, in case access to the remote authentication server is disrupted. This one nonroot user commonly has a generic name, such as **admin**.

Because user accounts are configured on multiple devices, they are commonly configured inside of a configuration group. As such, the examples shown here are in a configuration group called **global**. Using a configuration group for your user accounts is optional.

To create a user account:

1. Add a new user, using the user's assigned account login name.

```
[edit groups global]
user@host# edit system login user username
```

2. (Optional) Configure a full descriptive name for the account.

   If the full name includes spaces, enclose the entire name in quotation marks.

   ```
   [edit groups global system login user user-name]
   user@host# set full-name complete-name
   ```

   For example:

   ```
   user@host# show groups
   global {
     system {
       login {
         user admin {
           full-name "general administrator";
         }
       }
     }
   }
   ```

3. (Optional) Set the user identifier (UID) for the account.

   As with UNIX systems, the UID enforces user permissions and file access. If you do not set the UID, Junos OS assigns one for you. The format of the UID is a number in the range of 100 to 64000.

   ```
   [edit groups global system login user user-name]
   user@host# set uid uid-value
   ```

   For example:

   ```
   user@host# show groups
   global {
     system {
       login {
         user admin {
           uid 9999;
         }
       }
     }
   }
   ```

4. Assign the user to a login class.

   You can define your own login classes or assign one of the predefined Junos OS login classes.

   The predefined login classes are as follows:

   - super-user—all permissions
   - operator—clear, network, reset, trace, and view permissions

- read-only— view permissions
- unauthorized—no permissions

```
[edit groups global system login user user-name]
user@host# set class class-name
```

For example:

```
user@host# show groups
global {
    system {
        login {
            user admin {
                class super-user;
            }
        }
    }
}
```

5. Use one of the following methods to configure the user password.

   - To enter a clear-text password that the system encrypts for you, use the following command to set the user password:

     ```
     [edit groups global system login user user-name]
     user@host# set authentication plain-text-password password
     New Password: type password here
     Retype new password: retype password here
     ```

     As you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password as in some other systems. Plain-text passwords are therefore hidden and marked as ## SECRET-DATA in the configuration.

   - To enter a password that is already encrypted, use the following command to set the user password:

     CAUTION: Do not use the encrypted-password option unless the password is *already* encrypted, and you are entering the encrypted version of the password.

     If you accidentally configure the encrypted-password option with a plain-text password or with blank quotation marks (" "), you will not be able to log in to the device as this user.

     ```
     [edit groups global system login user user-name]
     user@host# set authentication encrypted-password "password"
     New Password: type password here
     Retype new password: retype password here
     ```

- To load previously generated public keys from a named file at a specified URL location, use the following command to set the user password:

```
[edit groups global system login user user-name]
user@host# set authentication load-key-file URL filename
```

- To enter an ssh public string, use the following command to set the user password:

```
[edit groups global system login user user-name]
user@host# set authentication (ssh-dsa | ssh-ecdsa | ssh-rsa) authorized-key
```

6. At the top level of the configuration, apply the configuration group.

   If you use a configuration group, you must apply it for it to take effect.

```
[edit]
user@host# set apply-groups global
```

7. Commit the configuration.

```
user@host# commit
```

8. To verify the configuration, log out and log back in as the new user.

Release History Table

Release	Description
18.3R1	Starting in Junos OS Release 18.3R1, the **ssh-dss** and **ssh-dsa** hostkey algorithms are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Related Documentation

- Junos OS Administrative Roles on page 79
- Junos OS User Access Privileges on page 90
- Junos OS User Accounts Overview on page 67

Junos OS Administrative Roles

Junos OS allows you to define a system user to act as a particular kind of administrator for the system. You can assign an administrative role to a user by configuring a login class to have the administrative role attributes. You can assign one of the role attributes such as audit-officer crypto-officer, security-officer, ids-officer to an administrative user. Read this topic for more information.

- Understanding Administrative Roles on page 80
- Example: Configuring Administrative Roles on page 82
- Configuring a Local Administrator Account on page 89

Understanding Administrative Roles

A system user can be a member of a class that allows the user to act as a particular kind of administrator for the system. Requiring a specific role to view or modify an item restricts the extent of information a user can obtain from the system. It also limits how much of the system is open to intentional or unintentional modification or observation by a user. We recommend that you use the following guidelines when you are designing administrative roles:

- Do not allow any user to log in to the system as **root**.
- Restrict each user to the smallest set of privileges needed to perform the user's duties.
- Do not allow any user to belong to a login class containing the **shell** permission flag. The **shell** permission flag allows users to run the **start shell** command from the CLI.
- Allow users to have rollback permissions. Rollback permissions allow users to undo an action performed by an administrator but does not allow them to commit the changes.

You can assign an administrative role to a user by configuring a login class to have the privileges required for that role. You can configure each class to allow or deny access to configuration statements and commands by name. These specific restrictions override and take precedence over any permission flags also configured in the class. You can assign one of the following role attributes to an administrative user.

- **Crypto-administrator**—Allows the user to configure and monitor cryptographic data.
- **Security-administrator**—Allows the user to configure and monitor security data.
- **Audit-administrator**—Allows the user to configure and monitor audit data.
- **IDS-administrator**—Allows the user to monitor and clear the intrusion detection service (IDS) security logs.

Each role can perform the following specific management functions:

- **Cryptographic Administrator**
  - Configures the cryptographic self-test.
  - Modifies the cryptographic security data parameters.
- **Audit Administrator**
  - Configures and deletes the audit review search and sort feature.
  - Searches and sorts audit records.
  - Configures search and sort parameters.
  - Manually deletes audit logs.
- **Security Administrator**

- Invokes, determines, and modifies the cryptographic self-test behavior.
- Enables, disables, determines, and modifies the audit analysis and audit selection functions and configures the device to automatically delete audit logs.
- Enables or disables security alarms.
- Specifies limits for quotas on Transport Layer connections.
- Specifies the limits, network identifiers, and time periods for quotas on controlled connection-oriented resources.
- Specifies the network addresses permitted to use Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP).
- Configures the time and date used in time stamps.
- Queries, modifies, deletes, and creates the information flow or access control rules and attributes for the unauthenticated information flow security function policy (SFP), the authenticated information flow SFP, the unauthenticated device services, and the discretionary access control policy.
- Specifies initial values that override default values when object information is created under unauthenticated information flow SFP, the authenticated information flow SFP, the unauthenticated target of evaluation (TOE) services, and the discretionary access control policy.
- Creates, deletes, or modifies the rules that control the address from which management sessions can be established.
- Specifies and revokes security attributes associated with the users, subjects, and objects.
- Specifies the percentage of audit storage capacity at which the device alerts administrators.
- Handles authentication failures and modifies the number of failed authentication attempts through SSH or from the CLI that can occur before progressive throttling is enforced for further authentication attempts and before the connection is dropped.
- Manages basic network configuration of the device.

- **IDS Administrator**—Specifies IDS security alarms, intrusion alarms, audit selections, and audit data.

You need to set the security-role attribute in the classes created for these administrative roles. This attribute restricts which users can show and clear the security logs, actions that cannot be performed through configuration alone.

For example, you need to set the security-role attribute in the **ids-admin** class created for the IDS administrator role if you want to restrict clearing and showing IDS logs to the IDS administrator role. Likewise, you need to set the security-role to one of the other admin values to restrict that class from being able to clear and show non-IDS logs only.

NOTE: When a user deletes an existing configuration, the configuration statements under the hierarchy level of the deleted configuration (that is, the child objects that the user does not have permission to modify), now remain in the device.

Example: Configuring Administrative Roles

This example shows how to configure individual administrative roles for a distinct, unique set of privileges apart from all other administrative roles.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

This example configures four users:

- **audit-officer** of the class **audit-admin**
- **crypto-officer** of the class **crypto-admin**
- **security-officer** of the class **security-admin**
- **ids-officer** of the class **ids-admin**

When a **security-admin** class is configured, the privileges for creating administrators are revoked from the user who created the **security-admin** class. Creation of new users and logins is at the discretion of the **security-officer**.

In this example, you create audit admin, crypto admin, security admin, and ids admin with permission flags pertaining to this role. Then you allow or deny access to configuration statements and commands by name for each administrative role. These specific restrictions take precedence over the permission flags also configured in the class. For example, only the **crypto-admin** can run the **request system set-encryption-key** command, which requires having the **security** permission flag to access it. Only the **security-admin** can include the **system time-zone** statement in the configuration, which requires having the **system-control** permission flag.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login class audit-admin permissions security
set system login class audit-admin permissions trace
set system login class audit-admin permissions maintenance
set system login class audit-admin allow-commands "^clear (log|security log)"
set system login class audit-admin deny-commands "^clear (security alarms|system
  login lockout)|^file (copy|delete|rename)|^request (security|system
  set-encryption-key)|^rollback|^set date|^show security
  (alarms|dynamic-policies|match-policies|policies)|^start shell";
set system login class audit-admin security-role audit-administrator
set system login class crypto-admin permissions admin-control
set system login class crypto-admin permissions configure
set system login class crypto-admin permissions maintenance
set system login class crypto-admin permissions security-control
set system login class crypto-admin permissions system-control
set system login class crypto-admin permissions trace
set system login class crypto-admin allow-commands "^request system
  set-encryption-key"
set system login class crypto-admin deny-commands "^clear (log|security alarms|security
  log|system login lockout)|^file (copy|delete|rename)|^rollback|^set date|^show security
  (alarms|dynamic-policies|match-policies|policies)|^start shell"
set system login class crypto-admin allow-configuration-regexps "security (ike|ipsec)
  (policy|proposal)" "security ipsec ^vpn$ .* manual
  (authentication|encryption|protocol|spi)" "system fips self-test after-key-generation"
set system login class crypto-admin security-role crypto-administrator
set system login class security-admin permissions all
set system login class security-admin deny-commands "^clear (log|security
  log)|^(clear|show) security alarms alarm-type idp|^request (security|system
  set-encryption-key)|^rollback|^start shell"
set system login class security-admin deny-configuration-regexps "security alarms
  potential-violation idp" "security (ike|ipsec) (policy|proposal)" "security ipsec ^vpn$
  .* manual (authentication| encryption|protocol|spi)" "security log cache" "security log
  exclude .* event-id IDP_.*" "system fips self-test after-key- generation"
set system login class security-admin security-role security-administrator
set system login class ids-admin permissions configure
set system login class ids-admin permissions security-control
set system login class ids-admin permissions trace
set system login class ids-admin permissions maintenance
set system login class ids-admin allow-configuration-regexps "security alarms
  potential-violation idp" "security log exclude .* event-id IDP_.*"
set system login class ids-admin deny-commands "^clear log|^(clear|show) security
  alarms (alarm-id|all|newer-than|older- than|process|severity)|^(clear|show) security
  alarms alarm-type
  (authentication|cryptographic-self-test|decryption-failures|encryption-failures|
  ike-phase1-failures|ike-phase2-failures|key-generation-self-test|
non-cryptographic-self-test|policy|replay-attacks)|^file (copy|delete|rename)|^request
  (security|system set-encryption-key)|^rollback|
^set date|^show security (dynamic-policies|match-policies|policies)|^start shell"
set system login class ids-admin deny-configuration-regexps "security alarms
  potential-violation (authentication|cryptographic-self-test|decryption-
failures|encryption-failures|ike-phase1-failures|ike-phase2-failures|
key-generation-self-test|non-cryptographic-self-test|policy|replay-attacks)"
set system login class ids-admin security-role ids-admin
set system login user audit-officer class audit-admin
set system login user crypto-officer class crypto-admin
set system login user security-officer class security-admin
```

```
set system login user ids-officer class ids-admin
set system login user audit-officer authentication plain-text-password
set system login user crypto-officer authentication plain-text-password
set system login user security-officer authentication plain-text-password
set system login user ids-officer authentication plain-text-password
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode*.

To configure users in administrative roles:

1. Create the **audit-admin** login class.

```
[edit]
user@host# set system login class audit-admin
[edit system login class audit-admin]
user@host# set permissions security
user@host# set permissions trace
user@host# set permissions maintenance
```

2. Configure the **audit-admin** login class restrictions.

```
[edit system login class audit-admin]
user@host# set allow-commands "^clear (log|security log)"
user@host# set deny-commands "^clear (security alarms|system login lockout)|^file
   (copy|delete|rename)|^request (security|system
   set-encryption-key)|^rollback|^set date|^show security
   (alarms|dynamic-policies|match-policies|policies)|^start shell"
user@host# set security-role audit-administrator
```

3. Create the **crypto-admin** login class.

```
[edit]
user@host# set system login class crypto-admin

[edit system login class crypto-admin]
user@host# set permissions admin-control
user@host# set permissions configure
user@host# set permissions maintenance
user@host# set permissions security-control
user@host# set permissions system-control
user@host# set permissions trace
```

4. Configure the **crypto-admin** login class restrictions.

```
[edit system login class crypto-admin]
user@host# set allow-commands "^request system set-encryption-key"
```

```
user@host# set deny-commands "^clear (log|security alarms|security log|system
   login lockout)|^file (copy|delete|rename)|^rollback|^set date|^show security
   (alarms|dynamic-policies|match-policies|policies)|^start shell"
user@host# set allow-configuration-regexps "security (ike|ipsec) (policy|proposal)"
   "security ipsec ^vpn$ .* manual (authentication|encryption|protocol|spi)" "system
   fips self-test after-key-generation"
user@host# set security-role crypto-administrator
```

5. Create the **security-admin** login class.

```
[edit]
user@host# set system login class security-admin

[edit system login class security-admin]
user@host# set permissions all
```

6. Configure the **security-admin** login class restrictions.

```
[edit system login class security-admin]
user@host# set deny-commands "^clear (log|security log)|^(clear|show) security
   alarms alarm-type idp|^request (security|system
   set-encryption-key)|^rollback|^start shell"
user@host# set deny-configuration-regexps "security alarms potential-violation
   idp" "security (ike|ipsec) (policy|proposal)" "security ipsec ^vpn$ .* manual
   (authentication| encryption|protocol|spi)" "security log cache" "security log
   exclude .* event-id IDP_.*" "system fips self-test after-key- generation"
user@host# set security-role security-administrator
```

7. Create the **ids-admin** login class.

```
[edit]
user@host# set system login class ids-admin

[edit system login class ids-admin]
user@host# set permissions configure
user@host# set permissions maintenance
user@host# set permissions security-control
user@host# set permissions trace
```

8. Configure the **ids-admin** login class restrictions.

```
[edit system login class ids-admin]
user@host# set allow-configuration-regexps "security alarms potential-violation
   idp" "security log exclude .* event-id IDP_.*"
set system login class ids-admin deny-commands "^clear log|^(clear|show) security
   alarms (alarm-id|all|newer-than|older- than|process|severity)|^(clear|show)
   security alarms alarm-type
   (authentication|cryptographic-self-test|decryption-failures|encryption-failures|
   ike-phase1-failures|ike-phase2-failures|key-generation-self-test|
```

```
non-cryptographic-self-test|policy|replay-attacks)|^file
   (copy|delete|rename)|^request (security|system set-encryption-key)|
^rollback|^set date|^show security (dynamic-policies|match-policies|policies)|^start
   shell"
set system login class ids-admin deny-configuration-regexps "security alarms
   potential-violation (authentication|cryptographic-self-test|decryption-
failures|encryption-failures|ike-phase1-failures|ike-phase2-failures|
key-generation-self-test|non-cryptographic-self-test|policy|replay-attacks)"
user@host# set security-role ids-administrator
```

9. Assign users to the roles.

```
[edit]
user@host# set system login

[edit system login]
user@host# set user audit-officer class audit-admin
user@host# set user crypto-officer class crypto-admin
user@host# set user security-officer class security-admin
user@host# set user ids-officer class ids-admin
```

10. Configure passwords for the users.

```
[edit system login]
user@host# set user audit-officer authentication plain-text-password
user@host# set user crypto-officer authentication plain-text-password
user@host# set user security-officer authentication plain-text-password
user@host# set user ids-officer authentication plain-text-password
```

Results

From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# show system
system {
   login {
      class audit-admin {
         permissions [ maintenance security trace ];
         allow-commands "^clear (log|security log)";
         deny-commands "^clear (security alarms|system login lockout)|^file
            (copy|delete|rename)|^request (security|system
            set-encryption-key)|^rollback|^set date|^show security
            (alarms|dynamic-policies|match-policies|policies)|^start shell";
         security-role audit-administrator;
      }
      class crypto-admin {
```

```
    permissions [ admin-control configure maintenance security-control system-control
      trace ];
    allow-commands "^request (system set-encryption-key)";
    deny-commands "^clear (log|security alarms|security log|system login lockout)|^file
      (copy|delete|rename)|^rollback|^set date|^show security
      (alarms|dynamic-policies|match-policies|policies)|^start shell";
    allow-configuration-regexps "security (ike|ipsec) (policy|proposal)" "security ipsec
      ^vpn$ .* manual (authentication|encryption|protocol|spi)" "system fips self-test
      after-key-generation" ;
    security-role crypto-administrator;
  }
  class security-admin {
    permissions [all];
    deny-commands "^clear (log|security log)|^(clear|show) security alarms alarm-type
      idp|^request (security|system set-encryption-key)|^rollback|^start shell";
    deny-configuration-regexps "security alarms potential-violation idp" "security
      (ike|ipsec) (policy|proposal)" "security ipsec ^vpn$ .* manual
      (authentication|encryption|protocol|spi)" "security log exclude .* event-id IDP_.*"
      "system fips self-test after-key-generation";
    security-role security-administrator;
  }
  class ids-admin {
    permissions [ configure maintenance security-control trace ];
    deny-commands "^clear log|^(clear|show) security alarms
      (alarm-id|all|newer-than|older-than|process|severity)|^(clear|show) security
      alarms alarm-type
    (authentication | cryptographic-self-test | decryption-failures | encryption-failures
    | ike-phase1-failures | ike-phase2-failures|key-generation-self-test |
    non-cryptographic-self-test |policy | replay-attacks) | ^file (copy|delete|rename)
    |^request (security|system set-encryption-key) | ^rollback |
    ^set date | ^show security (dynamic-policies|match-policies|policies) |^start shell";
    allow-configuration-regexps "security alarms potential-violation idp" "security log
      exclude .* event-id IDP_.*";
    deny-configuration-regexps "security alarms potential-violation
      (authentication|cryptographic-self-test|decryption-
    failures|encryption-failures|ike-phase1-failures|ike-phase2-failures|
    key-generation-self-test|non-cryptographic-self-test|policy|replay-attacks)"
    security-role ids-administrator;
  }
  user audit-officer {
    class audit-admin;
    authentication {
      encrypted-password "$1$ABC123"; ## SECRET-DATA
    }
  }
  user crypto-officer {
    class crypto-admin;
    authentication {
      encrypted-password "$1$ABC123."; ## SECRET-DATA
    }
  }
  user security-officer {
    class security-admin;
    authentication {
      encrypted-password "$1$ABC123."; ##SECRET-DATA
```

```
      }
    }
    user ids-officer {
      class ids-admin;
      authentication {
        encrypted-password "$1$ABC123/"; ## SECRET-DATA
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Login Permissions

Purpose Verify the login permissions for the current user.

Action From operational mode, enter the **show cli authorization** command.

```
user@host>show cli authorization
Current user: 'example' class 'super-user'
Permissions:
    admin       -- Can view user accounts
    admin-control-- Can modify user accounts
    clear       -- Can clear learned network info
    configure   -- Can enter configuration mode
    control     -- Can modify any config
    edit        -- Can edit full files
    field       -- Can use field debug commands
    floppy      -- Can read and write the floppy
    interface   -- Can view interface configuration
    interface-control-- Can modify interface configuration
    network     -- Can access the network
    reset       -- Can reset/restart interfaces and daemons
    routing     -- Can view routing configuration
    routing-control-- Can modify routing configuration
    shell       -- Can start a local shell
    snmp        -- Can view SNMP configuration
    snmp-control-- Can modify SNMP configuration
    system      -- Can view system configuration
    system-control-- Can modify system configuration
    trace       -- Can view trace file settings
    trace-control-- Can modify trace file settings
    view        -- Can view current values and statistics
    maintenance -- Can become the super-user
    firewall    -- Can view firewall configuration
    firewall-control-- Can modify firewall configuration
    secret      -- Can view secret statements
    secret-control-- Can modify secret statements
    rollback    -- Can rollback to previous configurations
    security    -- Can view security configuration
    security-control-- Can modify security configuration
```

```
    access      -- Can view access configuration
    access-control-- Can modify access configuration
    view-configuration-- Can view all configuration (not including secrets)
    flow-tap    -- Can view flow-tap configuration
    flow-tap-control-- Can modify flow-tap configuration
    idp-profiler-operation-- Can Profiler data
    pgcp-session-mirroring-- Can view pgcp session mirroring configuration
    pgcp-session-mirroring-control-- Can modify pgcp session mirroring configura
tion
    storage     -- Can view fibre channel storage protocol configuration
    storage-control-- Can modify fibre channel storage protocol configuration
    all-control -- Can modify any configuration
Individual command authorization:
    Allow regular expression: none
    Deny regular expression: none
    Allow configuration regular expression: none
    Deny configuration regular expression: none
```

This output summarizes the login permissions.

Configuring a Local Administrator Account

The following example shows how to configure a password- protected local administration account called **admin** with superuser privileges. Superuser privileges give a user permission to use any command on the router and are generally reserved for a select few users such as system administrators. It is important to protect the local administrator account with a password to prevent unauthorized users from gaining access to superuser commands that can be used to alter the system configuration. Even users with RADIUS authentication should configure a local password. If RADIUS fails or becomes unreachable, the login process will revert to password authentication on the local administrator account.

```
[edit]
system {
  login {
    user admin {
      uid 1000;
      class superuser;
      authentication {
        encrypted-password "<PASSWORD>"; # SECRET-DATA
      }
    }
  }
}
```

Related Documentation

- Junos OS Login Classes Overview on page 49
- Configuring Junos OS User Accounts by Using a Configuration Group on page 76

Junos OS User Access Privileges

Junos OS allows you to grant the access or permissions to the commands and configuration hierarchy levels and statements. This enables users to execute only those commands and configure and view only those statements for which they have access privileges. You can use extended regular expressions to specify which operational mode commands, configuration statements, and hierarchies are denied or allowed for users. This prevents unauthorized users from executing or configuring sensitive commands and statements that could potentially cause damage to the network. Read this topic for more information.

Understanding Junos OS Access Privilege Levels

Each top-level CLI command and each configuration statement have an access privilege level associated with them. Users can execute only those commands and configure and view only those statements for which they have access privileges. The access privileges for each login class are defined by one or more permission flags.

For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level specified in the **permissions** statement.

The following sections provide additional information about permissions:

Junos OS Login Class Permission Flags

Permission flags are used to grant a user access to operational mode commands and configuration hierarchy levels and statements. By specifying a specific permission flag on the user's login class at the **[edit system login class]** hierarchy level, you grant the user access to the corresponding commands and configuration hierarchy levels and statements. To grant access to all commands and configuration statements, use the **all** permissions flag.

NOTE: Each command listed represents that command and all subcommands with that command as a prefix. Each configuration statement listed represents the top of the configuration hierarchy to which that flag grants access.

The **permissions** statement specifies one or more of the permission flags listed in Table 5 on page 91. Permission flags are not cumulative, so for each class you must list all the permission flags needed, including **view** to display information and **configure** to enter configuration mode. Two forms of permissions control for individual parts of the configuration are:

- "Plain" form—Provides read-only capability for that permission type. An example is **interface**.
- Form that ends in **-control**—Provides read and write capability for that permission type. An example is **interface-control**.

For permission flags that grant access to configuration hierarchy levels and statements, the flags grant read-only privilege to that configuration. For example, the **interface** permissions flag grants read-only access to the **[edit interfaces]** hierarchy level. The **-control** form of the flag grants read-write access to that configuration. Using the preceding example, **interface-control** grants read-write access to the **[edit interfaces]** hierarchy level.

Table 5 on page 91 lists the Junos OS login class permission flags that you can configure by including the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level.

The permission flags grant a specific set of access privileges. Each permission flag is listed with the operational mode commands and configuration hierarchy levels and statements for which that flag grants access.

Table 5: Login Class Permission Flags

Permission Flag	Description
access	Can view the access configuration in configuration mode and with the **show configuration** operational mode command.
access-control	Can view and configure access information at the **[edit access]** hierarchy level.
admin	Can view user account information in configuration mode and with the **show configuration** operational mode command.
admin-control	Can view user account information and configure it at the **[edit system]** hierarchy level.
all-control	Can view user accounts and configure them at the **[edit system login]** hierarchy level.

Table 5: Login Class Permission Flags (continued)

Permission Flag	Description
all	Can access all operational mode commands and configuration mode commands. Can modify configuration in all the configuration hierarchy levels.
clear	Can clear (delete) information learned from the network that is stored in various network databases by using the **clear** commands.
configure	Can enter configuration mode by using the **configure** command.
control	Can perform all control-level operations—all operations configured with the **-control** permission flags.
field	Can view field debug commands. Reserved for debugging support.
firewall	Can view the firewall filter configuration in configuration mode.
firewall-control	Can view and configure firewall filter information at the **[edit firewall]** hierarchy level.
floppy	Can read from and write to the removable media.
flow-tap	Can view the flow-tap configuration in configuration mode.
flow-tap-control	Can view the flow-tap configuration in configuration mode and can configure flow-tap configuration information at the **[edit services flow-tap]** hierarchy level.
flow-tap-operation	Can make flow-tap requests to the router or switch. For example, a Dynamic Tasking Control Protocol (DTCP) client must have **flow-tap-operation** permission to authenticate itself to the Junos OS as an administrative user. NOTE: The **flow-tap-operation** option is not included in the **all-control** permissions flag.
idp-profiler-operation	Can view profiler data.
interface	Can view the interface configuration in configuration mode and with the **show configuration** operational mode command.

Table 5: Login Class Permission Flags (continued)

Permission Flag	Description
interface-control	Can view chassis, class of service (CoS), groups, forwarding options, and interfaces configuration information. Can edit configuration at the following hierarchy levels: • **[edit chassis]** • **[edit class-of-service]** • **[edit groups]** • **[edit forwarding-options]** • **[edit interfaces]**
maintenance	Can perform system maintenance, including starting a local shell on the router or switch and becoming the superuser in the shell by using the **su root** command, and can halt and reboot the router or switch by using the **request system** commands.
network	Can access the network by using the **ping**, **ssh**, **telnet**, and **traceroute** commands.
pgcp-session-mirroring	Can view the **pgcp** session mirroring configuration.
pgcp-session-mirroring-control	Can modify the **pgcp** session mirroring configuration.
reset	Can restart software processes by using the **restart** command and can configure whether software processes are enabled or disabled at the **[edit system processes]** hierarchy level.
rollback	Can use the **rollback** command to return to a previously committed configuration other than the most recently committed one.
routing	Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.
routing-control	Can view general routing, routing protocol, and routing policy configuration information and can configure general routing at the **[edit routing-options]** hierarchy level, routing protocols at the **[edit protocols]** hierarchy level, and routing policy at the **[edit policy-options]** hierarchy level.
secret	Can view passwords and other authentication keys in the configuration.
secret-control	Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.
security	Can view security configuration in configuration mode and with the **show configuration** operational mode command.

Table 5: Login Class Permission Flags (continued)

Permission Flag	Description
security-control	Can view and configure security information at the **[edit security]** hierarchy level.
shell	Can start a local shell on the router or switch by using the **start shell** command.
snmp	Can view Simple Network Management Protocol (SNMP) configuration information in configuration and operational modes.
snmp-control	Can view SNMP configuration information and can modify SNMP configuration at the **[edit snmp]** hierarchy level.
system	Can view system-level information in configuration and operational modes.
system-control	Can view system-level configuration information and configure it at the **[edit system]** hierarchy level.
trace	Can view trace file settings and configure trace file properties.
trace-control	Can modify trace file settings and configure trace file properties.
view	Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics. Cannot view the secret configuration.
"view-configuration" on page 1612	Can view all of the configuration excluding secrets, system scripts, and event options. NOTE: Only users with the **maintenance** permission can view commit script, op script, or event script configuration.

Allowing or Denying Individual Commands for Junos OS Login Classes

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level specified in the **permissions** statement.

Permission flags are used to grant a user access to operational mode commands and configuration hierarchy levels and statements. By specifying a specific permission flag on the user's login class at the **[edit system login class]** hierarchy level, you grant the user access to the corresponding commands and configuration hierarchy levels and statements. To grant access to all commands and configuration statements, use the **all** permissions flag. For permission flags that grant access to configuration hierarchy levels and statements, the flags grant read-only privilege to that configuration. For example, the **interface** permissions flag grants read-only access to the **[edit interfaces]** hierarchy

level. The **-control** form of the flag grants read-write access to that configuration. Using the preceding example, **interface-control** grants read-write access to the **[edit interfaces]** hierarchy level.

- The **all** login class permission bits take precedence over extended regular expressions when a user issues **rollback** command with **rollback** permission flag enabled.
- Expressions used to allow and deny commands for users on RADIUS and TACACS+ servers have been simplified. Instead of a single, long expression with multiple commands (**allow-commands=cmd1 cmd2 ... cmd*n***), you can specify each command as a separate expression. This new syntax is valid for **allow-configuration**, **deny-configuration**, **allow-commands**, **deny-commands**, and all user permission bits.
- Users cannot issue the **load override** command when specifying an extended regular expression. Users can only issue the **merge**, **replace**, and **patch** configuration commands.
- If you allow and deny the same commands, the **allow-commands** permissions take precedence over the permissions specified by the **deny-commands**. For example, if you include **allow-commands "request system software add"** and **deny-commands "request system software add"**, the login class user is allowed to install software using the **request system software add** command.
- Regular expressions for **allow-commands** and **deny-commands** can also include the **commit**, **load**, **rollback**, **save**, **status**, and **update** commands.
- If you specify a regular expression for **allow-commands** and **deny-commands** with two different variants of a command, the longest match is always executed.

  For example, if you specify a regular expression for **allow-commands** with the **commit-synchronize** command and a regular expression for **deny-commands** with the **commit** command, users assigned to such a login class would be able to issue the **commit synchronize** command, but not the **commit** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize** and it is specified for **allow-commands**.

  Likewise, if you specify a regular expression for **allow-commands** with the **commit** command and a regular expression for **deny-commands** with the **commit-synchronize** command, users assigned to such a login class would be able to issue the **commit** command, but not the **commit-synchronize** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize** and it is specified for **deny-commands**.

Example: Configuring User Permissions with Access Privilege Levels

This example shows how to view permissions for a user account and configure the user permissions with access privileges for a login class. This enables users to execute only those commands and configure and view only those statements for which they have access privileges. This prevents unauthorized users from executing or configuring sensitive commands and statements that could potentially cause damage to the network.

- Requirements on page 96
- Overview on page 96

Requirements

This example uses the following hardware and software components:

- One Juniper Networks device
- One TACACS+ (or RADIUS) server
- Junos OS build running on the Juniper Networks device

Before you begin:

- Establish connection between the device and the TACACS+ server.

  For information on configuring a TACACS+ server, see "Configuring TACACS+ Authentication" on page 207.

- Configure at least one user assigned to a login class on the Juniper Networks device. There can be more than one login class, each with varying permission configurations, and more than one user on the device.

Overview

Each top-level command-line interface (CLI) command and each configuration statement in Junos OS has an access privilege level associated with it. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level. Users can execute only those commands and configure and view only those statements for which they have access privileges. To configure access privilege levels, include the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level.

The access privileges for each login class are defined by one or more permission flags specified in the **permissions** statement. Permission flags are used to grant a user access to operational mode commands, statements, and configuration hierarchies. Permission flags are not cumulative, so for each login class you must list all the permission flags needed, including **view** to display information and **configure** to enter configuration mode. By specifying a specific permission flag on the user's login class, you grant the user access to the corresponding commands, statements, and configuration hierarchies. To grant access to all commands and configuration statements, use the **all** permissions flag. The permission flags provide read-only ("plain" form) and read and write (form that ends in -control) capability for a permission type.

NOTE: **The all login class permission bits take precedence over extended regular expressions when a user issues a rollback command with the rollback permission flag enabled.**

To configure user access privilege levels:

1. View permissions for a user account.

   You can view the permissions for a user account before configuring the access privileges for those permissions.

   To view the user permissions, enter **?** at the **[edit]** hierarchy level:

   ```
   [edit]
   ?
   ```

2. Configure user permissions with access privileges.

   All users who can log in to a device must be in a login class. For each login class, you can configure the access privileges that the associated users can have when they are logged in to the device.

   To configure access privilege levels for user permissions, include the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level, followed by the user permission, the **permissions** option, and the required permission flags.

   ```
   [edit system login]
   user@host# set class class-name permissions user-permission permissions [permission
     flags];
   ```

Configuration

Configuring User Permissions with Access Privilege Levels

Step-by-Step Procedure

To configure access privileges:

1. From the device, view the list of permissions available for the user account. In this example, the username of the user account is host.

   ```
   [edit]
   user@host> ?
     Possible completions:
       clear                Clear information in the system
       configure            Manipulate software configuration information
       file                 Perform file operations
       help                 Provide help information
       load                 Load information from file
       monitor              Show real-time debugging information
       mtrace               Trace multicast path from source to receiver
       op                   Invoke an operation script
       ping                 Ping remote target
       quit                 Exit the management session
       request              Make system-level requests
       restart              Restart software process
       save                 Save information to file
       set                  Set CLI properties, date/time, craft interface
     message
       show                 Show system information
       ssh                  Start secure shell on another host
   ```

```
    start                Start shell
    telnet               Telnet to another host
    test                 Perform diagnostic debugging
    traceroute           Trace route to remote host
```

The output lists the permissions for the user host. Customized login classes can be created by configuring different access privileges on these user permissions.

2. Configure an access privilege class to enable user host to configure and view SNMP parameters only. In this example, this login class is called network-management. To customize the network-management login class, include the SNMP permission flags to the **configure** user permission.

```
[edit system login class network-management]
user@host# set permissions configure permissions snmp
user@host# set permissions configure permissions snmp-control
```

Here, the configured permission flags provide both read (snmp) and read-and-write (snmp-control) capability for SNMP, and this is the only allowed access privilege for the network-management login class. In other words, all other access privileges other than configuring and viewing SNMP parameters are denied.

Results

From configuration mode, confirm your configuration by entering the **show system login** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show system login
class network-management {
  permissions [ configure snmp snmp-control ];
}
```

Verification

Log in as the username assigned with the new login class, and confirm that the configuration is working properly.

- Verifying SNMP Configuration on page 98
- Verifying non-SNMP Configuration on page 99

Verifying SNMP Configuration

Purpose Verify that SNMP configuration can be executed.

Action From configuration mode, execute basic SNMP commands at the **[edit snmp]** hierarchy level.

```
[edit snmp]
```

```
user@host# set name device1
user@host# set description switch1
user@host# set location Lab1
user@host# set contact example.com
user@host# commit
```

Meaning The user host assigned to the network-management login class is able to configure SNMP parameters, as the permission flags specified for this class include both snmp (read capabilities) and snmp-control (read and write capabilities) permission bits.

Verifying non-SNMP Configuration

Purpose Verify that non-SNMP configuration is denied for the network-management login class.

Action From the configuration mode, execute any non-SNMP configuration, for example, interfaces configuration.

```
[edit]
user@host# edit interfaces
  Syntax error, expecting <statement> or <identifier>.
```

Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies

This topic contains the following sections:

Understanding Regular Expressions

You can use extended regular expressions to specify which operational mode commands, configuration statements, and hierarchies are denied or allowed. You specify these regular expressions locally in the **allow/deny-commands**, **allow/deny-configuration,** and **allow/deny-commands-regexps** and **allow/deny-configuration-regexp** statements at the **[edit system login class *class-name*]** hierarchy level, or remotely by specifying Juniper Networks vendor-specific TACACS+ or RADIUS attributes in your authorization server's configuration.

NOTE: Starting in Junos OS Release 18.1, the **allow-commands-regexps** and **deny-commands-regexps** statements are supported for TACACS+ authorization.

The difference between a local and remote authorization configuration is the pattern in which the regular expressions statements are executed. While it is possible to specify multiple regular expressions using strings in the local authorization configuration, in a remote configuration, the regular expressions statements need to be split and specified in individual strings. When the authorization parameters are configured both remotely and locally, the regular expressions received during TACACS+ or RADIUS authorization get merged with any regular expressions available on the local device.

When specifying multiple regular expressions in a local configuration using the **allow-configuration**, **deny-configuration**, **allow-commands**, or **deny-commands** statements, regular expressions are configured within parentheses and separated using the pipe symbol. The complete expression is enclosed in double quotes. For example, you can specify multiple **allow-commands** parameters with the following syntax:

allow-commands "(cmd1)|(cmd2)|(cmd*n*)"

The same expression configured remotely on the authorization server uses the following syntax:

```
allow-commands1 = "cmd1"
allow-commands2 = "cmd2"
allow-commandsn = "cmdn"
```

When specifying multiple regular expressions in a local configuration using the **allow-configuration-regexps**, **deny-configuration-regexps**, **allow-commands-regexps**, or **deny-commands-regexps** statements, regular expressions are configured within double quotes and separated using the space operator. The complete expression is enclosed in square brackets. For example, you can specify multiple allow-commands parameters with the following syntax:

allow-commands-regexps ["cmd1" "cmd2" "cmd*n*"]

The same expression configured remotely on the authorization server uses the following syntax:

```
allow-commands-regexps1 = "cmd1"
allow-commands-regexps2 = "cmd2"
allow-commands-regexpsn = "cmdn"
```

Table 6 on page 101 differentiates the local and remote authorization configuration using regular expressions.

Table 6: Sample Local and Remote Authorization Configuration Using Regular Expressions

Local Configuration	Remote Configuration

login {
  class local {
  permissions configure;
  allow-commands "(ping .*)|(traceroute
  .*)|(show .*)|(configure
  .*)|(edit)|(exit)|(commit)|(rollback .*)";
  deny-commands .*;
  allow-configuration "(interfaces .* unit 0
  family ethernet-switching vlan mem.*
  .*)|(interfaces .* native.* .*)|(interfaces
  .* unit 0 family ethernet-switching
  interface-mo.* .*)|(interfaces .* unit
  .*)|(interfaces .* disable)|(interfaces .*
  description .*)|(vlans .* vlan-.* .*)"
  deny-configuration .*;
  }
}
	user = remote {
	  login = username
	  service = junos-exec {
	  allow-commands1 = "ping .*"
	  allow-commands2 = "traceroute .*"
	  allow-commands3 = "show .*"
	  allow-commands4 = "configure"
	  allow-commands5 = "edit"
	  allow-commands6 = "exit"
	  allow-commands7 = "commit"
	  allow-commands8 = ".*xml-mode" <<<<<
	  allow-commands9 = ".*netconf" <<<<<
	  allow-commands10 = ".*need-trailer" <<<<<
	  allow-commands11 = "rollback.*"
	  deny-commands1 = ".*"
	  allow-configuration1 = "interfaces .* unit 0 family
	  ethernet-switching vlan mem.* .*"
	  allow-configuration2 = "interfaces .* native.* .*"
	  allow-configuration3 = "interfaces .* unit 0 family
	  ethernet-switching interface-mo.* .*"
	  allow-configuration4 = "interfaces .* unit .*"
	  allow-configuration5 = "interfaces .* disable"
	  allow-configuration6 = "interfaces .* description .*"
	  allow-configuration7 = "interfaces .*"
	  allow-configuration8 = "vlans .* vlan-.* .*"
	  deny-configuration1 = ".*"
	  local-user-name = *local-username*
	  user-permissions = "configure"
	  }
	}

NOTE:

- You need to explicitly allow access to the NETCONF mode, either locally or remotely, by issuing the following three commands: **xml-mode**, **netconf**, and **need-trailer**.
- When the **deny-configuration = ".*"** statement is used, all the other desired configurations should be allowed using the **allow-configuration** statement. This can affect the allowed regular expressions buffer limit for the **allow-configuration** statement. When this limit exceeds, the allowed configuration might not work. This regular expression buffer size limit has been increased in Junos OS Release 14.1x53-D40, 15.1, and 16.1.

Specifying Regular Expressions

WARNING: When you specify regular expression for commands and configuration statements, pay close attention to the following examples, as

regular expression with invalid syntax might not produce the desired results, even if the configuration is committed without any error.

Regular expressions for commands and configuration statements should be specified in the same manner as executing the complete command or statement.
Table 7 on page 102 lists the regular expressions for configuring access privileges for the **[edit interfaces]** and **[edit vlans]** statement hierarchies, and for the **delete interfaces** command.

Table 7: Specifying Regular Expressions

Statement	Regular Expression	Configuration Notes
[edit interfaces] The **set** command for interfaces is executed as follows: [edit] user@host# **set interfaces** *interface-name* **unit** *interface-unit-number*	The **set interfaces** statement is incomplete by itself, and requires the **unit** option to execute the statement. As a result, the regular expression required for denying the **set interfaces** configuration must specify the entire executable string with the **.*** operator in place of statement variables: [edit system login class *class-name*] user@host# **set permissions** *configure* user@host# **set deny-configuration** *"interfaces .* unit .*"*	• The **.*** operator denotes everything from the specified point onward for that particular command or statement. In this example, it denotes any interface name with any unit value. • Specifying only the **deny-configuration "interfaces .*"** statement is incorrect and does not deny access to the interfaces configuration for the specified login class. • Other valid options can be included in the regular expression, for example: [edit system login class *class-name*] user@host# **set permissions** *configure* user@host# **set deny-configuration** *"interfaces .* description .*"* [edit system login class *class-name*] user@host# **set permissions** *configure* user@host# **set allow-configuration-regexps** *["interfaces .* description .*" "interfaces .* unit .* description .*" "interfaces .* unit .* family inet address .*" "interfaces.* disable"]* [edit system login class *class-name*] user@host# **set permissions** *configure* user@host# **set allow-configuration** *"interfaces .* unit 0 family ethernet-switching vlan mem.* .*"* **Note:** The **mem.*** regular expression in this example is used when multiple strings starting with the *mem* keyword are expected to be included in the specified regular expression. When only one **member** string is expected to be included, the **member .*** regular expression is used.

Table 7: Specifying Regular Expressions (continued)

Statement	Regular Expression	Configuration Notes
delete interfaces The **delete** command for interfaces is executed as follows: [edit] user@host# **delete interfaces** *interface-name*	The **delete interfaces** statement can be executed by itself and does not require additional statements to be complete. As a result, the regular expression required for denying the **delete interfaces** statement should specify the following: [edit system login class *class-name*] user@host# **set permissions** *configure* user@host# **set allow-configuration** ***"interfaces .*"*** user@host# **set deny-configuration** ***"interfaces .*"***	• The **.*** operator denotes everything from the specified point onward for that particular command or statement. In this example, it denotes any interface name. • For the **deny-configuration "interfaces .*"** regular expression to take effect, the specified login class should allow configuration permissions for the interfaces hierarchy using the **allow-configuration "interfaces .*"** regular expression.
[edit vlans] The **set** command for VLANs is executed as follows: [edit] user@host# **set vlans** *vlan-name* **vlan-id** *vlan-id*	Here, the **set vlans** statement is incomplete by itself, and requires the **vlan-id** option to execute the statement. As a result, the regular expression required for allowing the **set vlans** configuration must specify the entire executable string with the **.*** operator in place of statement variables: [edit system login class *class-name*] user@host# **set permissions** *configure* user@host# **set allow-configuration** ***"vlans .* vlan-id .*"***	• The **.*** operator denotes everything from the specified point onward for that particular command or statement. In this example, it denotes any VLAN name with any VLAN ID. • Other valid options under the **[edit vlans]** statement hierarchy can be included in the regular expression, for example: [edit system login class *class-name*] user@host# **set permissions** *configure* user@host# **set allow-configuration-regexps** ***["vlans .* vlan-id .*" "vlans .* vlan-id .* description .*" "vlans .* vlan-id .* filter .*"]***

Regular Expressions Operators

Table 8 on page 104 lists common regular expression operators that you can use for allowing or denying operational and configuration modes.

Command regular expressions implement the extended (modern) regular expressions, as defined in POSIX 1003.2.

Table 8: Common Regular Expression Operators

Operator	Match	Example
|	One of two or more terms separated by the pipe. Each term must be a complete standalone expression enclosed in parentheses ( ), with no spaces between the pipe and the adjacent parentheses.	[edit system login class *test*] user@host# **set permissions** *configure* user@host# **set allow-commands** *"(ping)|(traceroute)|(show system alarms)|(show system software)"* user@host# **set deny-configuration** *"(access)|(access-profile)|(accounting-options)|(applications)|(apply-groups)|(bridge-domains)|(chassis)|(class-of-service)"* With the above configuration, the users assigned to the test login class have operational mode access restricted to only the commands specified in the **allow-commands** statement, and access to the configuration mode, excluding the hierarchy levels specified in the **deny-configuration** statement.
^	At the beginning of an expression, used to denote where the command begins, where there might be some ambiguity.	[edit system login class *test*] user@host# **set permissions** *interface* user@host# **set permissions** *interface-control* user@host# **set allow-commands** *"(^show) (log|interfaces|policer))|(^monitor)"* With the above configuration, the users assigned to the test login class have access to configuring and viewing interface configuration from the operational and configuration mode. The **allow-commands** statement specifies access to commands that begin with **show** and **monitor** keywords. For the first filter, the commands specified include the **show log**, **show interfaces**, and **show policer** commands. The second filter specifies all commands starting with the **monitor** keyword, such as **monitor interfaces** or **monitor traffic** commands.
$	Character at the end of a command. Used to denote a command that must be matched exactly up to that point.	[edit system login class *test*] user@host# **set permissions** *interface* user@host# **set allow-commands** *"(show interfaces$)"* With the above configuration, the users assigned to the test login class can view the interface configuration in the configuration mode and with the **show configuration** operational mode command with the interface user permission. However, the regular expression specified in the **allow-commands** statement restricts the users to execute only the **show interfaces** command and denies access to the command extensions, such as **show interfaces detail** or **show interfaces extensive**.
[ ]	Range of letters or digits. To separate the start and end of a range, use a hyphen (-).	[edit system login class *test*] user@host# **set permissions** *clear* user@host# **set permissions** *configure* user@host# **set permissions** *network* user@host# **set permissions** *trace* user@host# **set permissions** *view* user@host# **set allow-configuration-regexps** *["interfaces [gx]e-.* unit [0-9]* description .*"]* With the above configuration, the users assigned to the test login class have operator-level user permissions, and have access to configure interfaces within the specified range of interface name and unit number (0 through 9).

Table 8: Common Regular Expression Operators (continued)

Operator	Match	Example
( )	A group of commands, indicating a complete, standalone expression to be evaluated. The result is then evaluated as part of the overall expression. Parentheses must be used in conjunction with pipe operators, as explained.	[edit system login class *test*] user@host# **set permissions *all*** user@host# **set allow-commands *"(clear)|(configure)"*** user@host# **deny-commands *"(mtrace)|(start)|(delete)"*** With the above configuration, users assigned to the test login class have superuser-level permissions, and have access to the commands specified in the **allow-commands** statement.
*	Zero or more terms.	[edit system login class *test*] user@host# **set permissions *configure*** user@host# **set deny-configuration *"(system login class m*)"*** With the above configuration, users assigned to the test login class whose login username begins with **m** are denied configuration access.
+	One or more terms.	[edit system login class *test*] user@host# **set permissions *configure*** user@host# **set deny-configuration *"(system login class m+)"*** With the above configuration, users assigned to the test login class whose login username begins with **m** are denied configuration access.
.	Any character except for a space " ".	[edit system login class *test*] user@host# **set permissions *configure*** user@host# **set deny-configuration *"(system login class m.)"*** With the above configuration, users assigned to the test login class whose login username begins with **m** are denied configuration access.
.*	Everything from the specified point onward.	[edit system login class *test*] user@host# **set permissions *configure*** user@host# **set deny-configuration *"(system login class m .*)"*** With the above configuration, users assigned to the test login class whose login username begins with **m** are denied configuration access. Similarly, the **deny-configuration "protocols .*"** statement denies all configuration access under the **[edit protocols]** hierarchy level. NOTE: • The *****, **+**, and **.** operations can be achieved by using **.***. • The **deny-commands .*** and **deny-configuration .*** statements deny access to all operational mode commands and configuration hierarchies, respectively.

NOTE: Junos OS does not support the ! regular expression operator.

Regular Expression Examples

Table 9 on page 106 lists the regular expressions used to allow configuration options under two configuration hierarchies—**[edit system ntp server]** and **[edit protocols rip]**—as an example for specifying regular expressions.

NOTE: Table 9 on page 106 does not provide a comprehensive list of all regular expressions and keywords for all configuration statements and hierarchies. The regular expressions listed in the table are supported in Junos OS Release 16.1, and are validated only for the **[edit system ntp server]** and **[edit protocols rip]** statement hierarchies.

Table 9: Regular Expressions Examples

Statement Hierarchy	Regular Expressions	Allowed Configuration	Denied Configuration
[edit system ntp server]			
key *key-number*	[edit system login class test] set permissions configure set allow-configuration-regexps ["system ntp server .*" "system ntp server .* key .*"] set deny-configuration-regexps ["system ntp server .* version .*" "system ntp server .* prefer"]	• server IP • server IP and key	• version • prefer
version *version-number*	[edit system login class test] set permissions configure set allow-configuration-regexps ["system ntp server .*" "system ntp server .* version .*"] set deny-configuration-regexps ["system ntp server .* key .*" "system ntp server .* prefer"]	• server IP • server IP and version	• key • prefer
prefer	[edit system login class test] set permissions configure set allow-configuration-regexps ["system ntp server .*" "system ntp server .* prefer"]; set deny-configuration-regexps ["system ntp server .* key .*" "system ntp server .* version .*"]	• server IP • server IP and prefer	• key • version
[edit protocols rip]			

Table 9: Regular Expressions Examples (continued)

Statement Hierarchy	Regular Expressions	Allowed Configuration	Denied Configuration
message-size *message-size*	[edit system login class test] set permissions configure set allow-configuration-regexps "protocols rip message-size .*" set deny-configuration-regexps ["protocols rip metric-in .*" "protocols rip route-timeout .*" "protocols rip update-interval .*"]	• message-size	• metric-in • route-timeout • update-interval
metric-in *metric-in*	[edit system login class test] set permissions configure set allow-configuration-regexps "protocols rip metric-in .*" set deny-configuration-regexps ["protocols rip message-size .*" "protocols rip route-timeout .*" "protocols rip update-interval .*"]	• metric-in	• message-size • route-timeout • update-interval
route-timeout *route-timeout*	[edit system login class test] set permissions configure set allow-configuration-regexps "protocols rip route-timeout .*" set deny-configuration-regexps ["protocols rip metric-in .*" "protocols rip message-size .*" "protocols rip update-interval .*"]	• route-timeout	• message-size • metric-in • update-interval
update-interval *update-interval*	[edit system login class test] set permissions configure set allow-configuration-regexps "protocols rip update-interval .*" set deny-configuration-regexps ["protocols rip metric-in .*" "protocols rip route-timeout .*" "protocols rip message-size .*"]	• update-interval	• message-size • metric-in • route-timeout

Examples of Defining Access Privileges Using allow-configuration and deny-configuration Statements

You can define access privileges using a combination of the following types of statements:

- permission flags
- **allow-configuration** and **deny-configuration** statements

The permission flags define the larger boundaries of what a person or login class can access and control. The **allow-configuration** and **deny-configuration** statements take precedence over permission flags and give the administrator finer control over exactly what the user has access to.

This topic explains defining access privileges using **allow-configuration** and **deny-configuration** statements by showing a series of examples of login class configuration using these statements. Examples 1 through 3 use both permission flags and **deny-configuration** statements to create login classes that allow users access to all except something. Each **allow-configuration** or **deny-configuration** statement is configured with one or more regular expressions to be allowed or denied.

Notice that *permission bit* and *permission flag* are used interchangeably.

Example 1 To create a login class that allows the user to configure everything except telnet parameters:

1. Set the user's login class permission bit to **all**.

```
[edit system login]
user@host# set class all-except-telnet permissions all
```

2. Include the following **deny-configuration** statement.

```
[edit system login class all-except-telnet]
user@host# set deny-configuration "system services telnet"
```

Example 2 To create a login class that allows the user to configure everything except anything within any login class whose name begins with "m":

1. Set the user's login class permission bit to **all**.

```
[edit system login]
user@host# set class all-except-login-class-m permissions all
```

2. Include the following **deny-configuration** statement.

```
[edit system login class all-except-login-class-m]
user@host# set deny-configuration "system login class m.*"
```

Example 3 This next example shows the creation of a login class with the **all** permission bit that prevents the user from editing a configuration or issuing commands (such as **commit**) at the **[edit system login class]** or **[edit system services]** hierarchy levels:

To create a login class that allows the user to configure everything except at the **[edit system login class]** or **[edit system services]** hierarchy levels:

1. Set the user's login class permission bit to **all**.

```
[edit system login]
user@host# set class all-except-login-class-or-system-services permissions all
```

2. Include the following **deny-configuration** statement.

```
[edit system login class all-except-login-class-or-system-services]
user@host# set deny-configuration "(system login class) | (system services)"
```

The next two examples show how to use the **allow-configuration** and **deny-configuration** statements to determine permissions inverse to each other for the **[edit system services]** hierarchy level.

Example 4 To create a login class that allows the user to have full configuration privileges at the **[edit system services]** hierarchy level and at only the **[edit system services]** hierarchy level:

1. Set the user's login class permission bit to **configure**.

```
[edit system login]
user@host# set class configure-only-system-services permissions configure
```

2. Include the following **allow-configuration** statement.

```
[edit system login class configure-only-system-services]
user@host# set allow-configuration "system services"
```

Example 5 To create a login class that allows the user full permissions for all configuration mode hierarchies except the **[edit system services]** hierarchy level:

1. Set the user's login class permission bit to **all**.

```
[edit system login]
user@host# set class all-except-system-services permissions all
```

2. Include the following **deny-configuration** statement.

```
[edit system login class all-except-system-services]
user@host# set deny-configuration "system services"
```

Example: Using Additive Logic With Regular Expressions to Specify Access Privileges

This example shows how to use additive logic when using regular expressions to set up configuration access privileges.

Requirements

This example uses the following hardware and software components:

- One Juniper Networks J Series, M Series, MX Series, or T Series device
- Junos OS Release 16.1 or later
  - There must be at least one user assigned to a login class.
  - There can be more than one login class, each with varying permission configurations, and more than one user on the device.

Overview

To control who can make configuration changes to the system, and what specifically they can change, you can create regular expressions that indicate specific portions of the configuration hierarchy that users in a named user class are permitted to access. For example, you can create regular expressions that specify a group of routing instances that users are allowed to modify, and prevent the users from making changes to any other routing instances, or to any other configuration level.

You configure regular expressions using the **allow-configuration-regexps** and **deny-configuration-regexps** statements. By default, **deny-configuration-regexps** statements take precedence over **allow-configuration-regexps** statements for users in the named user class to which they are applied.

If a configuration hierarchy appears in a **deny-configuration-regexps** statement for a named user class, it is not visible to the users, regardless of the contents of the **allow-configuration-regexps** statement. If a configuration hierarchy does not appear in a **deny-configuration-regexps** statement, it is visible if it appears in an

allow-configuration-regexps statement, or if there is no **allow-configuration-regexps** statement configured for the user class..

You can optionally change this default behavior so additive logic (that is, deny all by default / allow some as specified) is used in regular expressions. When additive logic is enabled, the behavior of existing regular expressions changes so that all configuration hierarchies are denied unless they are included in an **allow-configuration-regexps** statement for the named user class.

Configuration

To enable additive logic for regular expressions:

1. To explicitly allow one or more individual configuration mode hierarchies, include the **allow-configuration-regexps** statement at the **[edit system login class *class-name*]** hierarchy level, configured with the regular expressions to be allowed.

   ```
   [edit system login class class-name]
   user@host# set allow-configuration-regexps "regular expression 1" "regular expression
     2" "regular expression 3" "regular expression 4" ...
   ```

2. Assign the login class to one or more users.

   ```
   [edit system login]
   user@host# set user username class class-name
   ```

3. Enable additive logic for regular expressions.

   ```
   [edit system]
   user@host# set regex-additive-logic
   ```

4. Commit your changes.

   Users assigned this login class have access to the configuration hierarchies included in the **allow-configuration-regexps** statement, but no others.

Examples

Using Regular Expressions with Additive Logic

Purpose This section provides examples of regular expressions that use additive logic to give you ideas for creating configurations appropriate for your system.

Allow Specific Routing Instances The following example login class includes a regular expression that allows configuration of routing instances whose names start with **CUST-VRF-**; for example, **CUST-VRF-1**, **CUST-VRF-25**, **CUST-VRF-100**, and so on:

```
[edit system login class class-name]
user@host# set permissions configure view view-configuration
user@host# set allow-configuration-regexps "routing-instances CUST-VRF-.* .*"
```

If the following statement is included in the configuration, it prevents the user from configuring any other routing instances and denies access to any non-routing instance configuration hierarchy:

```
[edit system]
user@host# set regex-additive-logic
```

Allow BGP Peer Configuration Only

The following example login class includes a regular expression that allows configuration of BGP peers:

```
[edit system login class class-name]
user@host# set permissions configure view view-configuration
user@host# set allow-configuration-regexps "protocols bgp group *"
```

If the following statement is included in the configuration, it prevents the user from making any other changes, such as deleting or disabling BGP statements:

```
[edit system]
user@host# set regex-additive-logic
```

Verification

To verify that you have set the access privileges correctly:

1. Configure a login class and commit the changes.
2. Assign the login class to a *username*.
3. Log in as the *username* assigned with the new login class.
4. Attempt to perform the configurations that have been allowed.
   - You should be able to perform configuration changes to hierarchy levels and regular expressions that have been allowed.
   - All other hierarchies should not be visible.
   - Any allowed or denied expressions should take precedence over any permissions granted with the **permissions** statement.

Example: Configuring User Permissions with Access Privileges for Operational Mode Commands

This example shows how to configure custom login classes and assign access privileges for operational mode commands. This enables users of the customized login class to execute only those operational commands for which access privileges have been specified. This prevents unauthorized users from executing sensitive commands that could potentially cause damage to the network.

- Requirements on page 113
- Overview and Topology on page 113

Requirements

This example uses the following hardware and software components:

- One Juniper Networks device
- One TACACS+ (or RADIUS) server
- Junos OS build running on the Juniper Networks device

Before you begin:

- Establish a TCP connection between the device and the TACACS+ server. In the case of the RADIUS server, establish a UDP connection between the device and the RADIUS server.

  For information on configuring a TACACS+ server, see "Configuring TACACS+ Authentication" on page 207.

- Configure at least one user assigned to a login class on the Juniper Networks device. There can be more than one login class, each with varying permission configurations, and more than one user on the device.

Overview and Topology

Each top-level command-line interface (CLI) command and each configuration statement in Junos OS has an access privilege level associated with it. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level. Users can execute only those commands and configure and view only those statements for which they have access privileges. To configure access privilege levels, include the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level.

The access privileges for each login class are defined by one or more permission flags specified in the **permissions** statement. In addition to this, you can specify extended regular expressions with the following statements:

- **allow-commands** and **deny-commands**—Allow or deny access to operational mode commands only.
- **allow-configuration** and **deny-configuration**—Allow or deny access to a particular configuration hierarchy only.
- **allow-configuration-regexps** and **deny-configuration-regexps**—Allow or deny access to a particular configuration hierarchy using strings of regular expressions.
- **allow-commands-regexps** and **deny-commands-regexps**—(TACACS+ authorization only) Allow or deny access to a particular command using strings of regular expressions.

The above statements define a user's access privileges to individual operational mode commands, configuration statements, and hierarchies. These statements take precedence over the login class permissions set for a user.

Configuration Notes

When configuring the **allow-commands**, **deny-commands**, **allow-configuration**, and **deny-configuration** statements with access privileges, take the following into consideration:

- You can include the allow/deny statement only once in each login class.
- If the exact same command is configured under both **allow-commands** and **deny-commands** statements, or both **allow-configuration** and **deny-configuration** statements, then the allow operation takes precedence over the deny statement.

  For instance, with the following configuration, a user assigned to login class test is allowed to install software using the **request system software add** command, although the **deny-commands** statement also includes it:

  ```
  [edit system login]
  user@host# set class test permissions allow-commands "request system software
    add"
  user@host# set class test permissions deny-commands "request system software add"
  ```

  For instance, with the following configuration, a user assigned to login class test is allowed to access the **[edit system services]** configuration hierarchy, although the **deny-configuration** statement also includes it:

  ```
  [edit system login]
  user@host# set class test permissions allow-configuration "system services"
  user@host# set class test permissions deny-configuration "system services"
  ```

- If you specify a regular expression for **allow-commands** and **deny-commands** statements with two different variants of a command, the longest match is always executed.

  For instance, for the following configuration, a user assigned to test login class is allowed to execute the **commit synchronize** command and not the **commit** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize**, and it is specified for **allow-commands**.

  ```
  [edit system login]
  user@host# set class test allow-commands "commit-synchronize"
  user@host# set class test deny-commands commit
  ```

- Regular expressions for **allow-commands** and **deny-commands** statements can also include the **commit**, **load**, **rollback**, **save**, **status**, and **update** commands.
- Explicitly allowing configuration mode hierarchies or regular expressions using the **allow-configuration** statement adds to the regular permissions set using the **permissions** statement. Likewise, explicitly denying configuration mode hierarchies or regular expressions using the **deny-configuration** statement removes permissions for the specified configuration mode hierarchy, from the default permissions provided by the **permissions** statement.

  For example, for the following configuration, the login class user can edit the configuration at the **[edit system services]** hierarchy level and issue configuration mode commands (such as **commit**), in addition to just entering the configuration mode using

the **configure** command, which is the permission specified by the configure permission flag:

```
[edit system login]
user@host# set class test permissions configure allow-configuration "system services"
```

Likewise, for the following configuration, the login class user can perform all operations allowed by the *all* permissions flag, except issuing configuration mode commands (such as **commit**) or modifying the configuration at the **[edit system services]** hierarchy level:

```
[edit system login]
user@host# set class test permissions all deny-configuration "system services"
```

- The **allow/deny-configuration** statements are mutually exclusive with the **allow/deny-configuration-regexps** statements, and the **allow-deny-commands** statements are mutually exclusive with the **allow/deny-commands-regexps** statements. For example, you cannot configure both **allow-configuration** and **allow-configuration-regexps** in the same login class.
- If you have existing configurations using the **allow/deny-configuration** or **allow/deny-commands** statements, using the same configuration options with the **allow/deny-configuration-regexps** or **allow/deny-commands-regexps** statements might not produce the same results, as the search and match methods differ in the two forms of these statements.
- To define access privileges to parts of the configuration hierarchy, specify the full paths in the extended regular expressions with the **allow-configuration** and **deny-configuration** statements. Use parentheses around an extended regular expression that connects two or more expressions with the pipe (|) symbol.

  For example:

  ```
  [edit system login]
  user@host# set class test deny-configuration "(system login class) | (system services)"
  ```

- If the regular expression contains any spaces, operators, or wildcard characters, enclose the expression in quotation marks. Regular expressions are not case-sensitive; for example, **allow-commands** ***"show interfaces"***.
- Modifiers such as *set*, *log*, and *count* are not supported within the regular expression string to be matched. If a modifier is used, then nothing is matched.

  Incorrect configuration:

  ```
  [edit system login]
  user@host# set class test permission deny-commands "set protocols"
  ```

  Correct configuration:

  ```
  [edit system login]
  user@host# set class test permission deny-commands protocols
  ```

- Anchors are required when specifying complex regular expressions with the **allow-commands** statement.

  For example:

  ```
  [edit system login]
  user@host# set class test permissions allow-commands "(^monitor) | (^ping) | (^show)
    | (^exit)"


          OR
  set class test permissions allow-commands "allow-commands ="^(monitor | ping |
    show | exit)"
  ```

- When specifying extended regular expressions using the **allow/deny-commands** and **allow/deny-configuration** statements, each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses ( ). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.

  For example:

  ```
  [edit system login]
  user@host# set class test allow-commands "(ping .*)|(traceroute .*)|(show
    .*)|(configure .*)|(edit)|(exit)|(commit)|(rollback .*)"
  user@host# set class test deny-configuration "(system login class)|(system services)"
  ```

- When specifying extended regular expressions using the **allow/deny-configuration-regexps** or **allow/deny-commands-regexps** statement, each expression enclosed within quotes (") and separated by a space must be enclosed in angular brackets [ ].

  For example:

  ```
  [edit system login]
  user@host# set class test allow-configuration-regexps [ "interfaces .* description .*"
    “interfaces .* unit .* description .*” “interfaces .* unit .* family inet address .*”
    “interfaces.* disable" ]
  ```

- You can use the * wildcard character when denoting regular expressions. However, it must be used as a portion of a regular expression. You cannot use *[*]* or *[.*]* alone.
- You cannot configure the **allow-configuration** statement with the *(interfaces (description (|.*))* regular expression, as this evaluates to **allow-configuration = .*** regular expression.
- You can configure as many regular expressions as needed to be allowed or denied. Regular expressions to be denied take precedence over configurations to be allowed.

Topology

Figure 1: Configuring TACACS+ Server Authentication

Figure 1 on page 117 illustrates a simple topology, where Router R1 is a Juniper Networks device and has a TCP connection established with a TACACS+ server.

In this example, R1 is configured with three customized login classes—Class1, Class2, and Class3—for specifying access privileges with extended regular expressions using the **allow-commands** and **deny-commands** statements differently.

The purpose of each login class is as follows:

- **Class1**—Defines access privileges for the user with the **allow-commands** statement only. This login class provides operator-level user permissions, and should provide authorization for only rebooting the device.
- **Class2**—Defines access privileges for the user with the **deny-commands** statement only. This login class provides operator-level user permissions, and should deny access to **set** commands.
- **Class3**—Defines access privileges for the user with both the **allow-commands** and **deny-commands** statements. This login class provides superuser-level user permissions, and should provide authorization for accessing interfaces and viewing device information. It should also deny access to **edit** and **configure** commands.

Router R1 has three different users, User1, User2, and User3, assigned to Class1, Class2, and Class3 login classes, respectively.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

R1

```
set system authentication-order tacplus
set system authentication-order radius
set system authentication-order password
set system radius-server 10.209.1.66 secret "$ABC123"
set system tacplus-server 10.209.1.66
set system radius-options enhanced-accounting
set system tacplus-options enhanced-accounting
set system accounting events login
set system accounting events change-log
set system accounting events interactive-commands
set system accounting traceoptions file auditlog
```

```
set system accounting traceoptions flag all
set system accounting destination tacplus server 10.209.1.66
set system login class Class1 permissions clear
set system login class Class1 permissions network
set system login class Class1 permissions reset
set system login class Class1 permissions trace
set system login class Class1 permissions view
set system login class Class1 allow-commands "request system reboot"
set system login class Class2 permissions clear
set system login class Class2 permissions network
set system login class Class2 permissions reset
set system login class Class2 permissions trace
set system login class Class2 permissions view
set system login class Class2 deny-commands set
set system login class Class3 permissions all
set system login class Class3 allow-commands configure
set system login class Class3 deny-commands .*
set system login user User1 uid 2001
set system login user User1 class Class1
set system login user User1 authentication encrypted-password "$ABC123"
set system login user User2 uid 2002
set system login user User2 class Class2
set system login user User2 authentication encrypted-password "$ABC123"
set system login user User3 uid 2003
set system login user User3 class Class3
set system login user User3 authentication encrypted-password "$ABC123"
set system syslog file messages any any
```

Configuring Authentication Parameters for Router R1

Step-by-Step Procedure

The following example requires that you navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Router R1 authentication:

1. Configure the order in which authentication should take place for R1. In this example, TACACS+ server authentication is first, followed by RADIUS server authentication, and then the local password.

   ```
   [edit system]
   user@R1# set authentication-order tacplus
   user@R1# set authentication-order radius
   user@R1# set authentication-order password
   ```

2. Establish R1 connection with the TACACS+ server.

   ```
   [edit system]
   user@R1# set tacplus-server 10.209.1.66
   user@R1# set tacplus-options enhanced-accounting
   user@R1# set accounting destination tacplus server 10.209.1.66
   ```

3. Configure RADIUS server authentication parameters.

```
[edit system]
user@R1# set radius-server 10.209.1.66 secret "$ABC123"
user@R1# set radius-options enhanced-accounting
```

4. Configure R1 accounting configuration parameters.

```
[edit system]
user@R1# set accounting events login
user@R1# set accounting events change-log
user@R1# set accounting events interactive-commands
user@R1# set accounting traceoptions file auditlog
user@R1# set accounting traceoptions flag all
```

Configuring Access Privileges with allow-commands Statement Only (Class1)

Step-by-Step Procedure

To specify regular expressions using the **allow-commands** statement only:

1. Configure Class1 custom login class and assign operator-level user permissions. For information on the predefined system login classes, see the "Junos OS Login Classes Overview" on page 49.

```
[edit system login]
user@R1# set class Class1 permissions clear
user@R1t# set class Class1 permissions network
user@R1# set class Class1 permissions reset
user@R1# set class Class1 permissions trace
user@R1# set class Class1 permissions view
```

2. Specify the command to enable rebooting of R1 in the **allow-commands** statement.

```
[edit system login]
user@R1# set class Class1 allow-commands "request system reboot"
```

3. Configure the user account for the Class1 login class.

```
[edit system login]
user@R1# set user User1 uid 2001
user@R1# set user User1 class Class1
user@R1# set user User1 authentication encrypted-password "$ABC123"
```

Configuring Access Privileges with deny-commands Statement Only (Class2)

Step-by-Step Procedure

To specify regular expressions using the **deny-commands** statement only:

1. Configure the Class2 custom login class and assign operator-level user permissions. For information on the predefined system login classes, see the "Junos OS Login Classes Overview" on page 49.

```
[edit system login]
user@R1# set class Class1 permissions clear
user@R1# set class Class1 permissions network
user@R1# set class Class1 permissions reset
user@R1# set class Class1 permissions trace
user@R1# set class Class1 permissions view
```

2. Disable execution of any set commands in the **deny-commands** statement.

```
[edit system login]
user@R1# set class Class1 deny-commands "set"
```

3. Configure the user account for the Class2 login class.

```
user@R1# set login user User2 uid 2002
user@R1# set login user User2 class Class2
user@R1# set login user User2 authentication encrypted-password "$ABC123"
```

Configuring Access Privileges with Both allow-commands and deny-commands Statements (Class3)

Step-by-Step Procedure

To specify regular expressions using both the **allow-commands** and **deny-commands** statements:

1. Configure the Class3 custom login class and assign superuser-level user permissions. For information on the predefined system login classes, see the "Junos OS Login Classes Overview" on page 49.

```
[edit system login]
user@R1# set class Class3 permissions all
```

2. Specify the commands to enable only configure commands in the **allow-commands** statement.

```
[edit system login]
user@R1# set class Class3 allow-commands configure
```

3. Disable execution of all commands in the **deny-commands** statement.

```
[edit system login]
user@R1# set class Class3 deny-commands .*
```

4. Configure the user account for the Class1 login class.

```
[edit system login]
user@R1# set login user User3 uid 2003
user@R1# set login user User3 class Class3
user@R1# set login user User3 authentication encrypted-password "$ABC123"
```

Results

From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@R1# show system
authentication-order [ tacplus radius password ];
radius-server {
   10.209.1.66 secret "$ABC123";
}
tacplus-server {
   10.209.1.66;
}
radius-options {
   enhanced-accounting;
}
tacplus-options {
   enhanced-accounting;
}
accounting {
   events [ login change-log interactive-commands ];
   traceoptions {
      file auditlog;
      flag all;
   }
   destination {
      tacplus {
         server {
            10.209.1.66;
         }
      }
   }
}
login {
   class Class1 {
      permissions [ clear network reset trace view ];
      allow-commands "request system reboot";
   }
   class Class2 {
      permissions [ clear network reset trace view ];
```

```
        deny-commands set;
    }
    class Class3 {
        permissions all;
        allow-commands configure;
        deny-commands .*;
    }
    user User1 {
        uid 2001;
        class Class1;
        authentication {
            encrypted-password "$ABC123";
        }
    }
    user User2 {
        uid 2002;
        class Class2;
        authentication {
            encrypted-password "$ABC123";
        }
    }
    user User3 {
        uid 2003;
        class Class3;
        authentication {
            encrypted-password “$ABC123”;
        }
    }
}
syslog {
    file messages {
        any any;
    }
}
```

Verification

Log in as the username assigned with the new login class, and confirm that the configuration is working properly.

- Verifying Class1 Configuration on page 122
- Verifying Class2 Configuration on page 123
- Verifying Class3 Configuration on page 124

Verifying Class1 Configuration

Purpose Verify that the permissions and commands allowed in the Class1 login class are working.

Action From operational mode, run the **show system users** command.

```
User1@R1> show system users
12:39PM  up 6 days, 23 mins, 6 users, load averages: 0.00, 0.01, 0.00
USER     TTY      FROM                              LOGIN@  IDLE WHAT
User1  p0       abc.example.net 12:34AM 12:04 cli
User2  p1       abc.example.net 12:36AM 12:02 -cli (cli)
User3  p2       abc.example.net 10:41AM    11 -cli (cli)
```

From operational mode, run the **request system reboot** command.

```
User1@R1> request system ?
Possible completions:
  reboot               Reboot the system
```

Meaning The Class1 login class to which User1 is assigned has the operator-level user permissions, and is allowed to execute the **request system reboot** command.

The predefined operator login class has the following permission flags specified:

- **clear**—Can clear (delete) information learned from the network that is stored in various network databases by using the **clear** commands.
- **network**—Can access the network by using the **ping**, **ssh**, **telnet**, and **traceroute** commands.
- **reset**—Can restart software processes by using the **restart** command and can configure whether software processes are enabled or disabled at the **[edit system processes]** hierarchy level.
- **trace**—Can view trace file settings and configure trace file properties.
- **view**—Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics. Cannot view the secret configuration.

For the Class1 login class, in addition to the above-mentioned user permissions, User1 can execute the **request system reboot** command. The first output displays the view permissions as an operator, and the second output shows that the only **request** command that User1 can execute as an operator is the **request system reboot** command.

Verifying Class2 Configuration

Purpose Verify that the permissions and commands allowed for the Class2 login class are working.

Action From the operational mode, run the **ping** command.

```
User2@R1> ping 10.209.1.66
```

```
ping 10.209.1.66
PING 10.209.1.66 (10.209.1.66): 56 data bytes
64 bytes from 10.209.1.66: icmp_seq=0 ttl=52 time=212.521 ms
64 bytes from 10.209.1.66: icmp_seq=1 ttl=52 time=212.844 ms
64 bytes from 10.209.1.66: icmp_seq=2 ttl=52 time=211.304 ms
64 bytes from 10.209.1.66: icmp_seq=3 ttl=52 time=210.963 ms
^C
--- 10.209.1.66 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 210.963/211.908/212.844/0.792 ms
```

From the CLI prompt, check the available permissions.

```
User2@R1> ?
```

```
Possible completions:
  clear                Clear information in the system
  file                 Perform file operations
  help                 Provide help information
  load                 Load information from file
  monitor              Show real-time debugging information
  mtrace               Trace multicast path from source to receiver
  op                   Invoke an operation script
  ping                 Ping remote target
  quit                 Exit the management session
  request              Make system-level requests
  restart              Restart software process
  save                 Save information to file
  show                 Show system information
  ssh                  Start secure shell on another host
  start                Start shell
  telnet               Telnet to another host
  test                 Perform diagnostic debugging
  traceroute           Trace route to remote host
```

From the CLI prompt, execute any set command.

```
User2@R1> set
```

```
            ^
unknown command.
```

Meaning The Class2 login class to which User2 is assigned has the operator-level user permissions, and is denied access to all **set** commands. This is displayed in the command outputs.

The permission flags specified for the predefined operator login class are the same as that of Class1.

Verifying Class3 Configuration

Purpose Verify that the permissions and commands allowed for the Class3 login class are working.

Action From the CLI prompt, check the available permissions.

```
User3@R1> ?
Possible completions:
  configure           Manipulate software configuration information
```

From the operational mode, enter configuration mode.

```
User3@R1> configure
Entering configuration mode

[edit]
User3@R1#
```

Meaning The Class3 login class to which User3 is assigned has the superuser (all) user permissions, but is allowed to execute the **configure** command only, and is denied access to all other operational mode commands. Because the regular expressions specified in the **allow/deny-commands** statements take precedence over the user permissions, User3 on R1 has access only to configuration mode, and is denied access to all other operational mode commands.

Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies

This example shows how to configure custom login classes and assign access privileges to portions of the configuration hierarchy. This enables users of the customized login class to execute only those configuration statements and hierarchies for which access privileges have been specified. This prevents unauthorized users from accessing device configurations that could potentially cause damage to the network.

Requirements

This example uses the following hardware and software components:

- One Juniper Networks device
- One TACACS+ (or RADIUS) server
- Junos OS build running on the Juniper Networks device

Before you begin:

- Establish a TCP connection between the device and the TACACS+ server. In the case of the RADIUS server, establish a UDP connection between the device and the RADIUS server.

  For information on configuring a TACACS+ server, see "Configuring TACACS+ Authentication" on page 207.

- Configure at least one user assigned to a login class on the Juniper Networks device. There can be more than one login class, each with varying permission configurations, and more than one user on the device.

Overview and Topology

Each top-level command-line interface (CLI) command and each configuration statement in Junos OS has an access privilege level associated with it. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level. Users can execute only those commands and configure and view only those statements for which they have access privileges. To configure access privilege levels, include the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level.

The access privileges for each login class are defined by one or more permission flags specified in the **permissions** statement. In addition to this, you can specify extended regular expressions with the following statements:

- **allow-commands** and **deny-commands**—Allow or deny access to operational mode commands.
- **allow-configuration** and **deny-configuration**—Allow or deny access to parts of the configuration hierarchy.

  These statements perform slower matching, with more flexibility, especially in wildcard matching. However, it can take a very long time to evaluate all of the possible statements if a great number of full-path regular expressions or wildcard expressions are configured, possibly impacting performance.

- **allow-configuration-regexps** and **deny-configuration-regexps**—Allow or deny access to a particular configuration hierarchy using strings of regular expressions. These statements are similar to **allow-configuration** and **deny-configuration** statements, except that in the **allow/deny-configuration-regexps** statements you can configure sets of strings in which the strings include spaces when using the first set of statements.

The above statements define a user's access privileges to individual operational mode commands, configuration statements, and hierarchies. These statements take precedence over a login class permissions bit set for a user.

Difference between allow/deny-configuration and allow/deny-configuration-regexps statements

The **allow-configuration** and **deny-configuration** statements were introduced before Junos OS Release 7.4. The **allow-configuration-regexps** and **deny-configuration-regexps**

statements were introduced in Junos OS Release 11.2. In Junos OS Release 11.4, the **allow-configuration** and **deny-configuration** statements were deprecated, but because these statements were useful in executing simple configurations, these statements were undeprecated in Junos OS Release 11.4R6, and starting with the 11.4R6 release, both the **allow/deny-configuration** and the **allow/deny-configuration-regexps** statements are supported.

The **allow/deny-configuration-regexps** statements split up the regular expression into tokens and match each piece against each part of the specified configuration's full path, whereas the **allow/deny-configuration** statements match against the full string. For **allow/deny-configuration-regexps** statements, you configure a set of strings in which each string is a regular expression, with spaces between the terms of the string. This provides very fast matching, but with less flexibility. For specifying wildcard expressions you must set up wildcards for each token of the space-delimited string you want to match, and this makes it more tedious to use wildcard expressions for these statements.

For example:

- This example shows that **options** is the only matched expression against the first token of the statement.

  ```
  [edit system]
  login {
    class test {
      permissions configure;
      allow-configuration-regexps .*options;
    }
  }
  ```

  The above configuration matches the following statements:

  - set policy-**options** condition *condition* dynamic-db
  - set routing-**options** static route *static-route* next-hop *next-hop*
  - set event-**options** generate-event *event* time-interval *seconds*

  The above configuration does not match the following statements:

  - system host-name host-**options**
  - interfaces *interface-name* description **options**

- This example shows that **ssh** is the only matched expression against the third token of the statement.

  ```
  [edit system]
  login {
    class test {
      permissions configure;
      allow-configuration-regexps ".* .* .*ssh";
    }
  }
  ```

  In the above example, the three tokens include **.***, **.***, and **.*ssh**, respectively.

The above configuration matches the following statements:

- system host-name hostname-**ssh**
- system services **ssh**
- system services outbound-**ssh**

The above configuration does not match the following statement:

- interfaces *interface-name* description **ssh**

You can restrict configuration access easily using the **deny-configuration** statement as compared to using the **deny-configuration-regexps** statement. Table 10 on page 128 illustrates the use of both the **deny-configuration** and **deny-configuration-regexps** statements in different configurations to achieve the same result of restricting access to a particular configuration.

Table 10: Restricting Configuration Access Using deny-configurtion and deny-configuration-regexps Statements

Configuration Denied	Using: deny-configuration	Using: deny-configuration-regexps	Result

xnm-ssl	[edit system]
	login {
	class test {
	permissions configure;
	allow-configuration .*;
	deny-configuration .*xnm-ssl;
	}
	}
		[edit system]
		login {
		class test {
		permissions configure;
		allow-configuration .*;
		deny-configuration-regexps ".* .*
		.*-ssl"";
		}
		}
			The following configuration statement is denied:
			• system services xnm-ssl

ssh	[edit system]
	login {
	class test {
	permissions configure;
	allow-configuration .*;
	deny-configuration ".*ssh";
	}
	}
		[edit system]
		login {
		class test {
		permissions configure;
		allow-configuration .*;
		deny-configuration-regexps ".*ssh";
		deny-configuration-regexps ".*
		.*ssh";
		deny-configuration-regexps ".* .*
		.*ssh";
		}
		}
			The following configuration statements are denied:
			• system host-name hostname-ssh
			• system services ssh
			• system services outbound-ssh
			• security ssh-known-host

Although the **allow/deny-configuration** statements are also useful when simple configuration is desired, the **allow/deny-configuration-regexps** statements provide better performance and overcome the ambiguity that existed when combining expressions set in the **allow/deny-configuration** statements.

NOTE: The **allow/deny-configuration** and **allow/deny-configuration-regexps** statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the **allow/deny-configuration** statement, or the **allow/deny-configuration-regexps** statement. If you have existing configurations using the **allow/deny-configuration** statements, using the same configuration options with the **allow/deny-configuration-regexps** statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

Configuration Notes

When configuring the **allow-configuration**, **deny-configuration**, **allow-configuration-regexps**, and **deny-configuration-regexps** statements with access privileges, take the following into consideration:

- You can include one **deny-configuration** and one **allow-configuration** statement in each login class.
- The **allow/deny-configuration** and **allow/deny-configuration-regexps** statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the **allow/deny-configuration** statement, or the **allow/deny-configuration-regexps** statement. If you have existing configurations using the **allow/deny-configuration** statements, using the same configuration options with the **allow/deny-configuration-regexps** statements might not produce the same results, as the search and match methods differ in the two forms of these statements.
- Explicitly allowing configuration mode hierarchies or regular expressions using the **allow-configuration** statement adds to the regular permissions set using the **permissions** statement. Likewise, explicitly denying configuration mode hierarchies or regular expressions using the **deny-configuration** statement removes permissions for the specified configuration mode hierarchy, from the default permissions provided by the **permissions** statement.

  For example, for the following configuration, the login class user can edit the configuration at the **[edit system services]** hierarchy level and issue configuration mode commands (such as **commit**), in addition to just entering the configuration mode using the **configure** command, which is the permission specified by the configure permission flag:

  ```
  [edit system login]
  user@host# set class test permissions configure allow-configuration "system services"
  ```

  Likewise, for the following configuration, the login class user can perform all operations allowed by the *all* permissions flag, except issuing configuration mode commands (such as **commit**) or modifying the configuration at the **[edit system services]** hierarchy level:

  ```
  [edit system login]
  user@host# set class test permissions all deny-configuration "system services"
  ```

- To define access privileges to parts of the configuration hierarchy, specify the full paths in the extended regular expressions with the **allow-configuration** and **deny-configuration** statements. Use parentheses around an extended regular expression that connects two or more expressions with the pipe (|) symbol.

  For example:

  ```
  [edit system login]
  user@host# set class test deny-configuration "(system login class)|(system services)"
  ```

- When specifying extended regular expressions using the **allow/deny-commands** and **allow/deny-configuration** statements, each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses ( ). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.

  For example:

  ```
  [edit system login]
  user@host# set class test allow-commands "(ping .*)|(traceroute .*)|(show
    .*)|(configure .*)|(edit)|(exit)|(commit)|(rollback .*)"
  user@host# set class test deny-configuration "(system login class)|(system services)"
  ```

- When specifying extended regular expressions using the **allow-deny-configuration-regexps** statement, each expression enclosed within quotes (") and separated by a space must be enclosed in angular brackets [ ].

  For example:

  ```
  [edit system login]
  user@host# set class test allow-configuration-regexps [ "interfaces .* description .*"
    “interfaces .* unit .* description .*” “interfaces .* unit .* family inet address .*”
    “interfaces.* disable" ]
  ```

- If the exact same command is configured under both **allow-configuration** and **deny-configuration** statements, then the allow operation takes precedence over the deny statement.

  For instance, with the following configuration, a user assigned to login class test is allowed to access the **[edit system services]** configuration hierarchy, although the **deny-configuration** statement also includes it:

  ```
  [edit system login]
  user@host# set class test permissions allow-configuration "system services"
  user@host# set class test permissions deny-configuration "system services"
  ```

  For instance, if a certain command or configuration is allowed, for example, using permission *all*, then we can use the **deny-configuration** command to deny access to a particular hierarchy.

- Modifiers such as *set*, *log*, and *count* are not supported within the regular expression string to be matched. If a modifier is used, then nothing is matched.

Incorrect configuration:

```
[edit system login]
user@host# set class test permission deny-configuration "set protocols"
```

Correct configuration:

```
[edit system login]
user@host# set class test permission deny-configuration protocols
```

- You can use the * wildcard character when denoting regular expressions. However, it must be used as a portion of a regular expression. You cannot use *[*]* or *[.*]* alone.
- You cannot configure the **allow-configuration** statement with the *(interfaces (description (|.*))* regular expression, as this evaluates to **allow-configuration = .*** regular expression.
- You can configure as many regular expressions as needed to be allowed or denied. Regular expressions to be denied take precedence over configurations to be allowed.

Topology

Figure 2: Configuring TACACS+ Server Authentication

Figure 2 on page 131 illustrates a simple topology, where Router R1 is a Juniper Networks device and has a TCP connection established with a TACACS+ server.

In this example, R1 is configured with two customized login classes—Class1 and Class2—for specifying access privileges with extended regular expressions using the **allow-configuration**, **deny-configuration**, **allow-configuration-regexps**, and **deny-configuration-regexps** statements differently.

The purpose of the login classes is as follows:

- **Class1**—Define access privileges for the user with the **allow-configuration** and **deny-configuration** statements. This login class should provide access to configure interfaces hierarchy only, and deny all other access on the device. To do this, the user permissions should include *configure* to provide configuration access. In addition to this, the **allow-configuration** statement should allow interfaces configuration, and the **deny-configuration** statement should deny access to all other configurations. Because the allow statement takes precedence over the deny statement, the users assigned to the Class1 login class can access only the **[edit interfaces]** hierarchy level.
- **Class2**—Define access privileges for the user with the **allow-configuration-regexps** and **deny-configuration-regexps** statements. This login class provides superuser-level user permissions, and in addition, explicitly allows configuration under multiple hierarchy levels for interfaces. It also denies configuration access to the **[edit system]** and **[edit protocols]** hierarchy levels.

Router R1 has two users, User1 and User2, assigned to the Class1 and Class2 login classes, respectively.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

R1

```
set system authentication-order tacplus
set system authentication-order radius
set system authentication-order password
set system radius-server 10.209.1.66 secret "$ABC123"
set system tacplus-server 10.209.1.66
set system radius-options enhanced-accounting
set system tacplus-options enhanced-accounting
set system accounting events login
set system accounting events change-log
set system accounting events interactive-commands
set system accounting traceoptions file auditlog
set system accounting traceoptions flag all
set system accounting destination tacplus server 10.209.1.66
set system login class Class1 permissions configure
set system login class Class1 allow-configuration "interfaces .* unit .*"
set system login class Class1 deny-configuration .*
set system login class Class2 permissions all
set system login class Class2 allow-configuration-regexps [ "interfaces .* description .*"
   "interfaces .* unit .* description .*" "interfaces .* unit .* family inet address .*"
   "interfaces.* disable" ]
set system login class Class2 deny-configuration-regexps [ "system" "protocols" ]
set system login user User1 uid 2004
set system login user User1 class Class1
set system login user User1 authentication encrypted-password "$ABC123"
set system login user User2 uid 2006
set system login user User2 class Class2
set system login user User2 authentication encrypted-password "$ABC123"
set system syslog file messages any any
```

Configuring Authentication Parameters for Router R1

Step-by-Step Procedure

The following example requires that you navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Router R1 authentication:

1. Configure the order in which authentication should take place for R1. In this example, TACACS+ server authentication is first, followed by RADIUS server authentication, then the local password.

   ```
   [edit system]
   user@R1# set authentication-order tacplus
   ```

```
user@R1# set authentication-order radius
user@R1# set authentication-order password
```

2. Establish R1 connection with the TACACS+ server.

```
[edit system]
user@R1# set tacplus-server 10.209.1.66
user@R1# set tacplus-options enhanced-accounting
user@R1# set accounting destination tacplus server 10.209.1.66
```

3. Configure RADIUS server authentication parameters.

```
[edit system]
user@R1# set radius-server 10.209.1.66 secret "$ABC123"
user@R1# set radius-options enhanced-accounting
```

4. Configure the R1 accounting configuration parameters.

```
[edit system]
user@R1# set accounting events login
user@R1# set accounting events change-log
user@R1# set accounting events interactive-commands
user@R1# set accounting traceoptions file auditlog
user@R1# set accounting traceoptions flag all
```

Configuring Access Privileges with allow-configuration and deny-configuration Statements (Class1)

Step-by-Step Procedure

To specify regular expressions using the **allow-configuration** and **deny-configuration** statements:

1. Configure the Class1 custom login class and assign configuration user permissions.

```
[edit system login]
user@R1# set class Class1 permissions configure
```

2. Specify the regular expression in the **allow-configuration** statement to allow configuration at the **[edit interfaces]** hierarchy level. To allow **set** commands at the **[edit interfaces]** hierarchy level, the regular expression used is ***interfaces .* unit .****.

```
[edit system login]
user@R1# set class Class1 allow-configuration "interfaces .* unit .*"
```

3. Specify the regular expression in the **deny-configuration** statement to disable all configuration access. The regular expression used to deny all configuration access is **.***.

```
[edit system login]
user@R1# set class Class1 deny-configuration .*
```

4. Configure the user account for the Class1 login class.

```
[edit system login]
user@R1# set system login user User1 uid 2004
user@R1# set system login user User1 class Class1
user@R1# set system login user User1 authentication encrypted-password "$ABC123"
```

Configuring Access Privileges with allow-configuration-regexps and deny-configuration-regexps Statements (Class2)

Step-by-Step Procedure

To specify regular expressions using the **allow-configuration-regexps** and **deny-configuration-regexps** statements:

1. Configure the Class2 custom login class and assign superuser (all) user permissions. For information on the predefined system login classes, see "Junos OS Login Classes Overview" on page 49.

```
[edit system login]
user@R1# set class Class2 permissions all
```

2. Specify the regular expression to allow access to multiple hierarchies under the **[edit interfaces]** hierarchy level.

```
[edit system login]
user@R1# set class Class2 allow-configuration-regexps [ "interfaces .* description
  .*" "interfaces .* unit .* description .*" "interfaces .* unit .* family inet address .*"
  "interfaces.* disable" ]
```

3. Specify the regular expression to deny configuration at the **[edit system]** and **[edit protocols]** hierarchy levels.

```
[edit system login]
user@R1# set class Class2 deny-configuration-regexps [ "system" "protocols" ]
```

4. Configure the user account for the Class2 login class.

```
[edit system login]
user@R1# set system login user User2 uid 2006
user@R1# set system login user User2 class Class2
user@R1# set system login user User2 authentication encrypted-password "$ABC123"
```

Results

From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@R1# show system
authentication-order [ tacplus radius password ];
radius-server {
   10.209.1.66 secret "$ABC123";
}
tacplus-server {
   10.209.1.66;
}
radius-options {
   enhanced-accounting;
}
tacplus-options {
   enhanced-accounting;
}
accounting {
   events [ login change-log interactive-commands ];
   traceoptions {
      file auditlog;
      flag all;
   }
   destination {
      tacplus {
         server {
            10.209.1.66;
         }
      }
   }
}
login {
   class Class1 {
      permissions configure;
      allow-configuration "interfaces .* unit .*";
      deny-configuration .*;
   }
   class Class2 {
      permissions all;
      allow-configuration-regexps [ "interfaces .* description .*" "interfaces .* unit .*
         description .*" "interfaces .* unit .* family inet address .*" "interfaces.* disable" ];
      deny-configuration-regexps [ "system" "protocols" ];
   }
   user User1 {
      uid 2001;
      class Class1;
      authentication {
         encrypted-password "$ABC123";
      }
   }
   user User2 {
```

```
      uid 2002;
      class Class2;
      authentication {
         encrypted-password "$ABC123";
      }
   }
}
syslog {
   file messages {
      any any;
   }
}
```

Verification

Log in as the username assigned with the new login class, and confirm that the configuration is working properly.

- Verifying Class1 Configuration on page 136
- Verifying Class2 Configuration on page 137

Verifying Class1 Configuration

Purpose Verify that the permissions allowed in the Class1 login class are working.

Action From the CLI prompt, check the available permissions.

```
User1@R1> ?
Possible completions:
  clear               Clear information in the system
  configure           Manipulate software configuration information
  file                Perform file operations
  help                Provide help information
  load                Load information from file
  op                  Invoke an operation script
  quit                Exit the management session
  request             Make system-level requests
  save                Save information to file
  set                 Set CLI properties, date/time, craft interface message
  start               Start shell
  test                Perform diagnostic debugging
```

From the configuration mode, check the available configuration permissions.

```
User1@R1# edit ?
Possible completions:
> interfaces          Interface configuration
```

Meaning User1 has *configure* user permissions seen in the first output, and the only configuration access allowed for User1 is at the interfaces hierarchy level. All other configuration is denied, as seen in the second output.

Verifying Class2 Configuration

Purpose Verify that the Class2 configuration is working.

Action From the configuration mode, access the interfaces configuration.

```
[edit interfaces]
User2@R1# set ?
  Possible completions:
     <interface-name> Interface name
  + apply-groups         Groups from which to inherit configuration data
  + apply-groups-except  Don't inherit configuration data from these groups
    ge-0/0/3             Interface name
  > interface-range      Interface ranges configuration
  > interface-set        Logical interface set configuration
  > traceoptions         Interface trace options
```

From the configuration mode, access the system and protocols configuration hierarchies.

```
User2@R1# edit system
              ^
Syntax error, expecting <statement> or <identifier>.
```

```
User2@R1# edit protocols
                ^
Syntax error, expecting <statement> or <identifier>.
```

Meaning User2 has permissions to configure interfaces of R1, but the **[edit system]** and **[edit protocols]** hierarchy levels are denied access, as seen in the output.

See Also
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 99

Related Documentation
- Junos OS Login Classes Overview on page 49
- Junos OS User Accounts on page 67

CHAPTER 3

Passwords for User Access

Root Password

When the router, switch, or security device is powered on first time, it is ready to be configured. Initially, you log in as the user **root** with no password. Later, you must configure a plain-text password for the root-level user (whose username is *root*). Configuring a plain-text password is one way to protect access to the root level by unauthorized users. If you forget the root password for the router, you can use the password recovery procedure to reset the root password. Read this topic for more information.

Configuring the Root Password

The Junos OS is preinstalled on the router or switch. When the router or switch is powered on, it is ready to be configured. Initially, you log in as the user **root** with no password. The root directory of a UNIX device is the entry point to all other folders and files on that device. As a result, access to the root directory is restricted by default to a predefined user account known as the *root user*. The root user (also referred to as *superuser*) has unrestricted access and full permissions within the system. The expression "log in as root" is commonly used when an action requires the user to log into the device as the root user.

NOTE: If you configure a blank password using the **encrypted-password** statement at the **[edit system root-authentication]** hierarchy level for root authentication, you can commit a configuration but you *cannot* log in as the root user and gain root level access to the router or switch.

After you log in, you should configure the root (superuser) password by including the **root-authentication** statement at the **[edit system]** hierarchy level and configuring one of the password options:

```
[edit system]
root-authentication {
   (encrypted-password "password"| plain-text-password);
   load-key-file URL filename;
   ssh-dsa "public-key" <from hostname>;
   ssh-ecdsa "public-key" <from hostname>;
   ssh-rsa "public-key" <from hostname>;
}
```

If you configure the **plain-text-password** option, you are prompted to enter and confirm the password:

```
[edit system]
user@host# set root-authentication plain-text-password
New password: type password here
Retype new password: retype password here
```

The default requirements for plain-text passwords are:

- The password must be between 6 and 128 characters long
  - You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
  - Valid passwords must contain at least one uppercase letter or one lowercase letter, or one character class.

You can use the **load-key-file** *URL filename* statement to load an SSH key file that was previously generated using **ssh-keygen**. The *URL filename* is the path to the file's location

and name. When using this option, the contents of the key file are copied into the configuration immediately after entering the **load-key-file** *URL* statement. This command loads RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys.

Starting in Junos OS Release 18.3R1, the **ssh-dss** and **ssh-dsa** hostkey algorithms are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Optionally, you can use the **ssh-dsa**, **ssh-ecdsa**, or **ssh-rsa** statements to directly configure SSH RSA, DSA, or ECDSA keys to authenticate root logins. You can configure more than one public key for SSH authentication of root logins as well as for user accounts. When a user logs in as root, the public keys are referenced to determine whether the private key matches any of them.

```
[edit system]
user@host# set root-authentication load-key-file my-host:.ssh/id_dsa.pub
.file.19692 | 0 KB | 0.3 kB/s | ETA: 00:00:00 | 100%
[edit system]
```

From configuration mode, you can confirm your SSH key entries by entering the **show** command. It should look something like this:

```
[edit system]
user@hos# show
root-authentication {
   ssh-rsa "$ABC123"; #
      SECRET-DATA
}
```

Junos-FIPS software has special password requirements. FIPS passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If Junos-FIPS is installed on the router or switch, you cannot configure passwords unless they meet this standard.

If you use the **encrypted-password** option, then a null-password (empty) is not permitted. You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

See Also

- *Protecting Network Security by Configuring the Root Password*
- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 153

Example: Configuring a Plain-Text Password for Root Logins

This example shows how to configure a plain-text password for the root-level user (whose username is *root*). Configuring a plain-text password is one way to protect access to the

root level by unauthorized users. You must prevent unauthorized users from gaining access to superuser commands that can be used to alter your system configuration.

Requirements

No special configuration beyond device initialization is required before configuring this example.

Make sure that you understand the requirements for a valid plain-text password. For Junos OS, the default requirements for a plain-text password are as follows:

- Must be from 6 up to 128 characters long.
- Can include most character classes (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
- Must contain at least one change of case or character class.

Overview

Junos OS is preinstalled on the router. When the router is powered on, it is ready to be configured. Initially, you log in as the root-level user with no password. To set the root password, you have several options. This example shows how to enter a plain-text password that Junos OS then encrypts for you.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following command and paste it into the window. When prompted, type the new password, and then when prompted, retype it.

```
set system root-authentication plain-text-password
```

Configuring a Plain-Text Password for User Root

Step-by-Step Procedure

To configure a plain-text password for the root-level user:

1. Type the **set** command for the plain-text password and press Enter.

   ```
   [edit]
   user@host# set system root-authentication plain-text-password
   New password:
   ```

2. Type the new password next to the **New password** prompt and press Enter.

   ```
   New password: new-password
   ```

```
Retype new password:
```

3. Retype the same password next to the **Retype new password** prompt and press Enter.

Results

From configuration mode, confirm your configuration by using the **show** command. It should look something like this:

```
[edit ]
user@host# show system
root-authentication {
   encrypted-password "$ABC123"; ## SECRET-DATA
}
```

If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

After you have confirmed that the configuration is correct, enter **commit** from configuration mode.

Verification

Verifying the Configuration of a Plain-Text Password for User Root

Purpose Verify the configuration of a plain-text password for the root-level user.

Action From operational mode, confirm your configuration by entering the **show configuration system** command.

```
user@host> show configuration system
root-authentication {
   encrypted-password "$ABC123"; ## SECRET-DATA
}
```

Meaning If you use a clear-text password, Junos OS displays the password as an encrypted string so that users viewing the configuration cannot see the unencrypted password. That is, as you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password as in some other systems. Plain-text passwords are hidden and marked as ## SECRET-DATA in the configuration.

See Also

- root-authentication on page 1434
- Changing the Requirements for Junos OS Plain-Text Passwords on page 152

Example: Configuring SSH Authentication for Root Logins

The following example shows how to configure two public DSA keys for SSH authentication of root logins:

```
[edit system]
root-authentication {
   encrypted-password "$ABC123";
   ## SECRET-DATA;
   ssh-dsa "2354 95 9304@user.device";
   ssh-dsa "0483 02 8362@user.device";
}
```

Release History Table

Release	Description
18.3R1	Starting in Junos OS Release 18.3R1, the **ssh-dss** and **ssh-dsa** hostkey algorithms are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Related Documentation

- *Protecting Network Security by Configuring the Root Password*
- Plain-Text Passwords on page 152
- *Release Information for Junos OS with Upgraded FreeBSD*

Recovering Root Password

If you forget the root password for a device running Junos OS, you can use the password recovery procedure to reset the root password. Read this topic to understand how to recover root password.

- Recovering the Root Password on page 144
- Recovering the Root Password on Junos OS with Upgraded FreeBSD on page 147
- Troubleshooting Loss of the Root Password on page 149

Recovering the Root Password

If you forget the root password for the router, you can use the password recovery procedure to reset the root password.

Before you begin, note the following:

- You need console access to recover the root password.
- This password recovery procedure does not apply to devices running Junos OS with Upgraded FreeBSD. See "Recovering the Root Password on Junos OS with Upgraded FreeBSD" on page 147. For the list of Junos OS devices with upgraded FreeBSD, see Junos kernel upgrade to FreeBSD 10+.

- For MX80 Series routers, try this procedure first, but if it does not work you can manually delete the root-authentication settings from the Junos configuration file and reset the password, as explained here: *Recovering the Root Password for MX80*

Video: Recovering the Root Password

To recover the root password:

1. Power off the router by pressing the power button on the front panel.
2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with the router into the RJ-45–to–DB-9 serial port adapter supplied with the router.
4. Plug the RJ-45–to–DB-9 serial port adapter into the serial port on the management device.
5. Connect the other end of the Ethernet rollover cable to the console port on the router.
6. Turn on the power to the management device.
7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).
8. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
9. Power on the router by pressing the power button on the front panel.

   Verify that the POWER LED on the front panel turns green.

   The terminal emulation screen on your management device displays the router's boot sequence.
10. When the following prompt appears, press the Spacebar to access the router's bootstrap loader command prompt:

Depending on your device hardware, the bootstrap loader might proceed quite quickly at this step without pausing for input. Therefore, you might need to press the spacebar multiple times at the beginning of the boot sequence.

```
Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [kernel] in 9 seconds...
```

11. At the following prompt, type **boot -s** to start the system in single-user mode.

```
ok boot -s
```

12. At the following prompt, type **recovery** to start the root password recovery procedure.

```
Enter full pathname of shell or 'recovery' for root password recovery or RETURN
for /bin/sh: recovery
```

13. Enter configuration mode in the CLI.

14. Set the root password.

```
[edit]
user@host# set system root-authentication plain-text-password
```

When you configure a plain-text password, Junos OS encrypts the password for you.

CAUTION: Do not use the **encrypted-password** option unless the password is *already* encrypted, and you are entering the encrypted version of the password. If you commit the **encrypted-password** option with a plain-text password or with blank quotation marks (" "), you will not be able to log in to the device as root, and you will need to repeat this password recovery process.

15. At the following prompt, enter the new root password, for example:

```
New password: password
```

```
Retype new password:
```

16. At the second prompt, reenter the new root password.

17. After you have finished configuring the password, commit the configuration.

```
root@host# commit
commit complete
```

18. Exit configuration mode in the CLI.

19. Exit operational mode in the CLI.

20. At the prompt, type **y** to reboot the router.

```
Reboot the system? [y/n] y
```

See Also

- Configuring the Root Password on page 140
- Recovering the Root Password on Junos OS with Upgraded FreeBSD on page 147

Recovering the Root Password on Junos OS with Upgraded FreeBSD

If you forget the root password for a device running Junos OS with Upgraded FreeBSD, you can use the password recovery procedure to reset the root password.

For the list of Junos OS devices with upgraded FreeBSD, see Junos kernel upgrade to FreeBSD 10+

NOTE: You need console access to recover the root password.

NOTE: This password recovery procedure only applies to devices running Junos OS with Upgraded FreeBSD. For password recovery on Junos OS devices, see "Recovering the Root Password" on page 144.

To recover the root password:

1. Power off the router by pressing the power button on the front panel.
2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with the router into the RJ-45–to–DB-9 serial port adapter supplied with the router.
4. Plug the RJ-45–to–DB-9 serial port adapter into the serial port on the management device.
5. Connect the other end of the Ethernet rollover cable to the console port on the router.
6. Turn on the power to the management device.

7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).

8. Configure the port settings as follows:

   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

9. Power on the router by pressing the power button on the front panel.

   Verify that the POWER LED on the front panel turns green.

   The terminal emulation screen on your management device displays the router's boot sequence.

10. Access the Junos Main Menu.

    - Prior to Junos OS Release 17.3, the Junos Main Menu appears for 3 seconds on startup before automatically booting the Junos volume. Press any key within the 3 second window to stop the autotmatic boot sequence and display the Junos Main Menu.

      NOTE: The Junos Main Menu will appear every time you reboot the router while connected to the console.

    - Starting in Junos OS Release 17.3, press Ctrl+c at the following part in the reboot to bring up the Junos Main Menu:

```
FreeBSD/x86 bootstrap loader, Revision 1.1
(builder@feyrith.juniper.net, Sun Feb  4 13:06:24 PST 2018)
/
Autoboot in 1 seconds... (press Ctrl-C to interrupt)
```

```
1.  Boot [J]unos volume
2.  Boot Junos volume in [S]afe mode

3.  [R]eboot

4.  [B]oot menu
5.  [M]ore options
```

11. At the Junos Main Menu, press the **M** or **5** key to activate the **5. [M]ore options** menu:

```
1.  Recover [J]unos volume
2.  Recovery mode - [C]LI
```

```
3.  Check [F]ile system

4.  Enable [V]erbose boot

5.  [B]oot prompt

6.  [M]ain menu
```

12. Press the **C** or **2** key to access the **2. Recovery mode - [C]LI** option. The router will reboot into CLI recovery mode.

13. When prompted, press the **Enter** key to immediately boot the router, or press any other key to bring up the command prompt.

14. Enter configuration mode in the CLI.

```
root>#  configure
Entering configuration mode
```

15. Set the root password.

    When you configure a plain-text password, Junos OS encrypts the password for you.

```
[edit]
root# set system root-authentication plain-text-password
```

CAUTION: Do not use the **encrypted-password** option unless the password is *already* encrypted, and you are entering the encrypted version of the password. If you commit the **encrypted-password** option with a plain-text password or with blank quotation marks (" "), you will not be able to log in to the router as root, and you will need to repeat this password recovery process.

16. At the following prompt, enter the new root password, for example:

```
New password: password

Retype new password:
```

17. At the second prompt, reenter the new root password.

Troubleshooting Loss of the Root Password

Problem **Description:** If you forget the root password for a switch, use the password recovery procedure to reset the root password.

NOTE: You need physical access to the switch to recover the root password.

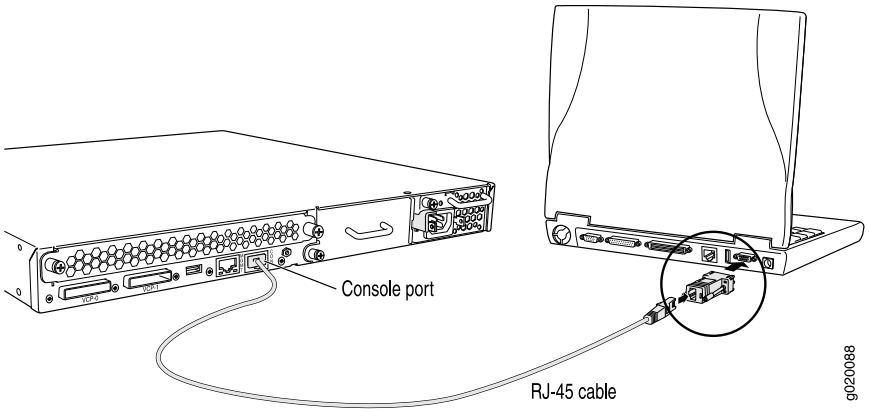
TIP: For a video on recovering the root password for routers, see "Root Password" on page 139. The procedure is similar for switches.

Solution To recover the root password:

1. Power off your switch by unplugging the power cord or turning off the power at the wall switch.

2. Insert one end of the Ethernet cable into the serial port on the management device and connect the other end to the console port on the back of the switch. See Figure 3 on page 150.

Figure 3: Connecting to the Console Port on the EX Series Switch



3. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).

4. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

5. Power on your switch by plugging in the power cord or turning on the power at the wall switch.

   NOTE: On EX2300 and EX3400 switches after step 5, use the following procedure:

   In the main menu that appears, select **[M]ore options > Recovery mode - [C]LI.**

   A series of messages describe consistency checks, mounting of filesystems, and initialization and checkout of management services. Then the CLI prompt appears.

   Proceed to Step 9 in this procedure.

6. When the following prompt appears, press the Spacebar to access the switch's bootstrap loader command prompt:

   ```
   Hit [Enter] to boot immediately, or space bar for command prompt.
   Booting [kernel] in 1 second...
   ```

   NOTE: If the switch is in unattended mode for U-Boot, access to the bootstrap loader command prompt is blocked. If the root password is lost, you must reset the switch to the factory default configuration using the LCD panel. For more information, see *Reverting to the Default Factory Configuration for the EX Series Switch*.

7. At the following prompt, type **boot -s** to start up the system in single-user mode:
   loader> boot -s

8. At the following prompt, type **recovery** to start the root password recovery procedure:
   Enter full path name of shell or 'recovery' for root password recovery or RETURN for /bin/sh: recovery

   A series of messages describe consistency checks, mounting of filesystems, and initialization and checkout of management services. Then the CLI prompt appears.

9. Enter configuration mode in the CLI:
   user@switch> configure

10. Set the root password. For example:
    user@switch# set system root-authentication plain-text-password

11. At the following prompt, enter the new root password. For example, juniper1:
    user@switch# juniper1

    ```
    Retype new password:
    ```

12. At the second prompt, reenter the new root password.

13. If you are finished configuring the network, commit the configuration.
    root@switch# commit

    ```
    commit complete
    ```

14. Exit configuration mode in the CLI.
    root@switch# exit

15. Exit operational mode in the CLI.
    root@switch> exit

16. At the prompt, enter **y** to reboot the switch.
    Reboot the system? [y/n] y

See Also

- *Connecting and Configuring an EX Series Switch (CLI Procedure)*
- *Connecting and Configuring an EX Series Switch (J-Web Procedure)*

Plain-Text Passwords

Changing the Requirements for Junos OS Plain-Text Passwords

For plain-text password requirements, see Special Requirements for Junos OS Plain-Text Passwords.

To change the requirements for plain-text passwords, include the **password** statement at the **[edit system login]** hierarchy level:

```
[edit system login]
password {
  change-type (set-transitions | character-set);
  format (sha1 | sha256 | sha512);
  maximum-length length;
  maximum-lifetime days
  minimum-changes number;
  minimum-character-changes number
```

```
    minimum-length length;
    minimum-lifetime days
    minimum-lower-cases number;
    minimum-numerics number;
    minimum-reusenumber
    minimum-punctuations number;
    minimum-upper-cases number;
}
```

NOTE: These statements apply to plain-text passwords only, not encrypted passwords.

See Also

- Configuring the Root Password on page 140
- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 153

Example: Changing the Requirements for Junos OS Plain-Text Passwords

This example shows how to set various maximum and minimum requirements for plain-text passwords to increase password strength.

Requirements

This example requires a device running Junos 12.2 or greater. The **minimum-length** and **maximum-length** password requirements statements are available in earlier releases, however, you must have Junos OS Release 12.2 or greater to configure **minimum-lower-cases**, **minimum-numerics**, **minimum-punctuations**, or **minimum-upper-cases**.

Overview

You can use a variety of requirements to strengthen plain-text passwords for greater security. Junos OS provides a number of possible configurations at the **[edit system login password]** hierarchy level that allow you to require users to create plain-text passwords that conform to a particular set of requirements that may include such things as length, number of changes, type of characters, numbers, or letter case.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set system login password minimum-length 12
set system login password maximum-length 22
set system login password minimum-numerics 1
set system login password minimum-upper-cases 1
set system login password minimum-lower-cases 1
set system login password minimum-punctuations 1
```

Configuring Requirements for Plain-Text Passwords

Step-by-Step Procedure

This example configures password requirements that require the user to creat a password that has a minimum length of 12 characters, a maximum length of 22 characters, and that includes at least one lower-case letter, at least one upper-case letter, at least one punctuation character, and at least one numeric character.

1. Navigate to configuration mode in the [system login password] hierarchy level.

```
user@host> edit
[edit]
user@host# edit system login password
```

2. Set a minimum length requirement of 12 characters and a maximum length requirement of 22 characters for user passwords.

```
[edit system login password]
user@host# set minimum-length 12
[edit system login password]
user@host# set maximum-length 22
```

3. Require users to set a password that has at least one lower-case letter and at least one upper-case letter.

```
[edit system login password]
user@host# set minimum-lower-cases 1
[edit system login password]
user@host# set minimum-upper-cases 1
```

4. Require users to set a password that has at least one punctuation-class character and at least one number.

```
[edit system login password]
user@host# set minimum-punctuations 1
[edit system login password]
user@host# set minimum-numerics 1
```

Results

From configuration mode, confirm your configuration by entering the show command at the edit system login password hierarchy level. if the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit system login password]
user@host# show
minimum-length 12;
maximum-length 22;
minimum-numerics 1;
minimum-upper-cases 1;
minimum-lower-cases 1;
```

See Also

- password (Login) on page 1327

Master Password for Configuration Encryption

Junos OS supports encryption method for configuration secrets using a master password. The master password derives an encryption key that uses AES256-GCM to protect certain secrets such as private keys, system master passwords, and other sensitive data by storing it in an AES256 encrypted format. For more information, read this topic.

- Hardening Shared Secrets in Junos OS on page 155
- Using Trusted Platform Module to Bind Secrets on SRX Series Devices on page 157

Hardening Shared Secrets in Junos OS

- Understanding Hardening Shared Secrets on page 155

Understanding Hardening Shared Secrets

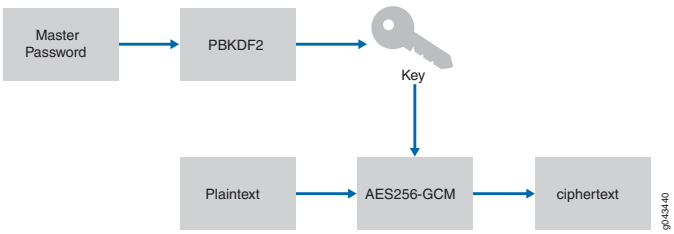
Existing shared secrets (9 format) in Junos OS currently use an obfuscation algorithm, which is not a very strong encryption for configuration secrets. If you want a strong encryption for your configuration secrets, you can configure a master password. The master password is used to derive an encryption key that is used with AES256-GCM to encrypt configuration secrets. This new encryption method uses the 8 formatted strings.

Starting with Junos OS Release 15.1X49-D50, new CLI commands are introduced to configure a system master password to provide stronger encryption for configuration secrets. The master password encrypts secrets like the RADIUS password, IKE preshared keys, and other shared secrets in the Junos OS management process (mgd) configuration. The master password itself is not saved as part of the configuration. The password quality is evaluated for strength, and the device gives feedback if weak passwords are used.

The master password is used as input to the password based key derivation function (PBKDF2) to generate an encryption key. the key is used as input to the Advanced Encryption Standard in Galois/Counter Mode (AES256-GCM). The plain text that the

user enters is processed by the encryption algorithm (with key) to produce the encrypted text (cipher text). See Figure 4 on page 156

Figure 4: Master Password Encryption



The 8 configuration secrets can only be shared between devices using the same master password.

The 8-encrypted passwords have the following format:

8crypt-algo$hash-algo$iterations$salt$ivtagencrypted. See Table 11 on page 156 for the master password format details.

Table 11: 8-encrypted Password Format

Format	Description
crypt-algo	Encryption/decryption algorithm to be used. Currently only AES256-GCM is supported.
hash-algo	Hash (prf) algorithm to be used for the PBKDF2 key derivation.
iterations	The number of iterations to use for the PBKDF2 hash function. Current iteration-count default is 100. The iteration count slows the hashing count, thus slowing attacker guesses.
salt	Sequence of ASCII64-encoded pseudorandom bytes generated during encryption that are to be used to *salt* (a random, but known string) the password and input to the PBKDF2 key derivation.
iv	A sequence of ASCII64-encoded pseudorandom bytes generated during encryption that are to be used as initialization vector for the AES256-GCM encryption function.
tag	ASCII64-encoded representation of the tag.
encrypted	ASCII64-encoded representation of the encrypted password.

The ASCII64 encoding is Base64 (RFC 4648) compatible, except no padding (character "=") is used to keep the strings short. For example:
8aes256-gcm$hmac-sha2-256$100$y/4YMC4YDLU$fzYDI4jjN6YCyQsYLsaf8A$Ilu4jLcZarD9YnyD/Hejww$okhBlc0cGakSqYxKww

Chassis Cluster Considerations

When defining a chassis cluster on SRX Series devices, be aware of the following restrictions:

- For SRX Series devices, first configure the master password on each node, and then build the cluster. The same master password should be configured on each node.
- In chassis cluster mode, the master password cannot be deleted.

NOTE: A change in the master password would mean disruption in chassis clustering; therefore you must change the password on both nodes independently.

Using Trusted Platform Module to Bind Secrets on SRX Series Devices

By enabling the Trusted Platform Module (TPM) on the SRX Series devices, the software layer leverages the use of the underlying TPM chip. TPM is a specialized chip that protects certain secrets at rest such as private keys, system master passwords, and other sensitive data by storing it in an AES256 encrypted format (instead of storing sensitive data in a clear text format). The device also generates a new SHA256 hash of the configuration each time the administrator commits the configuration. This hash is verified each time the system boots up. If the configuration has been tampered with, the verification fails and the device will not continue to boot. Both the encrypted data and the hash of the configuration is protected by the TPM module using the master encryption password.

NOTE: Hash validation is performed during any commit operation by performing a validation check of the configuration file against the saved hash from previous commits. In a chassis cluster system, hash is independently generated on the backup system as part of the commit process. A commit from any mode, that is, batch-config, dynamic-config, exclusive-config, or private config generates the integrity hash.

NOTE: Hash is saved only for the current configuration and not for any rollback configurations. Hash is not generated during reboot or shutdown of the device.

The TPM encrypts the following secrets:

- SHA256 hash of the configuration
- device master-password
- all key-pairs on the device

The TPM chip is available on the SRX300, SRX320, SRX340, and SRX345 devices. TPM is not enabled by default. To enable TPM, see "Enabling the TPM" on page 158.

Limitations

The following limitations and exceptions apply to the configuration file integrity feature using TPM:

- This feature is supported only on the SRX300, SRX320, SRX340 and SRX345 devices.
- If the master encryption password is not set, data is stored unencrypted.
- If the master encryption password and the multiple index backup files are deleted, data cannot be decrypted.
- If you set up the master encryption password, downgrading to older releases that do not implement TPM is not supported. You must delete the master encryption password and reenter all sensitive data before downgrading.
- If the master encryption password was deleted before the daemons had a chance to re-encrypt the data, then the data becomes unusable.
- The file integrity feature is not supported along with the configuration file encryption feature that uses keys saved in EEPROM. You can enable only one function at a time.

Enabling the TPM

NOTE: **Before enabling TPM, ensure that you have configured "set system master-password plain-text-password" otherwise, certain sensitive data will not be protected by the TPM.**

You can enable the TPM by setting the master encryption password using the following CLI command:

request security tpm master-encryption-password set plain-text-password

You will be prompted to enter the master encryption password twice, to make sure that these passwords match. The master encryption password is validated for required password strength.

After master encryption password is set, the system proceeds to encrypt the sensitive data with the master encryption password which is encrypted by the Master Binding Key that is owned and protected by the TPM chip.

NOTE: **If there is any issue with setting the master encryption password, a critical ERROR message is logged on the console and the process is aborted.**

Verifying the Status of the TPM

You can use the **show security tpm status** command to verify the status of the TPM. The following information is displayed:

- TPM enabled/disabled
- TPM ownership
- TPM's Master Binding Key status (created or not created)
- master encryption password status (set or not set)

Starting with Junos OS Release 15.1X49-D120 and Junos OS Release 17.4R1, Trusted Platform Module (TPM) firmware has been updated. The upgraded firmware version provides additional secure cryptography and improves security. Updated TPM firmware is available along with the Junos OS package. For updating TPM Firmware, see Upgrading TPM Firmware on SRX-Devices. To confirm the TPM firmware version, use the **show security tpm status** command. **TPM Family** and **TPM Firmware *version*** output fields are introduced.

Changing the Master Encryption Password

Changing the master encryption password is done using the CLI.

To change the master encryption password, enter the following command from operational mode:

request security tpm master-encryption-password set plain-text-password

NOTE: It is recommended that no configuration changes are made while you are changing the master encryption password.

The system checks if the master encryption password is already configured. If master encryption password is configured, then you are prompted to enter the current master encryption password.

The entered master encryption password is validated against the current master encryption password to make sure these master encryption passwords match. If the validation succeeds, you will be prompted to enter the new master encryption password as plain text. You will be asked to enter the key twice to validate the password.

The system then proceeds to re-encrypt the sensitive data with the new master encryption password. You must wait for this process of re-encryption to complete before attempting to change the master encryption password again.

If for some reason, the encrypted master encryption password file is lost or corrupted, the system will not be able to decrypt the sensitive data. The system can only be recovered by re-importing the sensitive data in clear text, and re-encrypting them.

If the system is compromised, the administrator can recover the system using of the following method:

- Clear the TPM ownership in u-boot and then install the image in boot loader using TFTP or USB (if USB port is not restricted).

NOTE: If the installed software version is older than Junos OS Release 15.1X49-D110 and the master encryption password is enabled, then installation of Junos OS Release 15.1X49-D110 will fail. You must backup the configuration, certificates, key-pairs, and other secrets and use the TFTP/USB installation procedure.

Release History Table

Release	Description
17.4R1	Starting with Junos OS Release 15.1X49-D120 and Junos OS Release 17.4R1, Trusted Platform Module (TPM) firmware has been updated. The upgraded firmware version provides additional secure cryptography and improves security. Updated TPM firmware is available along with the Junos OS package. For updating TPM Firmware, see Upgrading TPM Firmware on SRX-Devices. To confirm the TPM firmware version, use the **show security tpm status** command. **TPM Family** and **TPM Firmware *version*** output fields are introduced.
15.1X49-D50	Starting with Junos OS Release 15.1X49-D50, new CLI commands are introduced to configure a system master password to provide stronger encryption for configuration secrets.

Related Documentation

- master-password on page 1222
- Root Password on page 139
- Plain-Text Passwords on page 152

CHAPTER 4

User Authentication

Junos OS User Authentication Overview

Junos OS supports different methods such as local password authentication, RADIUS and TACACS+ to control access to the network. Authentication methods are used for validating users who attempt to access the router or switch using telnet. Authentication prevents unauthorized devices and users from gaining access to your LAN. For more information, read this topic.

Junos OS User Authentication Methods

The Junos OS supports three methods of user authentication: local password authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+).

With local password authentication, you configure a password for each user allowed to log in to the router or switch.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the router or switch using telnet. They are both distributed client-server systems—the RADIUS and TACACS+ clients run on the router or switch, and the server runs on a remote network system.

You can configure the router or switch to be both a RADIUS and TACACS+ client, and you can also configure authentication passwords in the Junos OS configuration file. You can prioritize the methods to configure the order in which the software tries the different authentication methods when verifying user access.

You can control access to your network using several different authentication methods—media access control (MAC) RADIUS, for example. Authentication prevents unauthorized devices and users from gaining access to your LAN. For MAC RADIUS authentication, end devices must be authenticated before they receive an IP address from a DHCP server.

NOTE: Note about the MAC RADIUS authentication:

- You can enable end devices to access the network without authenticating on the RADIUS server by configuring the MAC address of the end device in the static MAC bypass list by configuring the MAC address using the **authentication-whitelist** statement.
- You can configure one or more authentication methods on a single interface and thereby enable fallback to the next method if the first or second method is unsuccessful.
- On a single interface you can configure one or a combination of several authentication methods.
- The EAP method supported for MAC RADIUS authentication is EAP-MD5.
- You can configure MAC RADIUS authentication on interfaces that are connected to end devices.
- When you configure the **mac-radius restrict** option, the switch immediately attempts a MAC- RADIUS authentication by sending a request to the RADIUS server for authentication of the MAC address of the end device. If MAC address of the end device is configured for RADIUS authentication, LAN access between the two switches is created.

See Also

- Configuring RADIUS Server Authentication on page 182
- Configuring TACACS+ Authentication on page 207
- Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 169

Configuring Local User Template Accounts for User Authentication

You use local user template accounts when you need different types of templates for authentication. Each template can define a different set of permissions appropriate for the group of users who use that template. These templates are defined locally on the router or switch and referenced by the TACACS+ and RADIUS authentication servers.

When you configure local user templates and a user logs in, Junos OS issues a request to the authentication server to authenticate the user's login name. If a user is authenticated, the server returns the local username to Junos OS, which then determines whether a local username is specified for that login name (**local-username** for TACACS+, **Juniper-Local-User** for RADIUS). If so, Junos OS selects the appropriate local user template locally configured on the router or switch. If a local user template does not exist for the authenticated user, the router or switch defaults to the **remote** template.

To configure different access privileges for users who share the local user template account, include the **allow-commands** and **deny-commands** commands in the authentication server configuration file.

To configure a local user template, include the **user** *local-username* statement at the **[edit system login]** hierarchy level and specify the privileges you want to grant to the local users to whom the template applies:

```
[edit system login]
user local-username {
   full-name "Local user account";
   uid uid-value;
   class class-name;
}
```

This example configures the **sales** and **engineering** local user templates:

```
[edit]
system {
   login {
      user sales {
         uid uid-value;
         class class-name;
      }
      user engineering {
         uid uid-value;
         class class-name;
      }
   }
}
```

```
user = simon {
   ...
   service = junos-exec {
      local-user-name = sales
      allow-commands = "configure"
      deny-commands = "shutdown"
   }
}
user = rob {
   ...
   service = junos-exec {
      local-user-name = sales
      allow-commands = "(request system) | (show rip neighbor)"
      deny-commands = "clear"
```

```
    }
}
user = harold {
    ...
    service = junos-exec {
        local-user-name = engineering
        allow-commands = "monitor | help | show | ping | traceroute"
        deny-commands = "configure"
    }
}
user = jim {
    ...
    service = junos-exec {
        local-user-name = engineering
        allow-commands = "show bgp neighbor"
        deny-commands = "telnet | ssh"
    }
}
```

When the login users Simon and Rob are authenticated, the router or switch applies the sales local user template. When login users Harold and Jim are authenticated, the router or switch applies the engineering local user template.

See Also

- Example: Configuring Authentication Order on page 177
- user (Access) on page 1597

Configuring Remote Template Accounts for User Authentication

By default, the Junos OS uses remote template accounts for user authentication when:

- The authenticated user does not exist locally on the router or switch.
- The authenticated user's record in the authentication server specifies local user, or the specified local user does not exist locally on the router or switch.

To configure the remote template account, include the **user remote** statement at the **[edit system login]** hierarchy level and specify the privileges you want to grant to remote users:

```
[edit system login]
user remote {
    full-name "All remote users";
    uid uid-value;
    class class-name;
}
```

To configure different access privileges for users who share the remote template account, include the **allow-commands** and **deny-commands** statements in the authentication server configuration file.

See Also

- Example: Configuring Authentication Order on page 177

- user (Access) on page 1597

Example: Creating Template Accounts

This example shows how to create template accounts.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

You can create template accounts that are shared by a set of users when you are using RADIUS or TACACS+ authentication. When a user is authenticated by a template account, the CLI username is the login name, and the privileges, file ownership, and effective user ID are inherited from the template account.

By default, Junos OS uses the **remote** template account when:

- The authenticated user does not exist locally on the device.
- The authenticated user's record in the RADIUS or TACACS+ server specifies local user, or the specified local user does not exist locally on the device.

In this example, you create a remote template account and set the username to remote and the login class for the user as operator. You create a remote template that is applied to users authenticated by RADIUS or TACACS+ that do not belong to a local template account.

You then create a local template account and set the username as admin and the login class as superuser. You use local template accounts when you need different types of templates. Each template can define a different set of permissions appropriate for the group of users who use that template.

Configuration

Creating a Remote Template Account

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login user remote class operator
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To create a remote template account:

- Set the username and the login class for the user.

```
[edit system login]
user@host# set user remote class operator
```

Results

From configuration mode, confirm your configuration by entering the **show system login** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
   user@host# show system login
   user remote {
   class operator;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Creating a Local Template Account

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login user admin class superuser
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To create a local template account:

1. Set the username and the login class for the user.

```
[edit system login]
user@host# set user admin class superuser
```

Results From configuration mode, confirm your configuration by entering the **show system login** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
   user@host# show system login
   user admin {
   class super-user;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and specify a system authentication order. Do one of the following tasks:

- Configure a RADIUS server. See "Example: Configuring a RADIUS Server for System Authentication" on page 187.
- Configure a TACACS+ server. See "Example: Configuring a TACACS+ Server for System Authentication" on page 210.
- Configure system authentication order. See "Example: Configuring Authentication Order" on page 177.

Verification

Confirm that the configuration is working properly.

Verifying the Template Accounts Creation

Purpose Verify that the template accounts have been created.

Action From operational mode, enter the **show system login** command.

See Also

- Junos OS User Accounts Overview on page 67

Understanding Remote Authentication Servers

You probably already use a remote authentication server (or servers) in your network. It is a recommended best practice, because the servers allow you to centrally create a consistent set of user accounts for all devices in your network. There are many good reasons for implementing a authentication, authorization, and accountability (AAA) solution in your network, not the least of which is to make the management of user accounts easier.

There are two basic methods of remote authentication in use by most enterprises today—RADIUS and TACACS+. Junos OS supports both types and can be configured to query multiple remote authentication servers of both types. The idea behind a RADIUS or TACACS+ server is simple, a central authentication server that routers, switches, security devices, and even servers can use to authenticate users as they attempt to gain access to these systems. Think of the advantages that a central user directory brings for authentication auditing and access control in a client server model, and you have your justification for RADIUS or TACACS+ for your networks infrastructure.

Using a central server has multiple advantages over the alternative of creating local users on each device, a time-consuming and error-prone task. A central authentication system also simplifies the use of one-time password systems such as SecureID, which offer protection against password sniffing and password replay attacks, in which someone uses a captured password to pose as a system administrator.

- RADIUS—You should use RADIUS when your priorities are interoperability and performance.
  - Interoperability—RADIUS is more interoperable than TACACS+, primarily because of the proprietary nature of TACACS+. While TACACS+ supports more protocols, RADIUS is universally supported.
  - Performance—RADIUS is much lighter on your routers and switches and for this reason, network engineers generally prefer RADIUS over TACACS+.
- TACACS+—You should use TACACS+ when your priorities are security and flexibility.
  - Security—TACACS+ is more secure than RADIUS. Not only is the full session encrypted, but authorization and authentication are done separately to prevent someone from trying to force their way into your network.
  - Flexibility—TCP is a more flexible transport protocol than UDP. You can do more with it in more advanced networks. In addition, TACACS+ supports more of the enterprise protocols like NetBios or Appletalk.

Related Documentation

- Authentication Order for RADIUS, TACACS+, and Local Password on page 169
- RADIUS Authentication on page 182
- TACACS+ Authentication on page 206

Authentication Order for RADIUS, TACACS+, and Local Password

Junos OS supports different methods such as local password authentication, RADIUS and TACACS+ to control access to the network. Authentication methods are used for validating users who attempt to access the router or switch using telnet. You can prioritize the methods to configure the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch or security device. For more information, read this topic.

Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication

Using the **authentication-order** statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch.

If RADIUS and/or TACACS+ servers are configured in the authentication order but there is no response from them to a request, the Junos OS always defaults to trying local password authentication as a last resort. If the authentication order is set to **authentication-order password**, that will be the only authentication method attempted.

NOTE: It is not possible and would make no sense to try to configure local password authentication ahead of RADIUS or TACACS+ in the order because “no response” cannot happen. A local authentication request will always either be accepted or rejected.

The handling of a rejected authentication request when RADIUS or TACACS+ are present is more complicated.

- If **password** (local password authentication) is *not* in the authentication order, a RADIUS and/or TACACS+ rejection ends with the rejection.
- If **password** *is* included at the end of the authentication order and RADIUS and/or TACACS+ rejects the authentication, the Junos OS tries for a local authentication check.

In other words, including **password** as a final authentication order option is a means by which you can choose whether a RADIUS and/or TACACS+ rejection ends there or if the request is to be given one last chance for authentication locally.

Using RADIUS or TACACS+ Authentication

You can configure the Junos OS to be both a RADIUS and TACACS+ authentication client.

If an authentication method included in the **[authentication-order]** statement is not available, or if the authentication is available but returns a reject response, the Junos OS tries the next authentication method included in the **authentication-order** statement.

The RADIUS or TACACS+ server authentication might fail because of the following reasons:

- The authentication method is configured, but the corresponding authentication servers are not configured. For instance, the RADIUS and TACACS+ authentication methods are included in the **authentication-order** statement, but the corresponding RADIUS or TACACS+ servers are not configured at the respective **[edit system radius-server]** and **[edit system tacplus-server]** hierarchy levels.
- The RADIUS or TACACS+ server does not respond within the timeout period configured at the **[edit system radius-server]** or **[edit system tacplus-server]** hierarchy levels.
- The RADIUS or TACACS+ server is not reachable because of a network problem.

The RADIUS or TACACS+ server authentication might return a reject response because of the following reasons:

- The user profiles of users accessing a router or switch might not be configured on the RADIUS or TACACS+ server.
- The user enters incorrect logon credentials.

Using Local Password Authentication

You can explicitly configure the password authentication method or use this method as a fallback mechanism when remote authentication servers fail. The password authentication method consults the local user profiles configured at the **[edit system login]** hierarchy level. Users can log in to a router or switch using their local username and password in the following scenarios:

- The password authentication method (password) is explicitly configured as one of the authentication methods in the **[authentication-order** ***authentication-methods***] statement. In this case, the password authentication method is tried if no previous authentication accepts the logon credentials. This is true whether the previous authentication method fails to respond or returns a reject response because of an incorrect username or password.
- The password authentication method is not explicitly configured as one of the authentication methods in the **authentication-order** ***authentication-methods*** statement. In this case, the password authentication method is tried only if all configured authentication methods fail to respond. It is not consulted if any configured authentication method returns a reject response because of an incorrect username or password.

Order of Authentication Attempts

Table 12 on page 171 describes how the **authentication-order** statement at the **[edit system]** hierarchy level determines the procedure that the Junos OS uses to authenticate users for access to a router or switch.

Table 12: Order of Authentication Attempts

Syntax	Order of Authentication Attempts
authentication-order radius;	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS server is available but authentication is rejected, deny access. 4. If RADIUS servers are not available, try password authentication. NOTE: If a RADIUS server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [radius password];	1. Try configured RADIUS authentication servers. 2. If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.
authentication-order [radius tacplus];	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 5. If TACACS+ server is available but authentication is rejected, deny access. 6. If both RADIUS and TACACS+ servers are not available, try password authentication. NOTE: If either RADIUS or TACACS+ servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.

Table 12: Order of Authentication Attempts (continued)

Syntax	Order of Authentication Attempts
authentication-order [radius tacplus password];	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 5. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.
authentication-order tacplus;	1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ server is available but authentication is rejected, deny access. 4. If TACACS+ servers are not available, try password authentication. NOTE: If a TACACS+ server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [tacplus password];	1. Try configured TACACS+ authentication servers. 2. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.

Table 12: Order of Authentication Attempts (continued)

Syntax	Order of Authentication Attempts
authentication-order [tacplus radius];	1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 5. If RADIUS server is available but authentication is rejected, deny access. 6. If both TACACS+ and RADIUS servers are not available, try password authentication. NOTE: If either TACACS+ or RADIUS servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [tacplus radius password];	1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 5. If RADIUS servers fail to respond or return a reject response try password authentication, because it is explicitly configured in the authentication order.
authentication-order password;	1. Try to authenticate the user, using the password configured at the **[edit system login]** hierarchy level. 2. If the authentication is accepted, grant access. 3. If the authentication is rejected, deny access.

NOTE: If SSH public keys are configured, SSH user authentication first tries to perform public key authentication before using the authentication methods configured in the **authentication-order** statement. If you want SSH logins to use the authentication methods configured in the authentication-order statement without first trying to perform public key authentication, do not configure SSH public keys.

In a routing matrix based on a TX Matrix router, the authentication order must be configured only at the configuration groups **re0** and **re1**. The authentication order must not be configured at the **[edit system]** hierarchy. This is because the authentication order for the routing matrix is controlled on the switch-card chassis (or TX Matrix router) or switch-fabric chassis (for TX Matrix Plus router) only.

In Junos OS Release 10.0 and later, the superuser (belonging to the super-user login class) is also authenticated based on the authentication order that is configured for TACACS+, RADIUS, or password authentication using the **authentication-order** statement. For example, if the only configured authentication order is TACACS+, the superuser can only be authenticated by the TACACS+ server and password authentication cannot be used as an alternative. However, in Junos OS Release 9.6 and earlier, the superuser can use password authentication to login, even if password authentication is not configured explicitly using the **authentication-order** statement.

See Also

- Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 60
- Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 180

Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication

Using the **authentication-order** statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch. If you do not set the authentication order, by default users are verified based on their configured passwords.

When configuring a password using plain text and relying on Junos OS to encrypt it, you are still sending the password over the internet in plain text. Using pre-encrypted passwords is more secure because it means that the plain text of the password never has to be sent over the internet. Also, with passwords, only one user can be assigned to a password at a time.

On the other hand, both RADIUS and TACACS+ pre-ecrypt passwords. Both let you assign a set of users at a time instead of one by one. But here are how these authentication systems differ:

- RADIUS uses UDP, while TACACS+ uses TCP.
- RADIUS encrypts only the password during transmission whereas TACACS+ encrypts the entire session.
- RADIUS combines authentication (device) and authorization (user) whereas TACACS+ separates authentication, authorization, and accountability.

In short, TACACAS+ is the more secure of the two. However, RADIUS has better performance and is more interoperable. RADIUS is widely supported, whereas TACACS+ is a Cisco proprietary product and not widely supported outside of Cisco.

You can configure the authentication order based on your system, its restrictions, and your IT policy and operational preferences.

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

```
[edit system]
authentication-order [ authentication-methods ];
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Following are the possible authentication order entry options:

- **radius**—Verify the user using RADIUS authentication servers.
- **tacplus**—Verify the user using TACACS+ authentication servers.
- **password**—Verify the user using the username and password configured locally by including the authentication statement at the **[edit system login user]** hierarchy level.

If RADIUS and/or TACACS+ servers are configured in the authentication order but there is no response from them to a request, the Junos OS always defaults to trying local password authentication as a last resort. If the authentication order is set to **authentication-order password**, that will be the only authentication method attempted.

NOTE: It is not possible and would make no sense to try to configure local password authentication ahead of RADIUS or TACACS+ in the order because "no response" cannot happen. A local authentication request will always either be accepted or rejected.

The handling of a rejected authentication request when RADIUS or TACACS+ are present is more complicated.

- If **password** (local password authentication) is *not* in the authentication order, a RADIUS and/or TACACS+ rejection ends with the rejection.
- If **password** *is* included at the end of the authentication order and RADIUS and/or TACACS+ rejects the authentication, the Junos OS tries for a local authentication check.

In other words, including **password** as a final authentication order option is a means by which you can choose whether a RADIUS and/or TACACS+ rejection ends there or if the request is to be given one last chance for authentication locally.

For more details, see "Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication" on page 169.

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

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

The Junos OS enforces a limit on the number of standing authentication server requests that the CHAP authentication can have at one time. Thus, an authentication server method—RADIUS, for example—might fail to authenticate a client when this limit is exceeded. If it fails, the authentication sequence is reinitiated by the router or switch until authentication succeeds and the link is brought up. However, if the RADIUS servers are

not available and if additional authentication methods such as **tacplus** or **password** are configured along with **radius**, the next authentication method is tried.

The following example shows how to configure **radius** and **password** authentication:

```
[edit system]
user@switch# authentication-order [ radius password ];
```

The following example shows how to delete the **radius** statement from the authentication order:

```
[edit system]
user@switch# delete authentication-order radius
```

The following example shows how to insert the **tacplus** statement after the **radius** statement:

```
[edit system]
user@switch# insert authentication-order tacplus after radius
```

See Also

- Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 215
- **authentication-order on page 894**

Example: Configuring Authentication Order

This example shows how to configure authentication order.

Requirements

Before you begin, perform the initial device configuration. See the Getting Started Guide for your device.

Overview

You can configure the authentication methods that the device uses to verify that a user can gain access. For each login attempt, the device tries the authentication methods in order, starting with the first one, until the password matches. If you do not configure system authentication, users are verified based on their configured local passwords.

This example configures the device to attempt user authentication with the local password first, then with the RADIUS server, and finally with the TACACS+ server.

When you use local password authentication, you must create a local user account for every user who wants to access the system. However, when you are using RADIUS or

TACACS+ authentication, you can create single accounts (for authorization purposes) that are shared by a set of users. You create these accounts using the remote and local user template accounts. When a user is using a template account, the command-line interface (CLI) username is the login name; however, the privileges, file ownership, and effective user ID are inherited from the template account.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
insert system authentication-order radius after password
insert system authentication-order tacplus after radius
```

GUI Step-by-Step Procedure

To configure authentication order:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Authentication Method and Order** tab.
4. Under Available Methods, select the authentication method the device should use to authenticate users, and use the arrow button to move the item to the Selected Methods list. Available methods include:
   - RADIUS
   - TACACS+
   - Local Password

   If you want to use multiple methods to authenticate users, repeat this step to add the additional methods to the Selected Methods list.
5. Under Selected Methods, use the Up Arrow and Down Arrow to specify the order in which the device should execute the authentication methods.
6. Click **OK** to check your configuration and save it as a candidate configuration.
7. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure authentication order:

1. Add RADIUS authentication to the authentication order.

```
[edit]
user@host# insert system authentication-order radius after password
```

2. Add TACACS+ authentication to the authentication order.

```
[edit]
user@host# insert system authentication-order tacplus after radius
```

Results

From configuration mode, confirm your configuration by entering the **show system authentication-order** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system authentication-order
authentication-order [password, radius, tacplus];
```

If you are done configuring the device, enter **commit** from configuration mode.

NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and create user template accounts. Do one of the following tasks:

- Configure a RADIUS server. See "Example: Configuring a RADIUS Server for System Authentication" on page 187.
- Configure a TACACS+ server. See "Example: Configuring a TACACS+ Server for System Authentication" on page 210.
- Configure a user. See "Example: Configuring New Users" on page 70.
- Configure template accounts. See "Example: Creating Template Accounts" on page 165.

Verification

Confirm that the configuration is working properly.

Verifying the Authentication Order Configuration

Purpose

Verify that the authentication order has been configured.

Action From operational mode, enter the **show system authentication-order** command.

See Also
- Junos OS User Accounts Overview on page 67
- Junos OS User Authentication Methods on page 161

Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication

The following example shows how to configure system authentication for RADIUS, TACACS+, and password authentication.

In this example, only the user Philip and users authenticated by a remote RADIUS server can log in. If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the router or switch. If the RADIUS server is not available, the user is authenticated using the **password** authentication method and allowed access to the router or switch. For more information about the password authentication method, see "Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication" on page 169.

When Philip tries to log in to the system, if the RADIUS server authenticates him, he is given access and privileges for the **super-user** class. Local accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same user ID (UID) 9999 and the privileges associated with the **operator** class.

```
[edit]
system {
   authentication-order radius;
   login {
      user philip {
         full-name "Philip";
         uid 1001;
         class super-user;
      }
      user remote {
         full-name "All remote users";
         uid 9999;
         class operator;
      }
   }
}
```

NOTE: For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time. For example, when you create a remote template account, a set of remote users can concurrently share a single UID. For more information about template accounts, see "Example: Configuring Authentication Order" on page 177.

When a user logs in to a device, the user's login name is used by the RADIUS or TACACS+ server for authentication. If the user is authenticated successfully by the authentication server and the user is not configured at the **[edit system login user]** hierarchy level, the device uses the default remote template user account for the user, provided a remote template account is configured at the **edit system login user remote** hierarchy level. The remote template account serves as a default template user account for all users that are authenticated by the authentication server but not having a locally configured user account on the device. Such users share the same login class and UID.

To configure an alternate template user, specify the **user-name** parameter returned in the RADIUS authentication response packet. Not all RADIUS servers allow you to change this parameter. The following shows a sample Junos OS configuration:

```
[edit]
system {
   authentication-order radius;
   login {
      user philip {
         full-name "Philip";
         uid 1001;
         class super-user;
      }
      user operator {
         full-name "All operators";
         uid 9990;
         class operator;
      }
      user remote {
         full-name "All remote users";
         uid 9999;
         class read-only;
      }
   }
}
```

Assume your RADIUS server is configured with the following information:

- User Philip with password "olympia"
- User Alexander with password "bucephalus" and username "operator"
- User Darius with password "redhead" and username "operator"
- User Roxane with password "athena"

Philip would be given access as a superuser (**super-user**) because he has his own local user account. Alexander and Darius share UID 9990 and have access as operators. Roxane has no template-user override, so she shares access with all the other remote users, getting read-only access.

See Also

- Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 175

Related Documentation

- Junos OS User Authentication Overview on page 161
- RADIUS Authentication on page 182
- TACACS+ Authentication on page 206

RADIUS Authentication

The Junos OS supports RADIUS for central authentication of users on multiple routers or switches or security devices. To use RADIUS authentication on the device, you must configure information about one or more RADIUS servers on the network. You can also configure RADIUS accounting on the device to collect statistical data about the users logging in to or out from a LAN and sending the data to a RADIUS accounting server. For more information, read this topic.

- Configuring RADIUS Server Authentication on page 182
- Example: Configuring a RADIUS Server for System Authentication on page 187
- Example: Configuring RADIUS Authentication on page 190
- Configuring RADIUS Authentication (QFX Series or OCX Series) on page 192
- Juniper Networks Vendor-Specific RADIUS Attributes on page 194
- Juniper-Switching-Filter VSA Match Conditions and Actions on page 197
- Understanding RADIUS Accounting on page 199
- Configuring RADIUS System Accounting on page 200

Configuring RADIUS Server Authentication

RADIUS authentication is a method of authenticating users who attempt to access the router or switch.

- Why Use RADIUS on page 182
- Configuring RADIUS Server Details on page 183
- Configuring RADIUS To Use the Management Instance on page 186

Why Use RADIUS

The Junos OS supports two protocols for central authentication of users on multiple routers: RADIUS and TACACS+. We recommend RADIUS because it is a multivendor IETF standard, and its features are more widely accepted than those of TACACS+ or other proprietary systems. In addition, we recommend using a one-time-password system for increased security, and all vendors of these systems support RADIUS.

You should use RADIUS when your priorities are interoperability and performance:

- Interoperability—RADIUS is more interoperable than TACACS+, primarily because of the proprietary nature of TACACS+. While TACACS+ supports more protocols, RADIUS is universally supported.
- Performance—RADIUS is much lighter on your routers and switches and for this reason, network engineers generally prefer RADIUS over TACACS+.

Configuring RADIUS Server Details

To use RADIUS authentication on the device, configure information about one or more RADIUS servers on the network by including one **radius-server** statement at the **[edit system]** hierarchy level for each RADIUS server.

Because remote authentication is configured on multiple devices, it is commonly configured inside of a configuration group. As such, the steps shown here are in a configuration group called **global**. Using a configuration group is optional.

NOTE: The remote statement must always be lowercase.

NOTE: This feature is supported on SRX1500, SRX5400, SRX5600, and SRX5800 devices.

To configure authentication by a RADIUS server:

1. Add an IPv4 or IPv6 server address.

   - Configure an IPv4 source-address and server-address:

     ```
     [edit groups global]
     user@host# set system radius-server server-address source-address source-address
     ```

     For example:

     ```
     [edit groups global]
     user@host# set system radius-server 192.168.17.28 source-address 192.168.17.1
     ```

   - Configure an IPv6 source-address and server address:

     ```
     [edit groups global system radius-server server-address]
     user@host# set server-address secret “secretkey” source-address-inet6
       source-address
     ```

     For example:

     ```
     [edit groups global system radius-server ::17.22.22.162]
     user@host# set secret $9$lPOv87ZGiH.5JGn/AtOB7-dVgo source-address-inet6
       ::17.22.22.1
     ```

     Source address is a valid IPv4 or IPv6 address configured on one of the router or switch interfaces. This sets a fixed address as the source address for locally generated IP packets.

     Server address is a unique IPv4 or IPv6 address that is assigned to a particular server and used to route information to the server. If the Junos OS device has several interfaces that can reach the RADIUS server, assign an IP address that Junos OS can use for all its communication with the RADIUS server.

2. Include a shared secret password.

   You must specify a password in the **secret *password*** statement. If the password contains spaces, enclose it in quotation marks. The secret password used by the local router or switch must match that used by the server. The secret password configures the password that the Junos OS device uses to access the RADIUS server.

   ```
   [edit groups global system radius-server server-address]
   user@host# set secret password
   ```

   For example:

   ```
   [edit groups global system radius-server 192.168.69.162]
   user@host# set secret $9$gQ4UHf5F36CiH.5Tz9CuO1hreM8xw2oIENVwgZG
   ```

3. If necessary, specify a port on which to contact the RADIUS server.

   By default, port number 1812 is used (as specified in RFC 2865).

NOTE: You can also specify an accounting port to send accounting packets with the **accounting-port** statement. The default is 1813 (as specified in RFC 2866).

```
[edit groups global system radius-server server-address]
user@host# set port port-number
```

For example:

```
[edit groups global system radius-server 192.168.69.162]
user@host# set port 1845
```

4. Specify the order in which Junos OS attempts authentication.

   You must include the **authentication-order** statement in your remote authentication configuration.

   The example assumes your network includes both RADIUS and TACACS+ servers. In this example, whenever a user attempts to log in, Junos OS begins by querying the RADIUS server for authentication. If it fails, it next attempts authentication with locally configured user accounts. Finally the TACACS+ server is tried.

   ```
   [edit groups global system]
   user@host# set authentication-order [ authentication-methods ]
   ```

   For example:

   ```
   [edit groups global system]
   user@host# set authentication-order [ radius password tacplus ]
   ```

5. Assign a login class to RADIUS-authenticated users.

   You can assign different user templates and login classes to RADIUS-authenticated users. This allows RADIUS-authenticated users to be granted different administrative permissions on the Junos OS device. By default, RADIUS-authenticated users use the **remote** user template and are assigned to the associated class, which is specified in the **remote** user template, if the **remote** user template is configured. The username **remote** is a special case in Junos OS. It acts as a template for users who are authenticated by a remote server, but do not have a locally configured user account on the device. In this method, Junos OS applies the permissions of the remote template to those authenticated users without a locally defined account. All users mapped to the remote template are of the same login class.

   In the Junos OS configuration, a user template is configured in the same way as a regular local user account, except that no local authentication password is configured because the authentication is remotely performed on the RADIUS server.

   - To use the same permissions for all RADIUS-authenticated users:

```
[edit groups global system login]
user@host# set user remote class class
```

For example:

```
[edit groups global system login]
user@host# set user remote class super-user
```

- To have different login classes be used for different RADIUS-authenticated users, granting them different permissions:

  a. Create multiple user templates in the Junos OS configuration.

     Every user template can be assigned a different login class.

     For example:

     ```
     [edit groups global system login]
     set user RO class read-only
     set user OP class operator
     set user SU class super-user
     set user remote full-name "default remote access user template"
     set user remote class read-only
     ```

  b. Have the RADIUS server specify the name of the user template to be applied to the authenticated user.

     For a RADIUS server to indicate which user template is to be applied, it needs to include the Juniper-Local-User-Name attribute (Vendor 2636, type 1, string) Juniper VSA (vendor-specific attribute) in the RADIUS Access-Accept message. The string value in the Juniper-Local-User-Name must correspond to the name of a configured user template on the device. For a list of relevant Juniper RADIUS VSAs, see "Juniper Networks Vendor-Specific RADIUS Attributes" on page 194.

     If the Juniper-Local-User-Name is not included in the Access-Accept message or the string contains a user template name that does not exist on the device, the user is assigned to the **remote** user template, if configured. If it is not configured, authentication fails for the user.

     After logging in, the remotely authenticated user retains the same username that was used to log in. However, the user inherits the user class from the assigned user template.

     In a RADIUS server, users can be assigned a Juniper-Local-User-Name string, which indicates the user template to be used in the Junos OS device. From the previous example, the string would be RO, OP, or SU. Configuration of the RADIUS server depends on the server being used.

Configuring RADIUS To Use the Management Instance

By default, Junos OS routes authentication, authorization, and accounting packets for RADIUS through the default routing instance. Starting in Junos OS Release 18.1R1, existing

RADIUS behavior is enhanced to support a management interface in a non-default VRF instance.

When the **routing-instance mgmt_junos** option is configured in both the **radius-server** ***server-ip-address*** and the **raius server** ***server-ip-address*** statements, provided the **management-instance** statement is also configured, RADIUS packets are routed through the management instance mgmt_junos.

```
[edit system]
radius-server server-address {
   accounting-port port-number;
   port number;
   retry number;
   routing-instance routing-instance-name; #use “mgmt_junos” for RI name
   secret password;
   source-address source-address;
   timeout seconds;
}
```

```
[edit system accounting destination radius]
server {
   server-address {
      accounting-port port-number;
      retry number;
      routing-instance routing-instance; #use “mgmt_junos” for RI name
      secret password;
      source-address address;
      timeout seconds;
   }
}
```

NOTE: The routing-instance mgmt_junos option must be configured in both the radius-server and the radius server statements. If not, even if the management-instance statement is set, RADIUS packets will still be sent using the default routing instance only.

For more details on this management instance, see *management-instance*.

See Also

- Juniper Networks Vendor-Specific RADIUS Attributes on page 194
- Configuring RADIUS System Accounting on page 200
- Example: Configuring RADIUS Authentication on page 190

Example: Configuring a RADIUS Server for System Authentication

This example shows how to configure a RADIUS server for system authentication.

- Requirements on page 188
- Overview on page 188

Requirements

Before you begin:

- Perform the initial device configuration. See the Getting Started Guide for your device.
- Configure at least one RADIUS server. For more details, see RADIUS Authentication and Accounting Servers Configuration Overview.

Overview

In this example, you add a new RADIUS server with an IP address of 172.16.98.1 and specify the shared secret password of the RADIUS server as Radiussecret1. The secret is stored as an encrypted value in the configuration database. Finally, you specify the source address to be included in the RADIUS server requests by the device. In most cases you can use the loopback address of the device, which in this example is 10.0.0.1.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system radius-server address 172.16.98.1
set system radius-server 172.16.98.1 secret Radiussecret1
set system radius-server 172.16.98.1 source-address 10.0.0.1
```

GUI Step-by-Step Procedure

To configure a RADIUS server for system authentication:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Authentication Method and Order** tab.
4. In the RADIUS section, click **Add**. The Add Radius Server dialog box appears.
5. In the IP Address box, type the server's 32–bit IP address.
6. In the Password and Confirm Password boxes, type the secret password for the server and verify your entry.
7. In the Server Port box, type the appropriate port.

8. In the Source Address box, type the source IP address of the server.
9. In the Retry Attempts box, specify the number of times that the server should try to verify the user's credentials.
10. In the Time Out box, specify the amount of time (in seconds) the device should wait for a response from the server.
11. Click **OK** to check your configuration and save it as a candidate configuration.
12. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a RADIUS server for system authentication:

1. Add a new RADIUS server and set its IP address.

```
[edit system]
user@host# set radius-server address 172.16.98.1
```

2. Specify the shared secret (password) of the RADIUS server.

```
[edit system]
user@host# set radius-server 172.16.98.1 secret Radiussecret1
```

3. Specify the device's loopback address source address.

```
[edit system]
user@host# set radius-server 172.16.98.1 source-address 10.0.0.1
```

Results

From configuration mode, confirm your configuration by entering the **show system radius-server** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system radius-server
radius-server 172.16.98.1 {
    secret Radiussecret1;
    source-address 10.0.0.1;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

NOTE: To completely set up RADIUS authentication, you must create user template accounts and specify a system authentication order. Do one of the following tasks:

- Configure a system authentication order. See "Example: Configuring Authentication Order" on page 177.
- Configure a user. See "Example: Configuring New Users" on page 70.
- Configure local user template accounts. See "Example: Creating Template Accounts" on page 165.

Verification

Confirm that the configuration is working properly.

Verifying the RADIUS Server System Authentication Configuration

Purpose Verify that the RADIUS server has been configured for system authentication.

Action From operational mode, enter the **show system radius-server** command.

See Also
- Junos OS User Authentication Methods on page 161
- Junos OS User Accounts Overview on page 67
- Configuring Local User Template Accounts for User Authentication on page 162
- Example: Configuring a TACACS+ Server for System Authentication on page 210

Example: Configuring RADIUS Authentication

The Junos OS supports two protocols for central authentication of users on multiple routers: RADIUS and TACACS+. We recommend RADIUS because it is a multivendor IETF standard, and its features are more widely accepted than those of TACACS+ or other proprietary systems. In addition, we recommend using a one-time-password system for increased security, and all vendors of these systems support RADIUS.

The Junos OS uses one or more template accounts to perform user authentication. You create the template account or accounts, and then configure the user access to use that account. If the RADIUS server is unavailable, the fallback is for the login process to use the local account that set up on the router or switch.

The following example shows how to configure RADIUS authentication:

```
[edit]
system {
   authentication-order [ radius password ];
```

```
    root-authentication {
        encrypted-password "$ABC123; # SECRET-DATA
    }
    name-server {
        10.1.1.1;
        10.1.1.2;
    }
}
```

The following example shows how to enable RADIUS authentication and define the shared secret between the client and the server. The secret enables the client and server to determine that they are talking to the trusted peer.

Define a timeout value for each server, so that if there is no response within the specified number of seconds, the router can try either the next server or the next authentication mechanism.

```
[edit]
system {
    radius-server {
        10.1.2.1 {
            secret "$ABC123”; # SECRET-DATA
            timeout 5;
        }
        10.1.2.2 {
            secret "$ABC123"; # SECRET-DATA
            timeout 5;
        }
    }
}
```

The following example shows how to configure RADIUS template accounts for different users or groups of users:

```
[edit]
system {
    login {
        user observation {
            uid 1001;
            class observation;
        }
        user operation {
            uid 1002;
            class operation;
        }
        user engineering {
            uid 1003;
            class engineering;
        }
    }
}
```

Configuring RADIUS Authentication (QFX Series or OCX Series)

RADIUS authentication is a method of authenticating users who attempt to access the router or switch. Tasks to configure RADIUS authentication are:

NOTE: The **source-address** statement is not supported at the **[edit system radius-options** or **[edit system-radius-server** *name***]** hierarchies on the QFabric system.

- Configuring RADIUS Server Details on page 192
- Configuring MS-CHAPv2 for Password-Change Support on page 193
- Specifying a Source Address for the Junos OS to Access External RADIUS Servers on page 194

Configuring RADIUS Server Details

To use RADIUS authentication on the router or switch, configure information about one or more RADIUS servers on the network by including one **radius-server** statement at the **[edit system]** hierarchy level for each RADIUS server:

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

server-address is the address of the RADIUS server.

You can specify a port on which to contact the RADIUS server. By default, port number **1812** is used (as specified in RFC 2865). You can also specify an accounting port to send accounting packets. The default is **1813** (as specified in RFC 2866).

You must specify a password in the **secret *password*** statement. If the password contains spaces, enclose it in quotation marks. The secret used by the local router or switch must match that used by the server.

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

You can use the **source-address** statement to specify a logical address for individual or multiple RADIUS servers.

To configure multiple RADIUS servers, include multiple **radius-server** statements.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the **user** statement at the **[edit system login]** hierarchy level, as described in "Example: Configuring Authentication Order" on page 177.

You can also configure RADIUS authentication at the **[edit access]** and **[edit access profile]** hierarchy level. Junos OS uses the following search order to determine which set of servers are used for authentication:

1. **[edit access profile *profile-name* radius-server *server-address*]**
2. **[edit access radius-server *server-address*]**
3. **[edit system radius-server *server-address*]**

Configuring MS-CHAPv2 for Password-Change Support

You can configure the Microsoft implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the router or switch to support changing of passwords. This feature provides users accessing a router or switch the option of changing the password when the password expires, is reset, or is configured to be changed at the next login.

Before you configure MS-CHAPv2 for password-change support, ensure that you:

- Configure the RADIUS server authentication parameters
- Set the **authentication-order** to use the RADIUS server for the initial password attempt

To configure MS-CHAP-v2, include the following statements at the **[edit system radius-options]** hierarchy level:

```
[edit system radius-options]
password-protocol mschap-v2;
```

The following example shows statements for configuring the MS-CHAPv2 password protocol, password authentication order, and user accounts:

```
[edit]
system {
   authentication-order [ radius password ];
   radius-server {
      192.168.69.149 secret "$ABC123"; ## SECRET-DATA
   }
   radius-options {
      password-protocol mschap-v2;
   }
   login {
      user bob {
         class operator;
```

```
    }
  }
}
```

Specifying a Source Address for the Junos OS to Access External RADIUS Servers

You can specify which source address Junos OS uses when accessing your network to contact an external RADIUS server for authentication. You can also specify which source address Junos OS uses when contacting a RADIUS server for sending accounting information.

To specify a source address for a RADIUS server, include the **source-address** statement at the **[edit system radius-server *server-address*]** hierarchy level:

```
[edit system radius-server server-address]
source-address source-address;
```

source-address is a valid IP address configured on one of the router or switch interfaces.

See Also

- Juniper Networks Vendor-Specific RADIUS Attributes on page 194
- Example: Configuring Authentication Order on page 177
- Example: Configuring RADIUS Authentication on page 190
- Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 215
- Junos OS User Authentication Methods on page 161

Juniper Networks Vendor-Specific RADIUS Attributes

Junos OS supports the configuration of Juniper Networks RADIUS vendor-specific attributes (VSAs). These VSAs are encapsulated in a RADIUS vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. Table 13 on page 194 lists the Juniper Networks VSAs you can configure.

Table 13: Juniper Networks Vendor-Specific RADIUS Attributes

Name	Description	Type	Length	String
Juniper-Local-User-Name	Indicates the name of the user template used by this user when logging in to a device. This attribute is used only in Access-Accept packets.	1	≥3	One or more octets containing printable ASCII characters.

Table 13: Juniper Networks Vendor-Specific RADIUS Attributes (continued)

Name	Description	Type	Length	String
Juniper-Allow-Commands	Contains an extended regular expression that enables the user to run operational mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	2	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 99.
Juniper-Deny-Commands	Contains an extended regular expression that denies the user permission to run operation mode commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	3	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 99.
Juniper-Allow-Configuration	Contains an extended regular expression that enables the user to run configuration mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	4	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 99.
Juniper-Deny-Configuration	Contains an extended regular expression that denies the user permission to run configuration commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	5	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 99.

Table 13: Juniper Networks Vendor-Specific RADIUS Attributes (continued)

Name	Description	Type	Length	String
Juniper-Interactive-Command	Indicates the interactive command entered by the user. This attribute is used only in Accounting-Request packets.	8	≥3	One or more octets containing printable ASCII characters.
Juniper-Configuration-Change	Indicates the interactive command that results in a configuration (database) change. This attribute is used only in Accounting-Request packets.	9	≥3	One or more octets containing printable ASCII characters.
Juniper-User-Permissions	Contains information the server uses to specify user permissions. This attribute is used only in Access-Accept packets. NOTE: When the **Juniper-User-Permissions** attribute is configured to grant the Junos OS **maintenance** or **all** permissions on a RADIUS server, the UNIX wheel group membership is not automatically added to a user's list of group memberships. Some operations such as running the **su root** command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions **maintenance** or **all**, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account.	10	≥3	One or more octets containing printable ASCII characters. The string is a list of permission flags separated by a space. The exact name of each flag must be specified in its entirety. See "Login Class Permission Flags" on page 91.
Juniper-Authentication-Type	Indicates the authentication method (local database, or RADIUS server) used to authenticate a user. If the user is authenticated using a local database, the attribute value shows 'local'. If the user is authenticated using RADIUS server, the attribute value shows 'remote'.	11	≥5	One or more octets containing printable ASCII characters.

Table 13: Juniper Networks Vendor-Specific RADIUS Attributes (continued)

Name	Description	Type	Length	String
Juniper-Session-Port	Indicates the source port number of the established session.	12	size of integer	Integer

For more information about the VSAs, see RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*.

Juniper-Switching-Filter VSA Match Conditions and Actions

Devices support the configuration of RADIUS server attributes specific to Juniper Networks. These attributes are known as vendor-specific attributes (VSAs) and are described in RFC 2138, *Remote Authentication Dial In User Service* (RADIUS).

Through VSAs, you can configure port-filtering attributes on the RADIUS server. VSAs are cleartext fields sent from the RADIUS server to the device as a result of authentication success or failure. Authentication prevents unauthorized user access by blocking a supplicant at the port until the device is authenticated by the RADIUS server. The VSA attributes are interpreted by the device during authentication, and the device takes appropriate actions. Implementing port-filtering attributes with authentication on the RADIUS server provides a central location for controlling LAN access for supplicants.

These port-filtering attributes specific to Juniper Networks are encapsulated in a RADIUS server VSA with the vendor ID set to the Juniper Networks ID number, 2636.

As well as configuring port-filtering attributes through VSAs, you can apply a port firewall filter that has already been configured on the device directly to the RADIUS server. Like port-filtering attributes, the filter is applied during the authentication process, and its actions are applied at the device port. Adding a port firewall filter to a RADIUS server eliminates the need to add the filter to multiple ports and devices.

The Juniper-Switching-Filter VSA works in conjunction with 802.1X authentication to centrally control access of supplicants to the network. You can use this VSA to configure filters on the RADIUS server, which are sent to the switch and applied to users that have been authenticated using 802.1X authentication.

The Juniper-Switching-Filter VSA can contain one or more filter terms. Filter terms are configured using one or more *match conditions* with a resulting *action*. Match conditions are the criteria that a packet must meet for a configured action to be applied on it. The action is the action that the switch takes if a packet meets the criteria in the match conditions. The action that the switch can take is either accept or deny a packet.

The following guidelines apply when you specify match conditions and actions for VSAs:

- Both **match** and **action** statements are mandatory.
- If no match condition is specified, any packet is considered a match by default.
- If no action is specified, the default action is to deny the packet.
- Any or all options can be included in each **match** and **action** statement.

- The AND operation is performed on fields that are of a different type, which are separated by commas. Fields of the same type cannot be repeated.
- For the **forwarding-class** option to be applied, the forwarding class must be configured on the switch. If the forwarding class is not configured on the switch, this option is ignored.

Table 14 on page 198 describes the match conditions that you can specify when you configure a VSA attribute as a firewall filter by using the **match** command on the RADIUS server. The string that defines a match condition is called a *match statement*.

Table 14: Match Conditions

Option	Description
destination-mac *mac-address*	Destination media access control (MAC) address of the packet.
source-vlan *source-vlan*	Name of the source VLAN.
source-dot1q-tag *tag*	Tag value in the 802.1Q header, in the range **0** through **4095**.
destination-ip *ip-address*	Address of the final destination node.
ip-protocol *protocol-id*	IPv4 protocol value. In place of the numeric value, you can specify one of the following text synonyms: **ah**, **egp (8)**, **esp (50**, **gre (47)**, **icmp (1)**, **igmp (2)**, **ipip (4)**, **ipv6 (41)**, **ospf (89)**, **pim (103)**, **rsvp (46)**, **tcp (6)**, or **udp (17)**
source-port *port*	TCP or User Datagram Protocol (UDP) source port field. Normally, you specify this match statement in conjunction with the **ip-protocol** match statement to determine which protocol is being used on the port. In place of the numeric field, you can specify one of the text options listed under **destination-port**.
destination-port *port*	TCP or UDP destination port field. Normally, you specify this match statement in conjunction with the **ip-protocol** match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify one of the following text synonyms (the port numbers are also listed): **afs (1483)**, **bgp (179)**, **biff (512)**, **bootpc (68)**, **bootps (67)**, **cvspserver (2401)**, **cmd (514)**, **dhcp (67)**, **domain (53)**, **eklogin (2105)**, **ekshell (2106)**, **exec (512)**, **finger (79)**, **ftp (21)**, **ftp-data (20)**, **http (80)**, **https (443)**, **ident (113)**, **imap (143)**, **kerberos-sec (88)**, **klogin (543)**, **kpasswd (761)**, **krb-prop (754)**, **krbupdate (760)**, **kshell (544)**, **ldap (389)**, **login (513)**, **mobileip-agent (434)**, **mobilip-mn (435)**, **msdp (639)**, **netbios-dgm (138)**, **netbios-ns (137)**, **netbios-ssn (139)**, **nfsd (2049)**, **nntp (119)**, **ntalk (518)**, **ntp (123)**, **pop3 (110)**, **pptp (1723)**, **printer (515)**, **radacct (1813)**, **radius (1812)**, **rip (520)**, **rkinit (2108)**, **smtp (25)**, **snmp (161)**, **snmptrap (162)**, **snpp (444)**, **socks (1080)**, **ssh (22)**, **sunrpc (111)**, **syslog (514)**, **telnet (23)**, **tacacs-ds (65)**, **talk (517)**, **tftp (69)**, **timed (525)**, **who (513)**, **xdmcp (177)**, **zephyr-clt (2103)**, **zephyr-hm (2104)**

When you define one or more terms that specify the filtering criteria, you also define the action to take if the packet matches all criteria. Table 15 on page 199 shows the actions that you can specify in a term.

Table 15: Actions for VSAs

Option	Description
(**allow** | **deny**)	Accept a packet or discard a packet silently without sending an Internet Control Message Protocol (ICMP) message.
forwarding-class *class-of-service*	(Optional) Classify the packet in one of the following forwarding classes: • **assured-forwarding** • **best-effort** • **expedited-forwarding** • **network-control**
loss-priority (**low** | **medium** | **high**)	(Optional) Set the packet loss priority (PLP) to **low**, **medium**, or **high**. Specify both the forwarding class and the loss priority.

See Also
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 297
- Understanding Dynamic Filters Based on RADIUS Attributes on page 306

Understanding RADIUS Accounting

Devices support IETF RFC 2866, *RADIUS Accounting*. Configuring RADIUS accounting on the device supports collecting statistical data about users logging in to or out from a LAN and sending the data to a RADIUS accounting server. The statistical data gathered can be used for general network monitoring, analyzing and tracking usage patterns, or billing a user based upon the amount of time or type of services accessed.

To configure RADIUS accounting, specify one or more RADIUS accounting servers to receive the statistical data from the device, and select the type of accounting data to be collected.

The RADIUS accounting server you specify can be the same server used for RADIUS authentication, or it can be a separate RADIUS server. You can specify a list of RADIUS accounting servers. If the primary server (the first one configured) is unavailable, each RADIUS server in the list is tried in the order in which they are configured in the Junos OS.

The RADIUS accounting process between the device and a RADIUS server works like this:

1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. For example, on FreeRADIUS, the default port is 1813.

2. The device forwards an *accounting-request* packet containing an event record to the accounting server. The event record associated with this supplicant contains an *Acct-Status-Type* attribute whose value indicates the beginning of user service for this supplicant. When the supplicant's session ends, the accounting request contains an *Acct-Status-Type* attribute value indicating the end of user service. The RADIUS accounting server records this as a stop-accounting record containing session information and the length of the session.

3. The RADIUS accounting server logs these events in a file as start-accounting or stop-accounting records. On FreeRADIUS, the filename is the server's address; for example, 192.0.2.0.

4. The accounting server sends an *accounting-response* packet back to the device confirming it has received the accounting request.

5. If the device does not receive a response from the server, it continues to send accounting requests until an accounting response is returned from the accounting server.

The statistics collected through this process can be displayed from the RADIUS server; to see those statistics, the user accesses the log file configured to receive them.

See Also
- Configuring RADIUS System Accounting on page 200

Configuring RADIUS System Accounting

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.

Tasks for configuring RADIUS system accounting are:

1. Configuring Auditing of User Events on a RADIUS Server on page 200
2. Specifying RADIUS Server Accounting and Auditing Events on page 201
3. Configuring RADIUS Server Accounting on page 201

Configuring Auditing of User Events on a RADIUS Server

To audit user events, include the following statements at the **[edit system accounting]** hierarchy level:

```
[edit system accounting]
events [ events ];
destination {
  radius {
    server {
      server-address {
        accounting-port port-number;
        retry number;
        routing-instance routing-instance;
        secret password;
        source-address address;
        timeout seconds;
      }
    }
  }
```

```
}
```

Specifying RADIUS Server Accounting and Auditing Events

To specify the events you want to audit when using a RADIUS server for authentication, include the **events** statement at the **[edit system accounting]** hierarchy level:

```
[edit system accounting]
events [ events ];
```

events is one or more of the following:

- **login**—Audit logins
- **change-log**—Audit configuration changes
- **interactive-commands**—Audit interactive commands (any command-line input)

Configuring RADIUS Server Accounting

To configure RADIUS server accounting, include the **server** statement at the **[edit system accounting destination radius]** hierarchy level:

```
server {
  server-address {
    accounting-port port-number;
    retry number;
    routing-instance routing-instance;
    secret password;
    source-address address;
    timeout seconds;
  }
}
```

server-address specifies the address of the RADIUS server. To configure multiple RADIUS servers, include multiple **server** statements.

NOTE: If no RADIUS servers are configured at the **[edit system accounting destination radius]** statement hierarchy level, the Junos OS uses the RADIUS servers configured at the **[edit system radius-server]** hierarchy level.

accounting-port ***port-number*** specifies the RADIUS server accounting port number.

The default port number is 1813.

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.

routing-instance *routing-instance* is the name of the non-default management instance. Use **mgmt_junos** as the routing-instance name. See *Management Interface in a Nondefault Instance*.

You must specify a secret (password) that the local router or switch passes to the RADIUS client by including the **secret** statement. If the password contains spaces, enclose the entire password in quotation marks (“ “).

In the **source-address** statement, specify a source address for the RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. The source address is a valid IPv4 address (in case if radius-server address is IPv4) or IPv6 address (in case if radius-server address is IPv6) configured on one of the router or switch interfaces.

Optionally, you can specify the number of times that the router or switch attempts to contact a RADIUS authentication server by including the **retry** statement. By default, the router or switch retries three times. You can configure the router or switch to retry from 1 through 10 times.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a RADIUS server by including the **timeout** statement. By default, the router or switch waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

Starting with Junos OS Release 14.1 and Junos OS Release 17.3R1, you can configure the **enhanced-accounting** statement to view the attribute values of a logged in user. If you use the **enhanced-accounting** statement at the **[edit system radius-options]** hierarchy level, the RADIUS attributes such as access method, remote port, and access privileges can be audited. You can limit the number of attribute values to be displayed for auditing by using the **enhanced-avs-max** *<number>* statement at the **[edit system accounting]** hierarchy level.

```
[edit system radius-options]
enhanced-accounting;
```

```
[edit system accounting]
enhanced-avs-max <number>;
```

When a Juniper Networks router or switch is configured with RADIUS accounting, it sends **Accounting-Start** and **Accounting-Stop** messages to the RADIUS server. These messages contain information about user activities such as software logins, configuration changes, and interactive commands. This information is typically used for monitoring a network, collecting usage statistics, and ensuring that users are billed properly.

The following example shows three servers (10.5.5.5, 10.6.6.6, and 10.7.7.7) configured for RADIUS accounting:

```
system {
   accounting {
      events [ login change-log interactive-commands ];
      destination {
```



```
        radius {
          server {
            10.5.5.5 {
              accounting-port 3333;
              secret $ABC123;
              source-address 10.1.1.1;
              retry 3;
              timeout 3;
            }
            10.6.6.6 secret $ABC123;
            10.7.7.7 secret $ABC123;
          }
        }
      }
    }
}
```

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 18.1R1, existing RADIUS behavior is enhanced to support a management interface in a non-default VRF instance.
14.1	Starting with Junos OS Release 14.1 and Junos OS Release 17.3R1, you can configure the **enhanced-accounting** statement to view the attribute values of a logged in user.

Related Documentation

- Junos OS User Authentication Overview on page 161
- Authentication Order for RADIUS, TACACS+, and Local Password on page 169
- TACACS+ Authentication on page 206

RADIUS over TLS (RADSEC)

RADIUS over TLS is designed to provide secure communication of RADIUS requests using the Transport Secure Layer (TLS) protocol. RADIUS over TLS, also known as RADSEC, redirects regular RADIUS traffic to remote RADIUS servers connected over TLS. RADSec allows RADIUS authentication, authorization and accounting data to be passed safely across untrusted networks.

RADSEC uses TLS in combination with the Transmission Control Protocol (TCP). This transport profile provides stronger security than the User Datagram Protocol (UDP) which was originally used for RADIUS transmission. RADIUS over UDP encrypts the shared secret password using the MD5 algorithm, which is vulnerable to attacks. RADSEC mitigates the risk of attacks on MD5 by exchanging RADIUS packet payloads over an encrypted TLS tunnel.

NOTE: Due to limitations of the TCP protocol, RADSEC can have no more than 255 RADIUS messages in flight.

Configure the RADSEC Destination

RADSEC servers are represented by RADSEC destination objects. To configure RADSEC, you must define the RADSEC server as a destination, and direct RADIUS traffic to that destination.

You define the RADSEC server as a destination using the radsec statement at the **[edit access]** hierarchy level. RADSEC destinations are identified by a unique numeric ID. You can configure multiple RADSEC destinations with different parameters pointing to the same RADSEC server.

To redirect traffic from a standard RADIUS server to a RADSEC server, associate the RADIUS server with a RADSEC destination. For example, the RADIUS server **1.1.1.1** is associated with RADSEC destination **10**:

```
access {
   radius-server 1.1.1.1 {
      secret zzz;
      radsec-destination 10;
   }
}
```

You can also associate the RADIUS server with a RADSEC destination inside an access profile. For example, RADIUS server **2.2.2.2** in profile **acc_profile** is associated with RADSEC destination **10**:

```
access {
   profile acc_profile {
      secret zzz;
      radsec-destination 10;
   }
}
```

NOTE: You can redirect more than one RADIUS server to the same RADSEC destination.

To configure RADSEC:

1. Configure the RADSEC destination with a unique ID and an IP address.

```
[edit access]
user@host# radsec destination id-number address server-address
```

2. Configure the port of the RADSEC server. If no port is configured, the default RADSEC port 2083 is used.

```
[edit access radsec destination id-number]
user@host# port port-number
```

3. Redirect traffic from a RADIUS server to the RADSEC destination:

```
[edit access]
user@host# radius-server server-address radsec-destination id-number
```

Configure TLS Connection Parameters

The TLS connection provides encryption, authentication, and data integrity for the exchange of RADIUS messages. TLS relies on certificates and private-public key exchange pairs to secure the transmission of data between the RADSEC client and server. The RADSEC destination uses local certificates that are dynamically acquired from the Junos PKI infrastructure.

To enable RADSEC, you must specify the name of the local certificate. For information on configuring the local certificate and certificate authority (CA), see *Configuring Digital Certificates*.

1. Specify the name of the local certificate to be used for TLS communications.

```
[edit access]
user@host# radsec destination id-number tls-certificate certificate-name
```

2. Configure the certified name of the RADSEC server.

```
[edit access]
user@host# radsec destination id-number tls-peer-name cert-server-name
```

3. (Optional) Configure the TLS connection timeout (default is 5 seconds).

```
[edit access]
user@host# radsec destination id-number tls-timeout seconds
```

Example: Simple RADSEC Configuration

The following example is a simple RADSEC configuration with one RADIUS server and one RADSEC destination. RADIUS traffic is redirected from RADIUS server 1.1.1.1 to RADSEC destination 10.

```
access {
  radius-server 1.1.1.1 {
    secret zzz;
    radsec-destination 10;
  }
  radsec {
    destination 10 {
      address 10.1.1.1;
      max-tx-buffers 1000;
      id-reuse-timeout 30;
      port 1777;
      source-address 1.1.1.2;
      tls-certificate my_cert;
      tls-force-ciphers { medium | low };
      tls-min-version { v1.1 | v1.2 };
      tls-peer-name x0.radsec.com
      tls-timeout 10;
    }
  }
}
```

Monitoring Certificates

To view information about the state and statistics of local certificate acquisition: **show network-access radsec local-certificate**.

Monitoring RADSEC Destinations

To view statistics for the RADSEC destinations: **show network-access radsec statistics**.

To view the state of the RADSEC destinations: **show network-access radsec state**.

Related Documentation

- Example: Configuring RADIUS Authentication on page 190
- Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 180
- Example: Configuring Authentication Order on page 177
- Example: Configuring RADIUS Authentication on page 190

TACACS+ Authentication

The Junos OS supports TACACS+ for central authentication of users on multiple routers or switches or security devices. To use TACACS+ authentication on the device, you must configure information about one or more TACACS+ servers on the network. You can also

configure TACACS+ accounting on the device to collect statistical data about the users logging in to or out from a LAN and sending the data to a TACACS+ accounting server. For more information, read this topic.

Configuring TACACS+ Authentication

TACACS+ authentication is a method of authenticating users who attempt to access the router or switch.

NOTE: Starting with Release 13.3, Junos OS supports IPv6 along with the existing IPv4 support for user authentication using TACACS+ servers.

Tasks to configure TACACS+ configuration are:

Configuring TACACS+ Server Details

To use TACACS+ authentication on the router or switch, configure information about one or more TACACS+ servers on the network by including the **tacplus-server** statement at the **[edit system]** hierarchy level:

```
[edit system]
tacplus-server server-address {
   port port-number;
   routing-instance routing-instance;
   secret password;
   single-connection;
   timeout seconds;
}
```

server-address is the address of the TACACS+ server.

port-number is the TACACS+ server port number.

routing-instance ***routing-instance*** is the name of the routing instance used to send and receive TACACS+ packets. By default, Junos OS routes authentication, authorization, and accounting packets for TACACS+ through the default routing instance. Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support routing TACACS+ packets through a management interface in a non-default VRF instance named mgmt_junos. For more information on this VRF management instance, see "Configuring TACACS+ to Use the Management Instance" on page 209. Starting in Junos OS Release 18.2R1, you can route TACACS+ traffic through any routing instance you configure in authentication.

You must specify a secret (password) that the local router or switch passes to the TACACS+ client by including the **secret** statement. If the password included spaces, enclose the password in quotation marks. The secret used by the local router or switch must match that used by the server.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a TACACS+ server by including the **timeout** statement. By default, the router or switch waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds.

Optionally, you can have the software maintain one open Transmission Control Protocol (TCP) connection to the server for multiple requests, rather than opening a connection for each connection attempt by including the **single-connection** statement.

NOTE: Early versions of the TACACS+ server do not support the **single-connection** option. If you specify this option and the server does not support it, the Junos OS will be unable to communicate with that TACACS+ server.

To configure multiple TACACS+ servers, include multiple **tacplus-server** statements.

On a TX Matrix router, TACACS+ accounting should be configured only under the groups **re0** and **re1**.

NOTE: Accounting should not be configured at the **[edit system]** hierarchy level; on a TX Matrix router, control is done under the switch-card chassis only.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the **user** statement at the **[edit system login]** hierarchy level, as described in "Example: Configuring Authentication Order" on page 177.

See Also

- *routing-instance (Accounting and Authentication)*

Configuring TACACS+ to Use the Management Instance

By default, Junos OS routes authentication, authorization, and accounting packets for TACACS+ through the default routing instance. Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support a management interface in a non-default VRF instance.

```
[edit system]
tacplus-server server-address {
   routing-instance routing-instance;
}
```

When the **routing-instance mgmt_junos** option is configured in both the **tacplus-server** ***server-address*** and the **tacplus server** ***server-ip*** statements (see tacplus), provided the **management-instance** statement is also configured, TACACS+ packets are routed through the management instance mgmt_junos.

For more details on this management instance, see *management-instance*.

Specifying a Source Address for the Junos OS to Access External TACACS+ Servers

You can specify which source address the Junos OS uses when accessing your network to contact an external TACACS+ server for authentication. You can also specify which source address the Junos OS uses when contacting a TACACS+ server for sending accounting information.

To specify a source address for a TACACS+ server for authentication, include the **source-address** statement at the **[edit system tacplus-server** ***server-address*****]** hierarchy level:

```
[edit system tacplus-server server-address]
source-address source-address;
```

source-address is a valid IP address configured on one of the router or switch interfaces.

To specify a source address for a TACACS+ server for system accounting, include the **source-address** statement at the **[edit system accounting destination tacplus server** ***server-address*****]** hierarchy level:

```
[edit system accounting destination tacplus server server-address]
source-address source-address;
```

source-address is a valid IP address configured on one of the router or switch interfaces.

Configuring the Same Authentication Service for Multiple TACACS+ Servers

To configure the same authentication service for multiple TACACS+ servers, include statements at the **[edit system tacplus-server]** and **[edit system tacplus-options]** hierarchy levels. For information about how to configure a TACACS+ server at the **[edit system tacplus-server]** hierarchy level, see "Configuring TACACS+ Authentication" on page 207.

To assign the same authentication service to multiple TACACS+ servers, include the **service-name** statement at the **[edit system tacplus-options]** hierarchy level:

```
[edit system tacplus-options]
service-name service-name;
```

service-name is the name of the authentication service. By default, the service name is set to **junos-exec**.

The following example shows how to configure the same authentication service for multiple TACACS+ servers:

```
[edit system]
tacplus-server {
   10.2.2.2 secret "$ABC123"; ## SECRET-DATA
   10.3.3.3 secret "$ABC123";## SECRET-DATA
}
tacplus-options {
   service-name bob;
}
```

Configuring Juniper Networks Vendor-Specific TACACS+ Attributes

The Juniper Networks Vendor-Specific TACACS+ Attributes enable you to configure access privileges for users on a TACACS+ server. They are specified in the TACACS+ server configuration file on a per-user basis. The Junos OS retrieves these attributes through an authorization request of the TACACS+ server after authenticating a user. You do not need to configure these attributes to run the Junos OS with TACACS+.

To specify these attributes, include a **service** statement of the following form in the TACACS+ server configuration file:

```
service = junos-exec {
   local-user-name = <username-local-to-router>
   allow-commands = "<allow-commands-regex>"
   allow-configuration-regexps = "<allow-configuration-regex>"
   deny-commands = "<deny-commands-regex>"
   deny-configuration-regexps = "<deny-configuration-regex>"
}
```

This **service** statement can appear in a **user** or **group** statement.

Example: Configuring a TACACS+ Server for System Authentication

This example shows how to configure a TACACS+ server for system authentication.

Requirements

Before you begin:

- Perform the initial device configuration. See the Getting Started Guide for your device.
- Configure at least one TACACS+ server.

Overview

In this example, you set the IP address to 172.16.98.24 and the shared secret password of the TACACS+ server to Tacacssecret1. The secret password is stored as an encrypted value in the configuration database. You then set the loopback source address as 10.0.0.1

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system tacplus-server address 172.16.98.24
set system tacplus-server 172.16.98.24 secret Tacacssecret1
set system tacplus-server 172.16.98.24 source-address 10.0.0.1
```

GUI Step-by-Step Procedure

To configure a TACACS+ server for system authentication:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Authentication Method and Order** tab.
4. In the TACACS section, click **Add**. The Add TACACS Server dialog box appears.
5. In the IP Address box, type the server's 32–bit IP address.
6. In the Password and Confirm Password boxes, type the secret password for the server and verify your entry.
7. In the Server Port box, type the appropriate port.
8. In the Source Address box, type the locally configured interface address, which is used as the source address for TACACS+ packets.

NOTE: The Source Address box can accept either a hostname or an IP address.

9. In the Retry Attempts box, specify the number of times that the server should try to verify the user's credentials.

10. In the Time Out box, specify the amount of time (in seconds) the device should wait for a response from the server.

11. Click **OK** to check your configuration and save it as a candidate configuration.

12. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a TACACS+ server for system authentication:

1. Add a new TACACS+ server and set its IP address.

```
[edit system]
user@host# set tacplus-server address 172.16.98.24
```

2. Specify the shared secret (password) of the TACACS+ server.

```
[edit system]
user@host# set tacplus-server 172.16.98.24 secret Tacacssecret1
```

3. Specify the device's loopback address as the source address.

```
[edit system]
user@host# set tacplus-server 172.16.98.24 source-address 10.0.0.1
```

Results

From configuration mode, confirm your configuration by entering the **show system tacplus-server** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system tacplus-server
tacplus-server 172.16.98.24 {
   secret Tacacssecret1;
```

```
    source-address 10.0.0.1;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

NOTE: To completely set up TACACS+ authentication, you must create user template accounts and specify a system authentication order. Do one of the following tasks:

- Configure a system authentication order. See "Example: Configuring Authentication Order" on page 177.
- Configure a user. See "Example: Configuring New Users" on page 70.
- Configure local user template accounts. See "Example: Creating Template Accounts" on page 165.

Verification

Confirm that the configuration is working properly.

Verifying the TACACS+ Server System Authentication Configuration

Purpose Verify that the TACACS+ server has been configured for system authentication.

Action From configuration mode, enter the **show system tacplus-server** command.

See Also

- Junos OS User Authentication Methods on page 161
- Junos OS User Accounts Overview on page 67
- Configuring Local User Template Accounts for User Authentication on page 162

Configuring Periodic Refresh of the TACACS+ Authorization Profile

When you configure a Junos device to use a TACACS+ server for authentication, the device prompts users for login information, which is verified by the TACACS+ server. After the user is successfully authenticated, the JUNOS device sends an authorization request to the TACACS+ server to obtain the authorization profile for the user. Authorization profiles specify the access permissions for authenticated users or devices.

The TACACS+ server sends the authorization profile as part of an authorization response message. The remote user configured on the TACACS+ server is mapped to a local user configured on the JUNOS device. The JUNOS device combines the remote authorization profile with the locally-configured authorization profile for the user, which is configured at the [**edit system login class**] hierarchy level.

The exchange of authorization request and response messages occurs only once, after successful authentication, by default. You can configure the JUNOS device to periodically fetch the remote authorization profile from the TACACS+ server and refresh the authorization profile stored locally. This ensures that any change in the authorization parameters are reflected on the local device without the user having to restart the authentication process.

To enable periodic refresh of the authorization profile, you must set the time interval at which the JUNOS device checks the authorization profile configured remotely on the TACACS+ server. If there is a change in the remote authorization profile, the device fetches the authorization profile from the TACACS+ server and the authorization profile configured under the login class hierarchy. The device refreshes the authorization profile stored locally by combining the remote and locally-configured authorization profiles.

The time interval can be configured directly on the TACACS+ server or locally on the JUNOS device using the CLI. The time interval is configured in minutes, in the range of 15 to 1440 minutes.

- To configure periodic refresh of the authorization profile on the local device using the CLI, include the **authorization-time-interval** statement at the **[edit system tacplus-options]** hierarchy level:

  ```
  [edit system tacplus-options]
  authorization-time-interval [minutes];
  ```

- To configure the time interval for periodic refresh on the TACACS+ server, add the time interval as a parameter in the authorization profile using the following syntax:

  ```
  refresh-time-interval=minutes
  ```

Use the following guidelines to determine which time interval configuration takes precedence:

- If there is no refresh time interval configured on the TACACS server for periodic refresh, the JUNOS device does not receive the time interval value in the authorization response. In this case, the value configured locally on the JUNOS device will take effect.
- If the refresh time interval is configured on the TACACS server and there is no refresh time interval configured locally on the JUNOS device, the value configured on the TACACS server will take effect.
- If refresh time interval is configured on the TACACS server and also on the JUNOS device locally, the value configured on the TACACS server will take precedence.
- If there is no refresh time interval configured on the TACACS server and there is no refresh time interval configured on the JUNOS device, there will be no periodic refresh.
- If the refresh time interval configured on the TACACS server is out of range or invalid, the refresh time interval value configured locally will take effect.
- If the refresh time interval configured on the TACACS server is out of range or invalid and there is no refresh time interval configured locally, there will be no periodic refresh.

After the periodic refresh time interval is set, if the user changes the refresh interval before the authorization request is sent from the JUNOS device, the updated refresh interval takes effect after the next immediate periodic refresh.

See Also

- Defining Junos OS Login Classes on page 53
- authorization-time-interval on page 905

Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands

Use regular expressions to specify which operational or configuration mode commands are allowed or denied when you use a RADIUS or TACACS+ server for user authentication. You can specify the regular expressions using the appropriate Juniper Networks vendor-specific RADIUS or TACACS+ attributes in your authentication server configuration.

The following attributes are supported for configuring authorizations on RADIUS and TACACS+ servers:

- **user-permissions**
- **allow-configuration**
- **deny-configuration**
- **allow-commands**
- **deny-commands**
- **allow-configuration-regexp**
- **deny-configuration-regexp**
- (TACACS+ only) **allow-commands-regexp**
- (TACACS+ only) **deny-commands-regexp**

You can specify **allow-configuration**, **deny-configuration**, **allow-commands**, or **deny-commands** in a single extended regular expression, enclosing multiple commands in parentheses and separating them using the pipe symbol. For example, you can specify multiple **allow-commands** parameters using: **allow-commands= (cmd1 | cmd2 | cmd*n*)**. You can specify **user-permissions** as a list of comma-separated values, and not as a regular expression.

To configure authorizations using the **allow/deny-configuration-regexps** or **allow/deny-commands-regexps** attributes, you configure a set of strings in which each string is a regular expression, enclosed in double quotes and separated with a space operator. For example, you can specify multiple parameters for **allow-commands-regexp** using the following syntax: **allow-commands-regexps = (“*regexp1*” “*regexp2*”...)**.

On a RADIUS or TACACS+ server, you can also use a simplified version for regular expressions where you specify each individual expression on a separate line. The simplified version is valid for **allow-commands**, **deny-commands**, **allow-configuration**, **deny-configuration**, and **permissions** vendor-specific attributes.

For a RADIUS server, specify the individual regular expressions using the following syntax:

```
Juniper-Allow-Commands+="cmd1"
Juniper-Allow-Commands+="cmd2"
Juniper-Allow-Commands+="cmdn"
Juniper-Deny-Commands+="cmd1"
Juniper-Deny-Commands+="cmd2"
Juniper-Deny-Commands+="cmdn"
Juniper-Allow-Configuration+="regex1"
Juniper-Allow-Configuration+="regex2"
Juniper-Allow-Configuration+="regexn"
Juniper-Deny-Configuration+="regex1"
Juniper-Deny-Configuration+="regex2"
Juniper-Deny-Configuration+="regexn"
Juniper-User-Permissions+="permission-flag1"
Juniper-User-Permissions+="permission-flag2"
Juniper-User-Permissions+="permission-flagn"
```

For TACACS+ server, specify the individual regular expressions using the following syntax:

```
allow-commands1="cmd1"
allow-commands2="cmd2"
allow-commandsn="cmdn"
deny-commands1="cmd1"
deny-commands2="cmd2"
deny-commandsn="cmdn"
allow-configuration1="regex1"
allow-configuration2="regex2"
allow-configurationn="regexn"
deny-configuration1="regex1"
deny-configuration2="regex2"
deny-configurationn="regexn"
user-permissions1="permission-flag1"
user-permissions2="permission-flag2"
user-permissionsn="permission-flagn "
```

NOTE:

- Numeric values 1 to *n* in the syntax (for TACACS+ server) must be unique but need not be sequential. For example, the following syntax is valid:

```
allow-commands1="cmd1"
allow-commands3="cmd3"
allow-commands2="cmd2"
deny-commands3="cmd3"
deny-commands2="cmd2"
deny-commands1="cmd1"
```

- The limit on the number of lines of individual regular expressions is imposed by the TACACS+ or RADIUS server.
- When you issue the **show cli authorization** command, the command output displays the regular expression in a single line, even if you specify each individual expression on a separate line.

For more information about Juniper Networks vendor-specific RADIUS and TACACS+ attributes, see "Juniper Networks Vendor-Specific RADIUS Attributes" on page 194 and "Juniper Networks Vendor-Specific TACACS+ Attributes" on page 217.

NOTE: When RADIUS or TACACS+ authentication is configured for a router, regular expressions configured on the RADIUS or TACACS+ server merge with any regular expressions configured on the local router at the **[edit system login class]** hierarchy level using the **allow-commands**, **deny-commands**, **allow-configuration**, **deny-configuration**, or **permissions** statements. If the final expression has a syntax error, the overall result is an invalid regular expression.

See Also

- Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 169

Juniper Networks Vendor-Specific TACACS+ Attributes

Junos OS supports the configuration of Juniper Networks TACACS+ vendor-specific attributes (VSAs). These VSAs are encapsulated in a TACACS+ vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. Table 16 on page 217 lists the Juniper Networks VSAs you can configure.

Table 16: Juniper Networks Vendor-Specific TACACS+ Attributes

Name	Description	Length	String
local-user-name	Indicates the name of the user template used by this user when logging in to a device.	≥3	One or more octets containing printable ASCII characters.

Table 16: Juniper Networks Vendor-Specific TACACS+ Attributes (continued)

Name	Description	Length	String
allow-commands	Contains an extended regular expression that enables the user to run operational mode commands in addition to those commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 99.
allow-configuration	Contains an extended regular expression that enables the user to run configuration mode commands in addition to those commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 99.
deny-commands	Contains an extended regular expression that denies the user permission to run operational mode commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 99.
deny-configuration	Contains an extended regular expression that denies the user permission to run configuration mode commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 99.

Table 16: Juniper Networks Vendor-Specific TACACS+ Attributes (continued)

Name	Description	Length	String
user-permissions	Contains information the server uses to specify user permissions. NOTE: When the **user-permissions** attribute is configured to grant the Junos OS **maintenance** or **all** permissions on an IPv4 or IPv6 TACACS+ server, the UNIX wheel group membership is not automatically added to a user's list of group memberships. Some operations such as running the **su root** command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions **maintenance** or **all**, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account.	≥3	One or more octets containing printable ASCII characters. See "Understanding Junos OS Access Privilege Levels" on page 90.
authentication-type	Indicates the authentication method (local database, or TACACS+ server) used to authenticate a user. If the user is authenticated using a local database, the attribute value shows 'local'. If the user is authenticated using TACACS+ server, the attribute value shows 'remote'.	≥5	One or more octets containing printable ASCII characters.
session-port	Indicates the source port number of the established session.	size of integer	Integer

Configuring TACACS+ System Accounting

You can use TACACS+ to track and log software logins, configuration changes, and interactive commands. To audit these events, include the following statements at the **[edit system accounting]** hierarchy level:

```
[edit system accounting]
events [ events ];
destination {
  tacplus {
    server {
      server-address {
        port port-number;
        routing-instance routing-instance;
        secret password;
        single-connection;
        timeout seconds;
      }
    }
  }
}
```

Tasks for configuring TACACS+ system accounting are:

1. Specifying TACACS+ Auditing and Accounting Events on page 220
2. Configuring TACACS+ Server Accounting on page 220
3. Configuring TACACS+ To Use the Management Instance on page 222
4. Configuring TACACS+ Accounting on a TX Matrix Router on page 222

Specifying TACACS+ Auditing and Accounting Events

To specify the events you want to audit when using a TACACS+ server for authentication, include the **events** statement at the **[edit system accounting]** hierarchy level:

```
[edit system accounting]
events [ events ];
```

events is one or more of the following:

- **login**—Audit logins
- **change-log**—Audit configuration changes
- **interactive-commands**—Audit interactive commands (any command-line input)

Configuring TACACS+ Server Accounting

To configure TACACS+ server accounting, include the **server** statement at the **[edit system accounting destination tacplus]** hierarchy level:

```
[edit system accounting destination tacplus]
server {
  server-address {
    port port-number;
    routing-instance routing-instance;
    secret password;
    single-connection;
    timeout seconds;
  }
}
```

server-address specifies the address of the TACACS+ server. To configure multiple TACACS+ servers, include multiple **server** statements.

NOTE: If no TACACS+ servers are configured at the **[edit system accounting destination tacplus]** statement hierarchy level, the Junos OS uses the TACACS+ servers configured at the **[edit system tacplus-server]** hierarchy level.

We recommend that you add the following configuration at the **[edit system accounting destination tacplus]** statement hierarchy level to identify a destination and help avoid generating an error condition:

```
accounting {
    events [ login change-log interactive-commands ];
    destination {
        tacplus;
    }
}
```

port-number specifies the TACACS+ server port number.

routing-instance *routing-instance* is the name of the routing instance used to send and receive TACACS+ packets. By default, Junos OS routes authentication, authorization, and accounting packets for TACACS+ through the default routing instance. Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support routing TACACS+ packets through a management interface in a non-default VRF instance named mgmt_junos. For more information on this VRF management instance, see "Configuring TACACS+ To Use the Management Instance" on page 222. Starting in Junos OS Release 18.2R1, you can route TACACS+ traffic through any routing instance you configure in accounting.

You must specify a secret (password) that the local router or switch passes to the TACACS+ client by including the **secret** statement. If the password contains spaces, enclose the entire password in quotation marks (" "). The password used by the local router or switch must match that used by the server.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a TACACS+ server by including the **timeout** statement. By default, the router or switch waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds.

Optionally, you can maintain one open TCP connection to the server for multiple requests, rather than opening a connection for each connection attempt, by including the **single-connection** statement.

To ensure that start and stop requests for accounting of login events are correctly logged in the Accounting file instead of the Administration log file on a TACACS+ server, include either the **no-cmd-attribute-value** statement or the **exclude-cmd-attribute** at the **[edit system tacplus-options]** hierarchy level.

If you use the **no-cmd-attribute-value** statement, the value of the **cmd** attribute is set to a null string in the start and stop requests. If you use the **exclude-cmd-attribute** statement,

the **cmd** attribute is totally excluded from the start and stop requests. Both statements support the correct logging of accounting requests in the Accounting file, instead of the Administration file.

```
[edit system tacplus-options]
(no-cmd-attribute-value | exclude-cmd-attribute);
```

Configuring TACACS+ To Use the Management Instance

By default, Junos OS routes authentication, authorization, and accounting packets for TACACS+ through the default routing instance. Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support a management interface in a non-default VRF instance.

```
[edit system accounting destination tacplus]
server {
   server-address {
      routing-instance routing-instance;
   }
}
```

When the **routing-instance mgmt_junos** option is configured in both the **tacplus-server** ***server-address*** and the **tacplus server** ***server-ip*** statements, provided the **management-instance** statement is also configured, TACACS+ packets are routed through the management instance mgmt_junos.

NOTE: The **routing-instance mgmt_junos** option must be configured in both the **tacplus-server** and the **tacplus server** statements. If not, even if the **management-instance** statement is set, TACACS+ packets will still be sent using the default routing instance only.

For more details on this management instance, see *management-instance*.

Configuring TACACS+ Accounting on a TX Matrix Router

On a TX Matrix router, TACACS+ accounting should be configured only under the groups **re0** and **re1**.

NOTE: Accounting should *not* be configured at the **[edit system]** hierarchy; on a TX Matrix router, control is done under the switch-card chassis only.

Release History Table

Release	Description
18.2R1	Starting in Junos OS Release 18.2R1, you can route TACACS+ traffic through any routing instance you configure in authentication.
18.2R1	Starting in Junos OS Release 18.2R1, you can route TACACS+ traffic through any routing instance you configure in accounting.
17.4R1	Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support routing TACACS+ packets through a management interface in a non-default VRF instance named mgmt_junos.
17.4R1	Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support a management interface in a non-default VRF instance.
17.4R1	Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support routing TACACS+ packets through a management interface in a non-default VRF instance named mgmt_junos.
17.4R1	Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support a management interface in a non-default VRF instance.

Related Documentation

- Junos OS User Authentication Overview on page 161
- Authentication Order for RADIUS, TACACS+, and Local Password on page 169
- RADIUS Authentication on page 182

Authentication for Routing Protocols

You can configure an authentication method and password for routing protocol messages for IGPs, IS-IS, OSPF, and RIP, and RSVP. To prevent exchange of unauthenticated or forged packets, routers must ensure that they form routing protocol relationships (peering or neighboring relationships) to trusted peers. One way of doing this is by authenticating routing protocol messages. Neighboring routers use the password to verify the authenticity of packets sent by the protocol from the router or from a router interface. Read this topic for more information.

- Junos OS Authentication Methods for Routing Protocols on page 223
- Example: Configuring the Authentication Key for BGP and IS-IS Routing Protocols on page 224
- Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols on page 226

Junos OS Authentication Methods for Routing Protocols

Some interior gateway protocols (IGPs)—Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP)—and Resource Reservation Protocol (RSVP) allow you to configure an authentication method and password. Neighboring routers use the password to verify the authenticity of packets

sent by the protocol from the router or from a router interface. The following authentication methods are supported:

- Simple authentication (IS-IS, OSPF, and RIP)—Uses a simple text password. The receiving router uses an authentication key (password) to verify the packet. Because the password is included in the transmitted packet, this method of authentication is relatively insecure. We recommend that you not use this authentication method.
- MD5 and HMAC-MD5 (IS-IS, OSPF, RIP, and RSVP)—Message Digest 5 (MD5) creates an encoded checksum that is included in the transmitted packet. HMAC-MD5, which combines HMAC authentication with MD5, adds the use of an iterated cryptographic hash function. With both types of authentication, the receiving router uses an authentication key (password) to verify the packet. HMAC-MD5 authentication is defined in RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*.

In general, authentication passwords are text strings consisting of a maximum of 16 or 255 letters and digits. Characters can include any ASCII strings. If you include spaces in a password, enclose all characters in quotation marks (" ").

Junos-FIPS has special password requirements. FIPS passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If Junos-FIPS is installed on the router, you cannot configure passwords unless they meet this standard.

Example: Configuring the Authentication Key for BGP and IS-IS Routing Protocols

The main task of a router is to use its routing and forwarding tables to forward user traffic to its intended destination. Attackers can send forged routing protocol packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which in turn can degrade the functionality of the router and the network. To prevent such attacks, routers must ensure that they form routing protocol relationships (peering or neighboring relationships) to trusted peers. One way of doing this is by authenticating routing protocol messages. We strongly recommend using authentication when configuring routing protocols. The Junos OS supports HMAC-MD5 authentication for BGP, Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), and Resource Reservation Protocol (RSVP). HMAC-MD5 uses a secret key that is combined with the data being transmitted to compute a hash. The computed hash is transmitted along with the data. The receiver uses the matching key to recompute and validate the message hash. If an attacker has forged or modified the message, the hash will not match and the data will be discarded.

In the following examples, we configure BGP as the exterior gateway protocol (EGP) and IS-IS as the interior gateway protocol (IGP). If you use OSPF, configure it similarly to the IS-IS configuration shown.

Configuring BGP

The following example shows the configuration of a single authentication key for the BGP peer group internal peers. You can also configure BGP authentication at the neighbor or routing instance levels, or for all BGP sessions. As with any security configuration, there is a trade-off between the degree of granularity (and to some extent the degree of

security) and the amount of management necessary to maintain the system. This example also configures a number of tracing options for routing protocol events and errors, which can be good indicators of attacks against routing protocols. These events include protocol authentication failures, which might point to an attacker that is sending spoofed or otherwise malformed routing packets to the router in an attempt to elicit a particular behavior.

```
[edit]
protocols {
   bgp {
      group ibgp {
         type internal;
         traceoptions {
            file bgp-trace size 1m files 10;
            flag state;
            flag general;
         }
         local-address 10.10.5.1;
         log-updown;
         neighbor 10.2.1.1;
         authentication-key "$9$aH1j8gqQ1gjyjgjhgjgiiii";
      }
      group ebgp {
         type external;
         traceoptions {
            file ebgp-trace size 10m files 10;
            flag state;
            flag general;
         }
         local-address 10.10.5.1;
         log-updown;
         peer-as 2;
         neighbor 10.2.1.2;
         authentication-key "$9$aH1j8gqQ1gjyjgjhgjgiiii";
      }
   }
}
```

Configuring IS-IS

Although all IGPs supported by the Junos OS support authentication, some are inherently more secure than others. Most service providers use OSPF or IS-IS to allow fast internal convergence and scalability and to use traffic engineering capabilities with Multiprotocol Label Switching (MPLS). Because IS-IS does not operate at the network layer, it is more difficult to spoof than OSPF, which is encapsulated in IP and is therefore subject to remote spoofing and DoS attacks.

The following example also shows how to configure a number of tracing options for routing protocol events and errors, which can be good indicators of attacks against routing protocols. These events include protocol authentication failures, which might point to an attacker that is sending spoofed or otherwise malformed routing packets to the router in an attempt to elicit a particular behavior.

```
[edit]
protocols {
   isis {
      authentication-key "$9$aH1j8gqQ1gjyjgjhgjgiiiii"; # SECRET-DATA
      authentication-type md5;
      traceoptions {
         file isis-trace size 10m files 10;
         flag normal;
         flag error;
      }
      interface at-0/0/0.131 {
         lsp-interval 50;
         level 2 disable;
         level 1 {
            metric 3;
            hello-interval 5;
            hold-time 60;
         }
      }
      interface lo0.0 {
         passive;
      }
   }
}
```

Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols

You can configure an authentication key update mechanism for the Border Gateway Protocol (BGP) and Label Distribution Protocol (LDP) routing protocols. This mechanism allows you to update authentication keys without interrupting associated routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).

To configure this feature, include the **authentication-key-chains** statement at the **[edit security]** level, and include the **authentication-algorithm** *algorithm* and **authentication-key-chain** statements for the BGP or LDP routing protocols at the **[edit protocols]** level .

The following topics provide more details about configuring authentication key updates for BGP and LDP Routing Protocols:

- Configuring Authentication Key Updates on page 226
- Configuring BGP and LDP for Authentication Key Updates on page 227

Configuring Authentication Key Updates

To configure the authentication key update mechanism, include the **key-chain** statement at the **[edit security authentication-key-chains]** hierarchy level, and specify the **key** option to create a keychain consisting of several authentication keys.

```
[edit security authentication-key-chains]
key-chain key-chain-name {
```

```
    key key {
        secret secret-data;
        start-time yyyy-mm-dd.hh:mm:ss;
    }
}
```

key-chain—Assigns a name to the keychain mechanism. This name is also configured at the **[edit protocols bgp]** or the **[edit protocols ldp]** hierarchy levels to associate unique **authentication key-chain** attributes as specified using the following options:

- **key**—Each key within a keychain is identified by a unique integer value. The range is from 0 through 63.
- **secret**—Each key must specify a secret in encrypted text or plain text format. Even if you enter the secret data in plain-text format, the secret always appears in encrypted format.
- **start-time**—Start times for authentication key updates are specified in UTC (Coordinated Universal Time), and must be unique within the keychain.

Configuring BGP and LDP for Authentication Key Updates

To configure the authentication key update mechanism for the BGP and LDP routing protocols, include the **authentication-key-chain** statement at the **[edit protocols (bgp | ldp)]** hierarchy level to associate each routing protocol with the **[edit security authentication-key-chains]** authentication keys. You must also configure the **authentication-algorithm *algorithm*** statement at the **[edit protocols (bgp | ldp)]** hierarchy level.

```
[edit protocols (bgp | ldp)]
group group-name {
    neighbor address {
        authentication-algorithm algorithm;
        authentication-key-chain key-chain-name;
    }
}
```

NOTE: When configuring the authentication key update mechanism for BGP, you cannot commit the 0.0.0.0/allow statement with authentication keys or key chains. The CLI issues a warning and fails to commit such configurations.

For information about the BGP protocol, see the *Junos OS Routing Protocols Library*.

Related Documentation

- *authentication-algorithm*
- *authentication-key-chain* (Protocols BGP and BMP)
- *authentication-key-chain* (Protocol LDP)

CHAPTER 5

Remote Access Management

Remote Access Overview

You can access a router, switch, or security device remotely using DHCP, Finger, FTP, rlogin, SSH, and Telnet services and so on. This topic shows you how to configure remote access using Telnet, SSH, FTP, and Finger services. Read this topic for more information.

System Services Overview

For security reasons, remote access to the router is disabled by default. You must configure the router explicitly so that users on remote systems can access it. The router can be accessed from a remote system by means of the DHCP, finger, FTP, rlogin, SSH, and Telnet services. In addition, Junos XML protocol client applications can use Secure Sockets Layer (SSL) or the Junos XML protocol-specific clear-text service, among other services.

NOTE: To protect system resources, you can limit the number of simultaneous connections that a service accepts and the number of processes owned by a single user. If either limit is exceeded, connection attempts fail.

See Also

- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*
- DHCP Access Service Overview on page 542
- Configuring the Router as an Extended DHCP Local Server on page 567
- Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools on page 569
- *Configuring DTCP-over-SSH Service for the Flow-Tap Application*
- Configuring TACACS+ System Accounting on page 219

Configuring Telnet Service for Remote Access to a Router or Switch

To configure the router or switch to accept Telnet as an access service, include the **telnet** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
telnet {
  connection-limit limit;
  rate-limit limit;
}
```

By default, the router or switch supports a limited number of simultaneous Telnet sessions and connection attempts per minute.

Optionally, you can include either or both of the following statements to change the defaults:

- **connection-limit** *limit*—Maximum number of simultaneous connections per protocol (IPV4 and IPv6). The range is from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of telnet sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 telnet sessions and 10 IPv4 telnet sessions.
- **rate-limit** *limit*—Maximum number of connection attempts accepted per minute (from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 telnet session connection attempts per minute and 10 IPv4 telnet session connection attempts per minute.

You cannot include the **telnet** statement on devices that run the Junos-FIPS software. We recommend that you do not use Telnet in a Common Criteria environment.

See Also

- telnet on page 1531

Configuring FTP Service for Remote Access to the Router or Switch

To configure the router or switch to accept FTP as an access service, include the **ftp** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
ftp {
  connection-limit limit;
  rate-limit limit;
}
```

By default, the router or switch supports a limited number of simultaneous FTP sessions and connection attempts per minute. You can include either or both of the following statements to change the defaults:

- **connection-limit** *limit*—Maximum number of simultaneous connections per protocol (IPV4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 FTP sessions and 10 IPv4 FTP sessions.
- **rate-limit** *limit*—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150.When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 FTP session connection attempts and 10 IPv4 FTP session connection attempts.

You can use passive FTP to access devices that accept only passive FTP services. All commands and statements that use FTP also accept passive FTP. Include the **ftp** statement at the **[edit system services]** hierarchy level to use either active FTP or passive FTP.

To start a passive FTP session, use **pasvftp** (instead of **ftp**) in the standard FTP format (**ftp://*destination***). For example:

```
request system software add pasvftp://name.com/jinstall.tgz
```

You cannot include the **ftp** statement on routers or switches that run the Junos-FIPS software. We recommend that you do not use the finger service in a Common Criteria environment.

Configuring Finger Service for Remote Access to the Router

To configure the router to accept finger as an access service, include the **finger** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
finger {
  connection-limit limit;
  rate-limit limit;
}
```

By default, the router supports a limited number of simultaneous finger sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- **connection-limit** *limit*—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 clear-text service sessions and 10 IPv4 clear-text service sessions
- **rate-limit** *limit*—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 session connection attempts per minute and 10 IPv4 session connection attempts per minute.

You cannot include the **finger** statement on routers that run the Junos-FIPS software. We recommend that you do not use the finger service in a Common Criteria environment.

Configuring SSH Service for Remote Access to the Router or Switch

To configure the router or switch to accept SSH as an access service, include the **ssh** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
ssh {
  authentication-order [method 1 method2...];
  ciphers [ cipher-1 cipher-2 cipher-3 ...];
  client-alive-count-max seconds;
  client-alive-interval seconds;
  connection-limit limit;
  fingerprint-hash (md5 | sha2-256);
  hostkey-algorithm (algorithm | no-algorithm);
  key-exchange [algorithm1 algorithm2...];
  macs [algorithm1 algorithm2...];
  max-sessions-per-connection <number>;
  no-passwords;
  no-public-keys;
  no-tcp-forwarding;
  protocol-version [v2];
  rate-limit limit;
  root-login (allow | deny | deny-password);
  }
}
```

By default, the router or switch supports a limited number of simultaneous SSH sessions and connection attempts per minute. Use the following statements to change the defaults:

- **connection-limit** ***limit***—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of SSH sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 SSH sessions and 10 IPv4 SSH sessions.
- **max-sessions-per-connection** ***number***—Include this statement to specify the maximum number of SSH sessions allowed per single SSH connection. This allows you to limit the number of cloned sessions tunneled within a single SSH connection. The default value is 10.
- **rate-limit** ***limit***—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 SSH session connection attempts per minute and 10 IPv4 SSH session connection attempts per minute.
- **data-limit**—Data limit before renegotiating session keys (bytes)
- **time-limit**—Time limit before renegotiating session keys (minutes)

By default, a user can create an SSH tunnel over a CLI session to a router running Junos OS via SSH. This type of tunnel could be used to forward TCP traffic, bypassing any firewall filters or access control lists allowing access to resources beyond the router. Use the **no-tcp-forwarding** option to prevent a user from creating an SSH tunnel to a router via SSH.

For information about other configuration settings, see the following topics:

- Configuring the Root Login Through SSH on page 233
- Configuring the SSH Protocol Version on page 234
- Configuring the Client Alive Mechanism on page 234
- Configuring the SSH Fingerprint Hash Algorithm on page 234

Configuring the Root Login Through SSH

By default, users are allowed to log in to the router or switch as **root** through SSH when the authentication method does not require a password. To control user access through SSH, include the **root-login** statement at the **[edit systems services ssh]** hierarchy level:

```
[edit system services ssh]
root-login (allow | deny | deny-password);
```

allow—Allows users to log in to the router or switch as root through SSH.

deny—Disables users from logging in to the router or switch as root through SSH.

deny-password—Allows users to log in to the router or switch as root through SSH when the authentication method (for example, RSA) does not require a password.

The default is **deny-password**.

Configuring the SSH Protocol Version

By default, only version 2 of the SSH protocol is enabled.

To configure the router or switch to use version 2 of the SSH protocol, include the **protocol-version** statement and specify **v2** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
protocol-version [ v2 ];
```

Systems in FIPS mode always use SSH protocol version **v2**.

Configuring the Client Alive Mechanism

The client alive mechanism is valuable when the client or server depends on knowing when a connection has become inactive. It differs from the standard keepalive mechanism because the client alive messages are sent through the encrypted channel. The client alive mechanism is not enabled at default. To enable it, configure the **client-alive-count-max** and **client-alive-interval** statements. This option applies to SSH protocol version 2 only.

In the following example, unresponsive SSH clients will be disconnected after approximately 100 seconds (20 x 5).

```
[edit system services ssh]
client-alive-count-max 5;
client-alive-interval 20;
```

See Also

- ssh on page 1495

Configuring the SSH Fingerprint Hash Algorithm

To configure the hash algorithm used by the SSH server when it displays key fingerprints, include the **fingerprint-hash** statement and specify **md5** or **sha2-256** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
fingerprint-hash (md5 | sha2-256);
```

The **md5** hash algorithm is unavailable on systems in FIPS mode.

See Also

- ssh on page 1495

The telnet Command

You can use the CLI **telnet** command to open a Telnet session to a remote device:

```
user@host> telnet host <8bit> <bypass-routing> <inet> <interface interface-name>
<no-resolve> <port port> <routing-instance routing-instance-name> <source address>
```

NOTE: On SRX100, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, and SRX1500 devices, the maximum number of concurrent Telnet sessions is indicated in the following table. Platform support depends on the Junos OS release in your installation.

SRX100	SRX210 SRX220	SRX240	SRX300 SRX320 SRX340	SRX345	SRX1500
3	*3*	*5*	*3*	*5*	*5*

To exit the Telnet session and return to the Telnet command prompt, press Ctrl-].

To exit the Telnet session and return to the CLI command prompt, enter **quit**.

Table 17 on page 235 describes the **telnet** command options.

Table 17: CLI telnet Command Options

Option	Description
8bit	Use an 8-bit data path.
bypass-routing	Bypass the routing tables and open a Telnet session only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.
host	Open a Telnet session to the specified hostname or IP address.
inet	Force the Telnet session to an IPv4 destination.
interface ***source-interface***	Open a Telnet session to a host on the specified interface. If you do not include this option, all interfaces are used.
no-resolve	Suppress the display of symbolic names.
port ***port***	Specify the port number or service name on the host.
routing-instance ***routing-instance-name***	Use the specified routing instance for the Telnet session.
source ***address***	Use the specified source address for the Telnet session.

The ssh Command

You can use the CLI **ssh** command to use the secure shell (SSH) program to open a connection to a remote device:

```
user@host> ssh host <bypass-routing> <inet> <interface interface-name>
<routing-instance routing-instance-name> <source address> <v1> <v2>
```

NOTE: On SRX100, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, and SRX1500 devices, the maximum number of concurrent SSH sessions is indicated in the following table. Platform support depends on the Junos OS release in your installation.

SRX100	SRX210 SRX220	SRX240	SRX300 SRX320 SRX340	SRX345	SRX1500
3	*3*	*5*	*3*	*5*	*5*

Table 18 on page 236 describes the **ssh** command options.

Table 18: CLI ssh Command Options

Option	Description
bypass-routing	Bypass the routing tables and open an SSH connection only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.
host	Open an SSH connection to the specified hostname or IP address.
inet	Force the SSH connection to an IPv4 destination.
interface ***source-interface***	Open an SSH connection to a host on the specified interface. If you do not include this option, all interfaces are used.
routing-instance ***routing-instance-name***	Use the specified routing instance for the SSH connection.
source ***address***	Use the specified source address for the SSH connection.
v1	Force SSH to use version 1 for the connection.
v2	Force SSH to use version 2 for the connection.

Configuring SSH Host Keys for Secure Copying of Data

Secure Shell (SSH) uses encryption algorithms to generate a host, server, and session key system that ensures secure data transfer. You can configure SSH host keys to support secure copy (SCP) as an alternative to FTP for the background transfer of data such as

configuration archives and event logs. To configure SSH support for SCP, you must complete the following tasks:

- Specify SSH known hosts by including hostnames and host key information in the Routing Engine configuration hierarchy.
- Set an SCP URL to specify the host from which to receive data. Setting this attribute automatically retrieves SSH host key information from the SCP server.
- Verify that the host key is authentic.
- Accept the secure connection. Accepting this connection automatically stores host key information in the local host key database. Storing host key information in the configuration hierarchy automates the secure handshake and allows background data transfer using SCP.

Tasks to configure SSH host keys for secure copying of data are:

1. Configuring SSH Known Hosts on page 237
2. Configuring Support for SCP File Transfer on page 238
3. Updating SSH Host Key Information on page 238

Configuring SSH Known Hosts

To configure SSH known hosts, include the **host** statement, and specify hostname and host key options for trusted servers at the **[edit security ssh-known-hosts]** hierarchy level:

```
[edit security ssh-known-hosts]
host corporate-archive-server, ip-address {
   dsa-key key;
}
host archive-server-url {
   rsa-key key;
}
host server-with-ssh-version-1, ip-address {
   rsa1-key key;
}
```

Host keys are one of the following:

- **dsa-key** ***key***—Base64 encoded Digital Signature Algorithm (DSA) key for SSH version 2.
- **ecdsa-sha2-nistp256-key** *key*—Base64 encoded ECDSA-SHA2-NIST256 key.
- **ecdsa-sha2-nistp384-key** *key*—Base64 encoded ECDSA-SHA2-NIST384 key.
- **ecdsa-sha2-nistp521-key** *key*—Base64 encoded ECDSA-SHA2-NIST521 key.
- **ed25519-key** *key*—Base64 encoded ED25519 key.
- **rsa-key** ***key***—Base64 encoded public key algorithm that supports encryption and digital signatures for SSH version 1 and SSH version 2.
- **rsa1-key** ***key***—Base64 encoded RSA public key algorithm, which supports encryption and digital signatures for SSH version 1.

Starting in Junos OS Release 18.3R1, the **ssh-dss** and **ssh-dsa** hostkey algorithms are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Configuring Support for SCP File Transfer

To configure a known host to support background SCP file transfers, include the **archive-sites** statement at the **[edit system archival configuration]** hierarchy level.

```
[edit system archival configuration]
archive-sites {
   scp://username<:password>@host<:port>/url-path;
}
```

NOTE: When specifying a URL in a Junos OS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([ ]). For example, “scp://*username*<:*password*>@[*host*]<:*port*>/*url-path*”;

Setting the **archive-sites** statement to point to an SCP URL triggers automatic host key retrieval. At this point, Junos OS connects to the SCP host to fetch the SSH public key, displays the host key message digest or fingerprint as output to the console, and terminates the connection to the server.

```
user@host# set system archival configuration archive-sites “<scp-url-path>”
The authenticity of host <my-archive-server (<server-ip-address>)> can’t be established.
   RSA key fingerprint is <ascii-text key>. Are you sure you want to continue connecting
   (yes/no)?
```

To verify that the host key is authentic, compare this fingerprint with a fingerprint that you obtain from the same host using a trusted source. If the fingerprints are identical, accept the host key by entering **yes** at the prompt. The host key information is then stored in the Routing Engine configuration and supports background data transfers using SCP.

Updating SSH Host Key Information

Typically, SSH host key information is automatically retrieved when you set a URL attribute for SCP using the **archival configuration archive-sites** statement at the **[edit system]** hierarchy level. However, if you need to manually update the host key database, use one of the following methods.

1. Retrieving Host Key Information Manually on page 238
2. Importing Host Key Information from a File on page 239

Retrieving Host Key Information Manually

To manually retrieve SSH public host key information, use the **fetch-from-server** option with the **set security ssh-known-hosts** command. You must include a hostname attribute with the **set security ssh-known-hosts fetch-from-server** command to specify the host from which to retrieve the SSH public key.

```
user@host# set security ssh-known-hosts fetch-from-server <hostname>
```

Importing Host Key Information from a File

To manually import SSH host key information from the known-hosts file located at **/var/tmp/known-hosts** on the server, include the **load-key-file** option with the **set security ssh-known-hosts** command. You must include the path to the **known-hosts** file with the **set security ssh-known-hosts load-key-file** command to specify the location from which to import host key information.

```
user@host# set security ssh-known-hosts load-key-file /var/tmp/known-hosts
```

See Also

- *Importing SSL Certificates for Junos XML Protocol Support*

Configuring the SSH Service to Support Legacy Cryptography

Starting in Junos OS Release 16.1, the SSH server in Junos OS is based on OpenSSH 7 and defaults to a more secure set of ciphers and key-exchange algorithms. OpenSSH 7 omits some legacy cryptography.

NOTE: Lack of support for legacy cryptography in devices causes Junos Space device discovery to fail. To work around this issue, configure the device to support the **3des-cbc** or **blowfish-cbc** cipher, or both, and the **dh-group1-sha1** key-exchange method. This issue does not affect devices running Junos OS with upgraded FreeBSD.

NOTE: See the OpenSSH 7 documentation at https://www.openssh.com/ for more information about these extensions.

Junos OS Release 16.1 supports the following set of ciphers by default:

- **chacha20-poly1305@openssh.com**
- **aes128-ctr**
- **aes192-ctr**
- **aes256-ctr**
- **aes128-gcm@openssh.com**
- **aes256-gcm@openssh.com**

In Junos OS Release 16.1, the following ciphers are not supported by default, but you can configure your device to support them. They are listed from the most secure to the least secure:

- **aes256-cbc**
- **aes192-cbc**
- **aes128-cbc**
- **3des-cbc**
- **blowfish-cbc**
- **cast128-cbc**
- **arcfour256**
- **arcfour128**
- **arcfour**

Junos OS Release 16.1 supports the following set of key-exchange methods by default:

- **curve25519-sha256**
- **ecdh-sha2-nistp256**
- **ecdh-sha2-nistp384**
- **ecdh-sha2-nistp521**
- **group-exchange-sha2**
- **dh-group14-sha1**

In Junos OS Release 16.1, the following key-exchange methods are not supported by default, but you can configure your device to support them:

- **group-exchange-sha1**
- **dh-group1-sha1**

To configure the SSH service to support legacy cryptography:

NOTE: **By configuring an ordered set of ciphers, key-exchange methods, or message authentication codes (MACs), the newly defined set is applied to both server and client commands. Changes to the defaults affect the file copy command when you use Secure Copy Protocol (SCP).**

1. Add support for ciphers by using the **set system services ssh ciphers [*cipher 1 cipher 2 ...*]** command. We recommend that you add the ciphers to the end of the configuration list so that they are among the last options used. In the following example, the **3des-cbc** and **blowfish-cbc** ciphers are added to the default set:

   ```
   [edit system services ssh]
   ```

```
user@device# set ciphers [ chacha20-poly1305@openssh.com aes128-ctr aes192-ctr
  aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com 3des-cbc
  blowfish-cbc ]
```

2. Add support for key-exchange methods by using the **set system services ssh key-exchange [** *method 1 method 2* **...]** command. We recommend that you add the key-exchange methods to the end of the configuration list so that they are among the last options used. In the following example, the **dh-group1-sha1** key-exchange method is added to the default set:

```
[edit system services ssh]
user@device# set key-exchange [ curve25519-sha256 ecdh-sha2-nistp256
  ecdh-sha2-nistp384 ecdh-sha2-nistp521 group-exchange-sha2 dh-group14-sha1
  dh-group1-sha1 ]
```

3. Commit the configuration:

```
[edit]
user@device# commit
```

See Also
- ciphers on page 929
- key-exchange on page 1185
- macs on page 1217

Configuring Outbound SSH Service

You can configure a device running the Junos OS to initiate a TCP/IP connection with a client management application that would be blocked if the client attempted to initiate the connection (for example, if the device is behind a firewall). The **outbound-ssh** command instructs the device to create a TCP/IP connection with the client management application and to forward the identity of the device. Once the connection is established, the management application acts as the client and initiates the SSH sequence, and the device acts as the server and authenticates the client.

NOTE: There is no initiation command with outbound SSH. Once outbound SSH is configured and committed, the device begins to initiate an outbound SSH connection based on the committed configuration. The device repeatedly attempts to create this connection until successful. If the connection between the device and the client management application is dropped, the device again attempts to create a new outbound SSH connection until successful. This connection is maintained until the outbound SSH stanza is removed from the configuration.

To configure the device for outbound SSH connections, include the **outbound-ssh** statement at the **[edit system services]** hierarchy level:

[**edit system services outbound-ssh**]

The following topics describe the tasks for configuring the outbound SSH service:

Configuring the Device Identifier for Outbound SSH Connections

Each time the device establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the device to the management client. Within this transmission is the value of ***device-id***.

To configure the device identifier of the device, include the **device-id** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
device-id device-id;
```

The initiation sequence when **secret** is not configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
```

Sending the Public SSH Host Key to the Outbound SSH Client

Each time the router or switch establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the router or switch to the management client. Within this transmission is the value of *device-id*.

To configure the device identifier of the router or switch, include the **device-id** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
device-id device-id;
```

The initiation sequence when **secret** is not configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
```

During the initialization of an SSH connection, the client authenticates the identity of the device using the public SSH host key of the device. Therefore, before the client can initiate the SSH sequence, it needs the public SSH key of the device. When you configure the

secret statement, the device passes its public SSH key as part of the outbound SSH connection initiation sequence.

When the **secret** statement is set and the device establishes an outbound SSH connection, the device communicates its device ID, its public SSH key, and an SHA1 hash derived in part from the **secret** statement. The value of the **secret** statement is shared between the device and the management client. The client uses the shared secret to authenticate the public SSH host key it is receiving to determine whether the public key is from the device identified by the **device-id** statement.

Using the **secret** statement to transport the public SSH host key is optional. You can manually transport and install the public key onto the client system.

NOTE: Including the secret statement means that the device sends its public SSH host key every time it establishes a connection to the client. It is then up to the client to decide what to do with the SSH host key if it already has one for that device. We recommend that you replace the client's copy with the new key. Host keys can change for various reasons and by replacing the key each time a connection is established, you ensure that the client has the latest key.

To send the router's or switch's public SSH host key when the device connects to the client, include the **secret** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
secret password;
```

The following message is sent by the device when the **secret** attribute is configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
HOST-KEY: <public-hot-key>\r\n
HMAC:<HMAC(pub-SSH-host-key, <secret>>)>\r\n
```

Configuring Keepalive Messages for Outbound SSH Connections

Once the client application has the router's or switch's public SSH host key, it can then initiate the SSH sequence as if it had created the TCP/IP connection and can authenticate the device using its copy of the router's or switch's public host SSH key as part of that sequence. The device authenticates the client user through the mechanisms supported in the Junos OS (RSA/DSA public string or password authentication).

To enable the device to send SSH protocol keepalive messages to the client application, configure the **keep-alive** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
```

```
keep-alive {
   retry number;
   timeout seconds;
}
```

Configuring a New Outbound SSH Connection

When disconnected, the device begins to initiate a new outbound SSH connection. To specify how the device reconnects to the server after a connection is dropped, include the **reconnect-strategy** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client-id]
reconnect-strategy (sticky | in-order);
```

You can also specify the number of retry attempts and set the amount of time before the reconnection attempts stop. See "Configuring Keepalive Messages for Outbound SSH Connections" on page 243.

Configuring the Outbound SSH Client to Accept NETCONF as an Available Service

To configure the application to accept NETCONF as an available service, include the **services netconf** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
services {
   netconf;
}
```

Configuring Outbound SSH Clients

To configure the clients available for this outbound SSH connection, list each client with a separate address statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
   address address {
      retry number;
      timeout seconds;
      port port-number;
   }
```

NOTE: Outbound SSH connections support IPv4 and IPv6 address formats.

Configuring NETCONF-Over-SSH Connections on a Specified TCP Port

The Junos OS enables you to restrict incoming NETCONF connections to a specified TCP port without configuring a firewall. To configure the TCP port used for NETCONF-over-SSH connections, include the **port** statement at the **[edit system services netconf ssh]** hierarchy

level. The configured port accepts only NETCONF-over-SSH sessions. Regular SSH session requests for this port are rejected.

You can either configure the default port 830 for NETCONF connections over SSH, as specified in RFC 4742, *Using the NETCONF Configuration Protocol over Secure Shell (SSH)*, or configure any port from 1 through 65535.

NOTE:

- The default SSH port (22) continues to accept NETCONF sessions even with a configured NETCONF server port. To disable the SSH port from accepting NETCONF sessions, specify this in the login event script.
- We do not recommend configuring the default ports for FTP (21) and Telnet (23) services for configuring NETCONF-over-SSH connections.

See Also

- port (NETCONF) on page 1338

Configuring Password Retry Limits for Telnet and SSH Access

To prevent brute force and dictionary attacks, the device performs the following actions for Telnet or SSH sessions by default:

- Disconnects a session after a maximum of 10 consecutive password retries.
- After the second password retry, introduces a delay in multiples of 5 seconds between subsequent password retries.

  For example, the device introduces a delay of 5 seconds between the third and fourth password retry, a delay of 10 seconds between the fourth and fifth password retry, and so on.
- Enforces a minimum session time of 20 seconds during which a session cannot be disconnected. Configuring the minimum session time prevents malicious users from disconnecting sessions before the password retry delay goes into effect, and attempting brute force and dictionary attacks with multiple logins.

You can configure the password retry limits for Telnet and SSH access. In this example, you configure the device to take the following actions for Telnet and SSH sessions:

- Allow a maximum of four consecutive password retries before disconnecting a session.
- Introduce a delay in multiples of 5 seconds between password retries that occur after the second password retry.
- Enforce a minimum session time of 40 seconds during which a session cannot be disconnected.

To configure password retry limits for Telnet and SSH access:

1. Set the maximum number of consecutive password retries before a Telnet or SSH or telnet session is disconnected. The default number is **10**, but you can set a number from **1** through **10**.

```
[edit system login retry-options]
user@host# set tries-before-disconnect 4
```

2. Set the threshold number of password retries after which a delay is introduced between two consecutive password retries. The default number is **2**, but you can specify a value from **1** through **3**.

```
[edit system login retry-options]
user@host# set backoff-threshold 2
```

3. Set the delay (in seconds) between consecutive password retries after the threshold number of password retries. The default delay is in multiples of **5** seconds, but you can specify a value from **5** through **10** seconds.

```
[edit system login retry-options]
user@host# set backoff-factor 5
```

4. Set the minimum length of time (in seconds) during which a Telnet or SSH session cannot be disconnected. The default is **20** seconds, but you can specify an interval from **20** through **60** seconds.

```
[edit system login retry-options]
user@host# set minimum-time 40
```

5. If you are done configuring the device, enter **commit** from configuration mode.

Example: Configuring a Filter to Block Telnet and SSH Access

Requirements

You must have access to a remote host that has network connectivity with this device.

Overview

In this example, you create an IPv4 stateless firewall filter that logs and rejects Telnet or SSH access packets unless the packet is destined for or originates from the 192.168.1.0/24 subnet.

- To match packets destined for or originating from the **address 192.168.1.0/24** subnet, you use the **source-address 192.168.1.0/24** IPv4 match condition.
- To match packets destined for or originating from a TCP port, Telnet port, or SSH port, you use the **protocol tcp**, **port telnet**, and **telnet ssh** IPv4 match conditions.

Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode*.

To configure this example, perform the following tasks:

- Configure the Stateless Firewall Filter on page 247
- Apply the Firewall Filter to the Loopback Interface on page 248
- Confirm and Commit Your Candidate Configuration on page 248

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set firewall family inet filter local_acl term terminal_access from source-address
  192.168.1.0/24
set firewall family inet filter local_acl term terminal_access from protocol tcp
set firewall family inet filter local_acl term terminal_access from port ssh
set firewall family inet filter local_acl term terminal_access from port telnet
set firewall family inet filter local_acl term terminal_access then accept
set firewall family inet filter local_acl term terminal_access_denied from protocol tcp
set firewall family inet filter local_acl term terminal_access_denied from port ssh
set firewall family inet filter local_acl term terminal_access_denied from port telnet
set firewall family inet filter local_acl term terminal_access_denied then log
set firewall family inet filter local_acl term terminal_access_denied then reject
set firewall family inet filter local_acl term default-term then accept
set interfaces lo0 unit 0 family inet filter input local_acl
set interfaces lo0 unit 0 family inet address 127.0.0.1/32
```

Configure the Stateless Firewall Filter

Step-by-Step Procedure

To configure the stateless firewall filter that selectively blocks Telnet and SSH access:

1. Create the stateless firewall filter **local_acl**.

```
[edit]
```

```
user@myhost# edit firewall family inet filter local_acl
```

2. Define the filter term **terminal_access**.

```
[edit firewall family inet filter local_acl]
user@myhost# set term terminal_access from source-address 192.168.1.0/24
user@myhost# set term terminal_access from protocol tcp
user@myhost# set term terminal_access from port ssh
user@myhost# set term terminal_access from port telnet
user@myhost# set term terminal_access then accept
```

3. Define the filter term **terminal_access_denied**.

```
[edit firewall family inet filter local_acl]
user@myhost# set term terminal_access_denied from protocol tcp
user@myhost# set term terminal_access_denied from port ssh
user@myhost# set term terminal_access_denied from port telnet
user@myhost# set term terminal_access_denied then log
user@myhost# set term terminal_access_denied then reject
user@myhost# set term default-term then accept
```

Apply the Firewall Filter to the Loopback Interface

Step-by-Step Procedure

- To apply the firewall filter to the loopback interface:

```
[edit]
user@myhost# set interfaces lo0 unit 0 family inet filter input local_acl
user@myhost# set interfaces lo0 unit 0 family inet address 127.0.0.1/32
```

Confirm and Commit Your Candidate Configuration

Step-by-Step Procedure

To confirm and then commit your candidate configuration:

1. Confirm the configuration of the stateless firewall filter by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@myhost# show firewall
family inet {
   filter local_acl {
      term terminal_access {
         from {
            source-address {
               192.168.1.0/24;
            }
            protocol tcp;
            port [ssh telnet];
```

```
        }
        then accept;
      }
      term terminal_access_denied {
        from {
          protocol tcp;
          port [ssh telnet];
        }
        then {
          log;
          reject;
        }
      }
      term default-term {
        then accept;
      }
    }
}
```

2. Confirm the configuration of the interface by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@myhost# show interfaces
lo0 {
  unit 0 {
    family inet {
      filter {
        input local_acl;
      }
      source-address 127.0.0.1/32;
    }
  }
}
```

3. If you are done configuring the device, commit your candidate configuration.

```
[edit]
user@myhost# commit
```

Verification

Confirm that the configuration is working properly.

- Verifying Accepted Packets on page 250
- Verifying Logged and Rejected Packets on page 250

Verifying Accepted Packets

Purpose Verify that the actions of the firewall filter terms are taken.

Action

1. Clear the firewall log on your router or switch.

   ```
   user@myhost> clear firewall log
   ```

2. From a host at an IP address *within* the 192.168.1.0/24 subnet, use the **ssh *hostname*** command to verify that you can log in to the device using only SSH. This packet should be accepted, and the packet header information for this packet should not be logged in the firewall filter log buffer in the Packet Forwarding Engine.

   ```
   user@host-A> ssh myhost
   user@myhosts's password:
   --- JUNOS 11.1-20101102.0 built 2010-11-02 04:48:46 UTC
   % cli
   user@myhost>
   ```

3. From a host at an IP address *within* the 192.168.1.0/24 subnet, use the **telnet *hostname*** command to verify that you can log in to your router or switch using only Telnet. This packet should be accepted, and the packet header information for this packet should not be logged in the firewall filter log buffer in the Packet Forwarding Engine.

   ```
   user@host-A> telnet myhost
   Trying 192.168.249.71...
   Connected to myhost-fxp0.example.net.
   Escape character is '^]'.

   host (ttyp0)
   login: user
   Password:

   --- JUNOS 11.1-20101102.0 built 2010-11-02 04:48:46 UTC
   % cli
   user@myhost>
   ```

4. Use the **show firewall log** command to verify that the routing table on the device does not contain any entries with a source address in the 192.168.1.0/24 subnet.

   ```
   user@myhost> show firewall log
   ```

Verifying Logged and Rejected Packets

Purpose Verify that the actions of the firewall filter terms are taken.

Action

1. Clear the firewall log on your router or switch.

```
user@myhost> clear firewall log
```

2. From a host at an IP address *outside of* the 192.168.1.0/24 subnet, use the **ssh *hostname*** command to verify that you cannot log in to the device using only SSH. This packet should be rejected, and the packet header information for this packet should be logged in the firewall filter log buffer in the Packet Forwarding Engine.

```
user@host-B ssh myhost
ssh: connect to host sugar port 22: Connection refused
--- JUNOS 11.1-20101102.0 built 2010-11-02 04:48:46 UTC
%
```

3. From a host at an IP address *outside of* the 192.168.1.0/24 subnet, use the **telnet *hostname*** command to verify that you can log in to the device using only Telnet. This packet should be rejected, and the packet header information for this packet should be logged in the firewall filter log buffer in the PFE.

```
user@host-B> telnet myhost
Trying 192.168.249.71...
telnet: connect to address 192.168.187.3: Connection refused
telnet: Unable to connect to remote host
%
```

4. Use the **show firewall log** command to verify that the routing table on the device does not contain any entries with a source address in the 192.168.1.0/24 subnet.

```
user@myhost> show firewall log

Time     Filter    Action Interface Protocol Src Addr       Dest Addr
18:41:25 local_acl R      fxp0.0    TCP      192.168.187.5  192.168.187.1
18:41:25 local_acl R      fxp0.0    TCP      192.168.187.5  192.168.187.1
18:41:25 local_acl R      fxp0.0    TCP      192.168.187.5  192.168.187.1
...
18:43:06 local_acl R      fxp0.0    TCP      192.168.187.5  192.168.187.1
18:43:06 local_acl R      fxp0.0    TCP      192.168.187.5  192.168.187.1
18:43:06 local_acl R      fxp0.0    TCP      192.168.187.5  192.168.187.1
...
```

Release History Table

Release	Description
18.3R1	Starting in Junos OS Release 18.3R1, the **ssh-dss** and **ssh-dsa** hostkey algorithms are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Related Documentation

- *USB Modems for Remote Management of Security Devices*

Secure Web Access for Remote Management

You can manage a Juniper Networks device remotely through the J-Web interface. To enable secure Web access, the Juniper Networks devices support HTTP over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports on the device as needed. Read this topic for information.

Secure Web Access Overview

You can manage a Juniper Networks device remotely through the J-Web interface. To communicate with the device, the J-Web interface uses the Hypertext Transfer Protocol (HTTP). HTTP allows easy Web access but no encryption. The data that is transmitted between the Web browser and the device by means of HTTP is vulnerable to interception and attack. To enable secure Web access, the Juniper Networks devices support HTTP over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports as needed.

The Juniper Networks device uses the Secure Sockets Layer (SSL) protocol to provide secure device management through the Web interface. SSL uses public-private key technology that requires a paired private key and an authentication certificate for providing the SSL service. SSL encrypts communication between your device and the Web browser with a session key negotiated by the SSL server certificate.

An SSL certificate includes identifying information such as a public key and a signature made by a certificate authority (CA). When you access the device through HTTPS, an SSL handshake authenticates the server and the client and begins a secure session. If the information does not match or the certificate has expired, you cannot access the device through HTTPS.

Without SSL encryption, communication between your device and the browser is sent in the open and can be intercepted. We recommend that you enable HTTPS access on your WAN interfaces.

HTTP access is enabled by default on the built-in management interfaces. By default, HTTPS access is supported on any interface with an SSL server certificate.

See Also
- *Configuring Device Addresses (IPv4 and Loopback Addresses)*

Generating SSL Certificates for Secure Web Access (SRX Series Devices)

To generate an SSL certificate using the **openssl** command:

1. Enter **openssl** in the CLI. The **openssl** command generates a self-signed SSL certificate in privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.

   NOTE: Run this command on a LINUX or UNIX device because Juniper Networks Services Gateways do not support the openssl command.

   % openssl req –x509 –nodes –newkey rsa:1024 –keyout *filename*.pem -out *filename*.pem

   Replace ***filename*** with the name of a file in which you want the SSL certificate to be written—for example, **new.pem**.

2. When prompted, type the appropriate information in the identification form. For example, type **US** for the country name.

3. Display the contents of the file **new.pem**.

   cat new.pem

   Copy the contents of this file for installing the SSL certificate.

Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)

You can set up secure Web access for an EX Series switch. To enable secure Web access, you must generate a digital Secure Sockets Layer (SSL) certificate and then enable HTTPS access on the switch.

To generate an SSL certificate:

1. Enter the following **openssl** command in your SSH command-line interface on a BSD or Linux system on which **openssl** is installed. The **openssl** command generates a self-signed SSL certificate in the privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.

   % openssl req –x509 –nodes –newkey rsa:1024 –keyout *filename*.pem -out *filename*.pem

   where ***filename*** is the name of a file in which you want the SSL certificate to be written—for example, **my-certificate**.

2. When prompted, type the appropriate information in the identification form. For example, type **US** for the country name.

3. Display the contents of the file that you created.

   cat my-certificate.pem

You can use the J-Web Configuration page to install the SSL certificate on the switch. To do this, copy the file containing the certificate from the BSD or Linux system to the switch. Then open the file, copy its contents, and paste them into the Certificate box on the J-Web Secure Access Configuration page.

You can also use the following CLI statement to install the SSL certificate on the switch:

```
[edit]
user@switch# set security certificates local my-signed-cert load-key-file my-certificate.pem
```

See Also

- *Configuring Management Access for the EX Series Switch (J-Web Procedure)*
- *Overview of Port Security*

Generating a Self-Signed SSL Certificate Automatically

To generate a self-signed SSL certificate on Juniper Networks devices:

1. Establish basic connectivity.

2. Reboot the system. The self-signed certificate is automatically generated at bootup time.

   ```
   user@host> request system reboot
   Reboot the system ? [yes,no] yes
   ```

3. Specify **system-generated-certificate** under HTTPS Web management.

   ```
   [edit]
   user@host# show system services web-management https
     system-generated-certificate
   ```

Manually Generating Self-Signed SSL Certificates

To manually generate a self-signed SSL certificate on Juniper Networks devices:

1. Establish basic connectivity.

2. If you have root login access, you can manually generate the self-signed certificate by using the following commands:

   ```
   root@host> request security pki generate-key-pair size 512 certificate-id certname
   ```

```
Generated key pair sslcert, key size 512 bits
```

```
root@host> request security pki local-certificate generate-self-signed certificate-id
  cert-name email email domain-name domain name ip-address IP address subject
  "DC= Domain name, CN= Common-Name, OU= Organizational-Unit-name, O=
  Organization-Name, ST= state, C= Country"
```

```
Self-signed certificate generated and loaded successfully
```

NOTE: When generating the certificate, you must specify the subject, e-mail address, and either domain-name or ip-address.

3. To verify that the certificate was generated and loaded properly, enter the **show security pki local-certificate** operational command and specify **local-certificate** under HTTPS Web management.

```
[edit]
root@host# show system services web-management https local-certificate certname
```

Deleting Self-Signed Certificates (CLI Procedure)

You can delete a self-signed certificate that is automatically or manually generated from the EX Series switch. When you delete the automatically generated self-signed certificate, the switch generates a new self-signed certificate and stores it in the file system.

- To delete the automatically generated certificate and its associated key pair from the switch:

  ```
  user@switch> clear security pki local-certificate system-generated
  ```

- To delete a manually generated certificate and its associated key pair from the switch:

  ```
  user@switch> clear security pki local-certificate certificate-id certificate-id-name
  ```

- To delete all manually generated certificates and their associated key pairs from the switch:

  ```
  user@switch> clear security pki local-certificate all
  ```

Understanding Self-Signed Certificates on EX Series Switches

When you initialize a Juniper Networks EX Series Ethernet Switch with the factory default configuration, the switch generates a self-signed certificate, allowing secure access to the switch through the Secure Sockets Layer (SSL) protocol. Hypertext Transfer Protocol

over Secure Sockets Layer (HTTPS) and XML Network Management over Secure Sockets Layer (XNM-SSL) are the two services that can make use of the self-signed certificates.

NOTE: **Self-signed certificates do not provide additional security as do those generated by Certificate Authorities (CAs). This is because a client cannot verify that the server he or she has connected to is the one advertised in the certificate.**

The switches provide two methods for generating a self-signed certificate:

- Automatic generation

  In this case, the creator of the certificate is the switch. An automatically generated (also called “system-generated”) self-signed certificate is configured on the switch by default.

  After the switch is initialized, it checks for the presence of an automatically generated self-signed certificate. If it does not find one, the switch generates one and saves it in the file system.

  A self-signed certificate that is automatically generated by the switch is similar to an SSH host key. It is stored in the file system, not as part of the configuration. It persists when the switch is rebooted, and it is preserved when a **request system snapshot** command is issued.

  The switch uses the following distinguished name for the automatically generated certificate:

  “ CN=<device serial number>, CN=system generated, CN=self-signed”

  If you delete the system-generated self-signed certificate on the switch, the switch generates a self-signed certificate automatically.

- Manual generation

  In this case, you create the self-signed certificate for the switch. At any time, you can use the CLI to generate a self-signed certificate. Manually generated self-signed certificates are stored in the file system, not as part of the configuration.

Self-signed certificates are valid for five years from the time they are generated. When the validity of an automatically generated self-signed certificate expires, you can delete it from the switch so that the switch generates a new self-signed certificate.

System-generated self-signed certificates and manually generated self-signed certificates can coexist on the switch.

Manually Generating Self-Signed Certificates on Switches (CLI Procedure)

EX Series switches allow you to generate custom self-signed certificates and store them in the file system. The certificate you generate manually can coexist with the automatically generated self-signed certificate on the switch. To enable secure access to the switch

over SSL, you can use either the system-generated self-signed certificate or a certificate you have generated manually.

To generate self-signed certificates manually, you must complete the following tasks:

- Generating a Public-Private Key Pair on Switches on page 257
- Generating Self-Signed Certificates on Switches on page 257

Generating a Public-Private Key Pair on Switches

A digital certificate has an associated cryptographic key pair that is used to sign the certificate digitally. The cryptographic key pair comprises a public key and a private key. When you generate a self-signed certificate, you must provide a public-private key pair that can be used to sign the self-signed certificate. Therefore, you must generate a public-private key pair before you can generate a self-signed certificate.

To generate a public-private key pair:

```
user@switch> request security pki generate-key-pair certificate-id certificate-id-name
```

NOTE: Optionally, you can specify the encryption algorithm and the size of the encryption key. If you do not specify the encryption algorithm and encryption key size, default values are used. The default encryption algorithm is RSA, and the default encryption key size is 1024 bits.

After the public-private key pair is generated, the switch displays the following:

```
generated key pair certificate-id-name, key size 1024 bits
```

Generating Self-Signed Certificates on Switches

To generate the self-signed certificate manually, include the certificate ID name, the subject of the distinguished name (DN), the domain name, the IP address of the switch, and the e-mail address of the certificate holder:

```
user@switch> request security pki local-certificate generate-self-signed certificate-id
certificate-id-name domain-name domain-name email email-address ip-address switch-ip-address
subject subject-of-distinguished-name
```

The certificate you have generated is stored in the switch's file system. The certificate ID you have specified while generating the certificate is a unique identifier that you can use to enable the HTTPS or XNM-SSL services.

To verify that the certificate was generated and loaded properly, enter the **show security pki local-certificate** operational command.

See Also

- *Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure)*

Example: Configuring Secure Web Access

This example shows how to configure secure Web access on your device.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

NOTE: You can enable HTTPS access on specified interfaces. If you enable HTTPS without specifying an interface, HTTPS is enabled on all interfaces.

Overview

In this example, you import the SSL certificate that you have generated as a new and private key in PEM format. You then enable HTTPS access and specify the SSL certificate to be used for authentication. Finally, you specify the port as 8443 on which HTTPS access is to be enabled.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security certificates local new load-key-file /var/tmp/new.pem
set system services web-management https local-certificate new port 8443
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure secure Web access on your device:

1. Import the SSL certificate and private key.

   ```
   [edit security]
   user@host# set certificates local new load-key-file /var/tmp/new.pem
   ```

2. Enable HTTPS access and specify the SSL certificate and port.

```
[edit system]
user@host# set services web-management https local-certificate new port 8443
```

Results From configuration mode, confirm your configuration by entering the **show security** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security
certificates {
  local {
    new {
      "-----BEGIN RSA PRIVATE KEY-----\nMIICXQIBAAKBgQC/C5UI4frNqbi
        qPwbTiOkJvqoDw2YgYse0Z5zzVJyErgSg954T\nEuHM67Ck8hAOrCnb0YO+SY
        Y5rCXLf4+2s8k9EypLtYRw/Ts66DZoXI4viqE7HSsK\n5sQw/UDBIw7/MJ+OpA
        ... KYiFf4CbBBbjlMQJ0HFudW6ISVBslONkzX+FT\ni95ddka6iIRnArEb4VFCRh+
        e1QBdp1UjziYf7NuzDx4Z\n -----END RSA PRIVATE KEY-----\n-----BEGIN
        CERTIFICATE----- \nMIIDjDCCAvWgAwIBAgIBADANBgkqhkiG9w0BAQQ ...
        FADCBkTELMAkGA1UEBhMCdXMx\nCzAJBgNVBAgTAmNhMRIwEAYDVQQHEwlzdW5ue
        HB1YnMxDTALBgNVBAMTBGpucHIxJDAiBgkqhkiG\n9w0BCQEWFW5iaGFyZ2F2YUB
        fLUYAnBYmsYWOH\n -----END CERTIFICATE-----\n"; ## SECRET-DATA
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying an SSL Certificate Configuration on page 259
- Verifying a Secure Access Configuration on page 259

Verifying an SSL Certificate Configuration

Purpose Verify the SSL certificate configuration.

Action From operational mode, enter the **show security** command.

Verifying a Secure Access Configuration

Purpose Verify the secure access configuration.

Action From operational mode, enter the **show system services** command. The following sample output displays the sample values for secure Web access:

```
[edit]
user@host# show system services
web-management {
   http;
   https {
      port 8443;
      local-certificate new;
   }
}
```

Related Documentation

- Remote Access Overview on page 229
- Junos OS User Authentication Overview on page 161

Example: Controlling Management Access on SRX Series Devices

This example shows how to limit the management access to the specific IP addresses on an SRX Series devices to manage the device.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

To limit the IP addresses that can manage a device, you can configure a firewall filter. This firewall filters must include a term to deny all traffic except the IP address that you allow to manage the device. You must apply the firewall filter to the loopback interface (lo0) as this ensures that only management traffic (traffic to the device) is filtered.

In this example you:

- Configure a prefix-list called **manager-ip**. This list defines a set of IP addresses that are allowed to manage the SRX Series device.
- Configure a firewall filter **FILTER1** that rejects all requesters except IP addresses available in the **manager-ip** prefix list. In this way, you are ensuring that IP address list specified in the prefix list can manage the device.
- Apply **FILTER1** filter to the loopback interface. Any time a packet hits any of the interfaces on the device, the loopback interface applies the filter **FILTER1** .

Configuration

Configuring an IP Address List to Restrict Management Access to a Device

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set policy-options prefix-list manager-ip 192.168.4.254/32
set policy-options prefix-list manager-ip 10.0.0.0/8
set firewall filter FILTER1 term block_non_manager from source-address 0.0.0.0/0
set firewall filter FILTER1 term block_non_manager from source-prefix-list manager-ip
    except
set firewall filter FILTER1 term block_non_manager from protocol tcp
set firewall filter FILTER1 term block_non_manager from destination-port ssh
set firewall filter FILTER1 term block_non_manager from destination-port https
set firewall filter FILTER1 term block_non_manager from destination-port telnet
set firewall filter FILTER1 term block_non_manager from destination-port http
set firewall filter FILTER1 term block_non_manager then discard
set firewall filter FILTER1 term accept_everything_else then accept
set interfaces lo0 unit 0 family inet filter input FILTER1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Define a set of allowed host addresses in the prefix list.

```
[edit policy-options]
user@host# set prefix-list manager-ip 192.168.4.254/32
user@host# set prefix-list manager-ip 10.0.0.0/8
```

NOTE: The configured list is referenced in the actual filter, where you can change your defined set of addresses.

2. Configure a firewall filter to deny traffic from all IP addresses except the IP addresses defined in the prefix list.

```
[edit firewall filter]
user@host# set manager-ip term block_non_manager from source-address 0.0.0.0/0
user@host# set manager-ip term block_non_manager from source-prefix-list
    manager-ip except
user@host# set manager-ip term block_non_manager from protocol tcp
user@host# set manager-ip term block_non_manager from destination-port ssh
user@host# set manager-ip term block_non_manager from destination-port https
user@host# set manager-ip term block_non_manager from destination-port telnet
```

```
user@host# set manager-ip term block_non_manager from destination-port http
user@host# set manager-ip term block_non_manager then discard
```

Management traffic that uses any of the listed destination ports is rejected when the traffic comes from an address in the list.

3. Configure a default term that accepts all other traffic.

```
[edit firewall filter]
user@host# set manager-ip term accept_everything_else then accept
```

4. Apply stateless firewall filters to the loopback interface to filter the packets originating from the hosts to which you are granting management access.

```
[edit interfaces lo0 unit 0 ]
user@host# set family inet filter input manager-ip
```

This configuration applies to traffic terminating at the device itself. If you have IPsec traffic, or OSPF, RIP, BGP, or any other traffic that terminates at the interface of the device, then you must add the IP address of the interface to the prefix list.

Results From configuration mode, confirm your configuration by entering **show configuration** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show configuration policy-options
  prefix-list manager-ip {
  10.0.0.0/8;
  192.168.4.254/32;
}
```

```
user@host# show configuration firewall
  filter FILTER1 {
  term block_non_manager {
    from {
      source-address {
        0.0.0.0/0;
      }
      source-prefix-list {
        manager-ip except;
      }
      protocol tcp;
      destination-port [ ssh https telnet http ];
    }
    then {
      discard;
    }
  }
  term accept_everything_else {
```

```
      then accept;
    }
  }
```

```
user@host# show configuration interfaces
lo0 {
  unit 0 {
    family inet {
      filter {
        input FILTER1;
      }
    }
  }
}
```

```
user@host# show configuration interfaces lo0
unit 0 {
  family inet {
    filter {
      input FILTER1;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Interfaces

Purpose Verify if the interfaces are configured correctly.

Action From operational mode, enter the following commands:

- show policy-options
- show firewall
- show interfaces

Related Documentation
- Configuration Guidelines for Securing Console Port Access on page 263

Configuration Guidelines for Securing Console Port Access

You can use the console port on the device to connect to the device through an RJ-45 serial cable. From the console port, you can use the CLI to configure the device. By default, the console port is enabled. To secure the console port, you can configure the device to take the following actions:

- Log out of the console session when you unplug the serial cable connected to the console port.
- Disable root login connections to the console. This action prevents a non-root user from performing password recovery operation using the console.
- Disable the console port. We recommend disabling the console port to prevent unauthorized access to the device, especially when the device is used as customer premises equipment (CPE) and is forwarding sensitive traffic.

NOTE: It is not always possible to disable the console port, because console access is important during operations such as software upgrades.

WARNING: On SRX SRX300, SRX320, SRX340, and SRX345 devices, if both **set system ports console insecure** and **set chassis routing-engine bios uninterrupt** options are configured, there is no alternative recovery method available incase Junos OS fails to boot and the device might become unusable.

To secure the console port:

1. Do one of the following:
   - Disable the console port. Enter

     ```
     [edit system ports console]
     user@host# set disable
     ```

   - Disable root login connections to the console. Enter

     ```
     [edit system ports console]
     user@host# set insecure
     ```

     NOTE: After configuring the console port as insecure, if a user tries to perform password recovery operation by booting in single-user mode, the device will prompt for the root password. This way, the user will be unable to log in to single-user mode for password recovery unless the root password is known.

   - Log out the console session when the serial cable connected to the console port is unplugged. Enter

     ```
     [edit system ports console]
     user@host# set log-out-on-disconnect
     ```

NOTE: The **log-out-on-disconnect** statement is not operational on SRX1500, SRX4100, SRX4200, and SRX4600 devices; on these devices, you must manually log out from the console with the **request system logout** command.

2. If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- The telnet Command on page 235
- The ssh Command on page 236
- Configuring Password Retry Limits for Telnet and SSH Access on page 245

CHAPTER 6

Access Control on Switches

Access Control and Authentication on Switching Devices

You can control access to your network through a switch by using several different authentication. Junos OS switches support 802.1X, MAC RADIUS, and captive portal as an authentication methods to devices requiring to connect to a network. Read this topic for more information.

Understanding Authentication on Switches

You can control access to your network through a Juniper Networks EX Series Ethernet Switch by using authentication methods such as 802.1X, MAC RADIUS, or captive portal. Authentication prevents unauthenticated devices and users from gaining access to your LAN. For 802.1X and MAC RADIUS authentication, end devices must be authenticated before they receive an IP address from a Dynamic Host Configuration Protocol (DHCP) server. For captive portal authentication, the switch allows the end devices to acquire an IP address in order to redirect them to a login page for authentication.

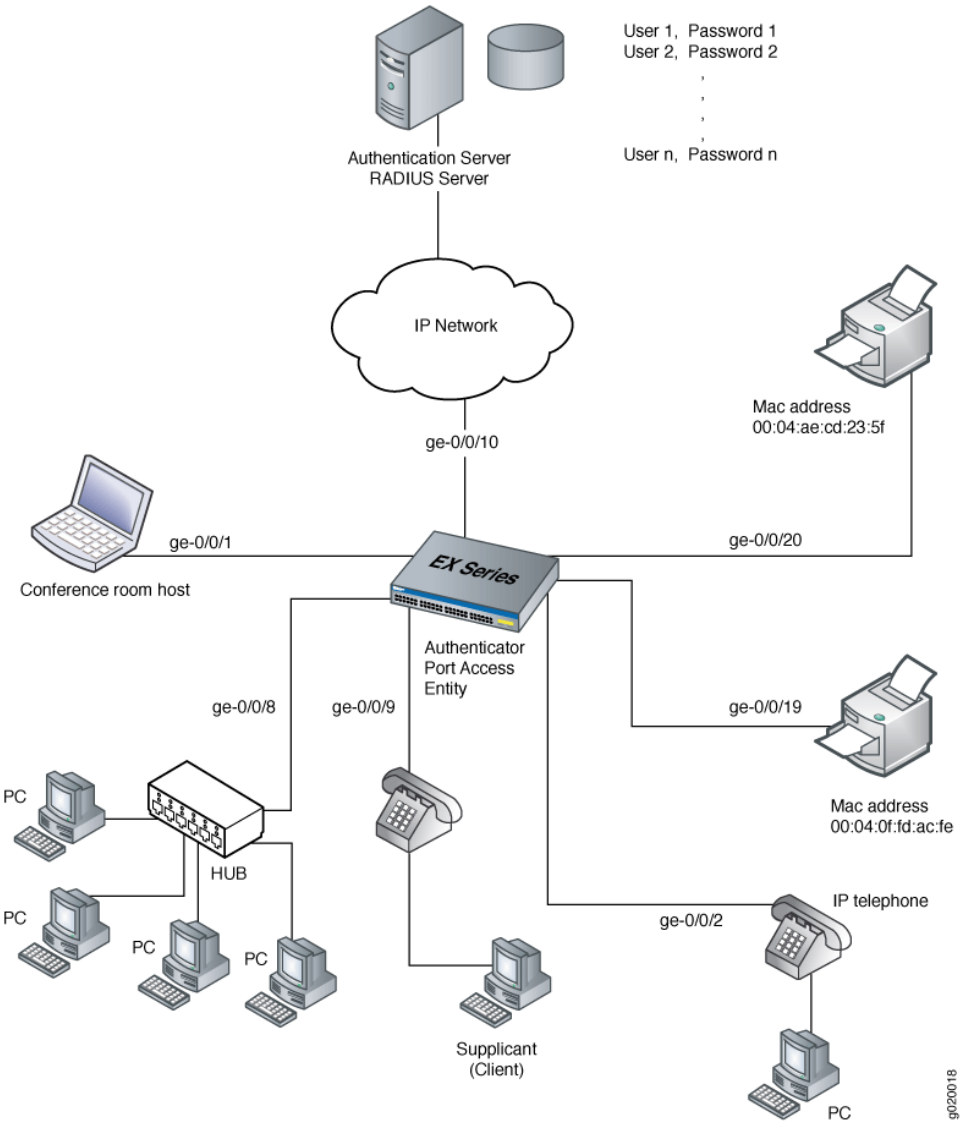
This topic covers:

Sample Authentication Topology

Figure 5 on page 269 illustrates a basic deployment topology for authentication on an EX Series switch:

NOTE: For illustration purposes, we have used an EX Series switch, but a QFX5100 switch can be used in the same way.

Figure 5: Example Authentication Topology



The topology contains an EX Series access switch connected to the authentication server on port ge-0/0/10. Interface ge-0/0/1 connects to the conference room host. Interface ge-0/0/8 is connected to four desktop PCs through a hub. Interfaces ge-0/0/9 and ge-0/0/2 are connected to IP phones with an integrated hub to connect the phone and desktop PC to a single port. Interfaces ge-0/0/19 and ge-0/0/20 are connected to printers.

802.1X Authentication

802.1X is an IEEE standard for port-based network access control (PNAC). It provides an authentication mechanism for devices seeking to access a LAN. The 802.1X authentication feature on an EX Series switch is based upon the IEEE 802.1X standard *Port-Based Network Access Control*.

The communication protocol between the end device and the switch is Extensible Authentication Protocol over LAN (EAPoL). EAPoL is a version of EAP designed to work with Ethernet networks. The communication protocol between the authentication server and the switch is RADIUS.

During the authentication process, the switch completes multiple message exchanges between the end device and the authentication server. While 802.1X authentication is in process, only 802.1X traffic and control traffic can transit the network. Other traffic, such as DHCP traffic and HTTP traffic, is blocked at the data link layer.

NOTE: You can configure both the maximum number of times an EAPoL request packet is retransmitted and the timeout period between attempts. For information, see "Configuring 802.1X Interface Settings (CLI Procedure)" on page 292.

An 802.1X authentication configuration for a LAN contains three basic components:

- *Supplicant* (also called end device)—Supplicant is the IEEE term for an end device that requests to join the network. The end device can be responsive or nonresponsive. A responsive end device is 802.1X-enabled and provides authentication credentials using EAP. The credentials required depend on the version of EAP being used—specifically, a username and password for EAP MD5 or a username and client certificates for Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), and Protected EAP (PEAP).

  You can configure a server-reject VLAN to provide limited LAN access for responsive 802.1X-enabled end devices that sent incorrect credentials. A server-reject VLAN can provide a remedial connection, typically only to the Internet, for these devices. See "Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients" on page 315 for additional information.

  NOTE: If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is dropped.

  A nonresponsive end device is one that is not 802.1X-enabled. It can be authenticated through MAC RADIUS authentication.

- *Authenticator port access entity*—The IEEE term for the authenticator. The switch is the authenticator, and it controls access by blocking all traffic to and from end devices until they are authenticated.

- *Authentication server*—The authentication server contains the backend database that makes authentication decisions. It contains credential information for each end device that is authenticated to connect to the network. The authenticator forwards credentials supplied by the end device to the authentication server. If the credentials forwarded by the authenticator match the credentials in the authentication server database, access is granted. If the credentials forwarded do not match, access is denied. The EX Series switches support RADIUS authentication servers.

NOTE: You cannot configure 802.1X authentication on redundant trunk groups (RTGs). For more information about RTGs, see *Understanding Redundant Trunk Links (Legacy RTG Configuration)*.

MAC RADIUS Authentication

The 802.1X authentication method only works if the end device is 802.1X-enabled, but many single-purpose network devices such as printers and IP phones do not support the 802.1X protocol. You can configure MAC RADIUS authentication on interfaces that are connected to network devices that do not support 802.1X and for which you want to allow to access the LAN. When an end device that is not 802.1X-enabled is detected on the interface, the switch transmits the MAC address of the device to the authentication server. The server then tries to match the MAC address with a list of MAC addresses in its database. If the MAC address matches an address in the list, the end device is authenticated.

You can configure both 802.1X and MAC RADIUS authentication methods on the interface. In this case, the switch first attempts to authenticate the end device by using 802.1X, and if that method fails, it attempts to authenticate the end device by using MAC RADIUS authentication. If you know that only non-responsive supplicants connect on that interface, you can eliminate the delay that occurs for the switch to determine that the end device is not 802.1X-enabled by configuring the **mac-radius restrict** option. When this option is configured, the switch does not attempt to authenticate the end device through 802.1X authentication but instead immediately sends a request to the RADIUS server for authentication of the MAC address of the end device. If the MAC address of that end device is configured as a valid MAC address on the RADIUS server, the switch opens LAN access to the end device on the interface to which it is connected.

The **mac-radius-restrict** option is useful when no other 802.1X authentication methods, such as guest VLAN, are needed on the interface. If you configure **mac-radius-restrict** on an interface, the switch drops all 802.1X packets.

The authentication protocols supported for MAC RADIUS authentication are EAP-MD5, which is the default, Protected EAP (EAP-PEAP), and Password Authentication Protocol (PAP). You can specify the authentication protocol to be used for MAC RADIUS authentication using the authentication-protocol statement.

Captive Portal Authentication

Captive portal authentication (hereafter referred to as captive portal) enables you to authenticate users on EX Series switches by redirecting Web browser requests to a login page that requires users to input a valid username and password before they can access the network. Captive portal controls network access by requiring users to provide information that is authenticated against a RADIUS server database by using EAP-MD5. You can also use captive portal to display an acceptable-use policy to users before they access your network.

Juniper Networks Junos operating system (Junos OS) for EX Series switches provides a template that enables you to easily design and modify the look of the captive portal login

page. You enable specific interfaces for captive portal. The first time an end device connected to a captive portal interface attempts to access a webpage, the switch presents the captive portal login page. After the device is successfully authenticated, it is allowed access to the network and to continue to the original page requested.

NOTE: If HTTPS is enabled, HTTP requests are redirected to an HTTPS connection for the captive portal authentication process. After authentication, the end device is returned to the HTTP connection.

If there are end devices that are not HTTP-enabled connected to the captive portal interface, you can allow them to bypass captive portal authentication by adding their MAC addresses to an authentication whitelist.

When a user is authenticated by the RADIUS server, any per-user policies (attributes) associated with that user are also sent to the switch.

Captive portal on switches has the following limitations:

- Captive portal does not support dynamic assignment of VLANs downloaded from the RADIUS server.
- If the user remains idle for more than about 5 minutes and there is no traffic passed, the user must log back in to the captive portal.

Static MAC Bypass of Authentication

You can allow end devices to access the LAN without authentication on a RADIUS server by including their MAC addresses in the static MAC bypass list (also known as the exclusion list).

You might choose to include a device in the bypass list to:

- Allow non-802.1X-enabled devices access to the LAN.
- Eliminate the delay that occurs for the switch to determine that a connected device is a non-802.1X-enabled host.

When you configure static MAC on the switch, the MAC address of the end device is first checked in a local database (a user-configured list of MAC addresses). If a match is found, the end device is successfully authenticated and the interface is opened up for it. No further authentication is done for that end device. If a match is not found and 802.1X authentication is enabled on the switch, the switch attempts to authenticate the end device through the RADIUS server.

For each MAC address, you can also configure the VLAN to which the end device is moved or the interfaces on which the host connects.

CAUTION: When you clear the learned MAC addresses from an interface, using the clear dot1x interface command, all MAC addresses are cleared, including those in the static MAC bypass list.

Fallback of Authentication Methods

You can configure 802.1X, MAC RADIUS, and captive portal authentication on a single interface to enable fallback to another method if authentication by one method fails. The authentication methods can be configured in any combination, except that you cannot configure both MAC RADIUS and captive portal on an interface without also configuring 802.1X. By default, an EX Series switch uses the following order of authentication methods:

1. 802.1X authentication—If 802.1X is configured on the interface, the switch sends EAPoL requests to the end device and attempts to authenticate the end device through 802.1X authentication. If the end device does not respond to the EAP requests, the switch checks whether MAC RADIUS authentication is configured on the interface.

2. MAC RADIUS authentication—If MAC RADIUS authentication is configured on the interface, the switch sends the MAC RADIUS address of the end device to the authentication server. If MAC RADIUS authentication is not configured, the switch checks whether captive portal is configured on the interface.

3. Captive portal authentication—If captive portal is configured on the interface, the switch attempts to authenticate the end device by using this method after the other authentication methods configured on the interface have failed.

For an illustration of the default process flow when multiple authentication methods are configured on an interface, see "Understanding Access Control on Switches" on page 274.

You can override the default order for fallback of authentication methods by configuring the **authentication-order** statement to specify that the switch use either 802.1X authentication or MAC RADIUS authentication first. Captive portal must always be last in the order of authentication methods. For more information, see "Configuring Flexible Authentication Order" on page 389.

NOTE: **Starting with Junos OS Release 15.1R3, if an interface is configured in multiple-supplicant mode, end devices connecting through the interface can be authenticated using different methods in parallel. Therefore, if an end device on the interface was authenticated after fall back to captive portal, then additional end devices can still be authenticated using 802.1X or MAC RADIUS authentication.**

See Also

- 802.1X for Switches Overview on page 289
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- Configuring MAC RADIUS Authentication (CLI Procedure) on page 325

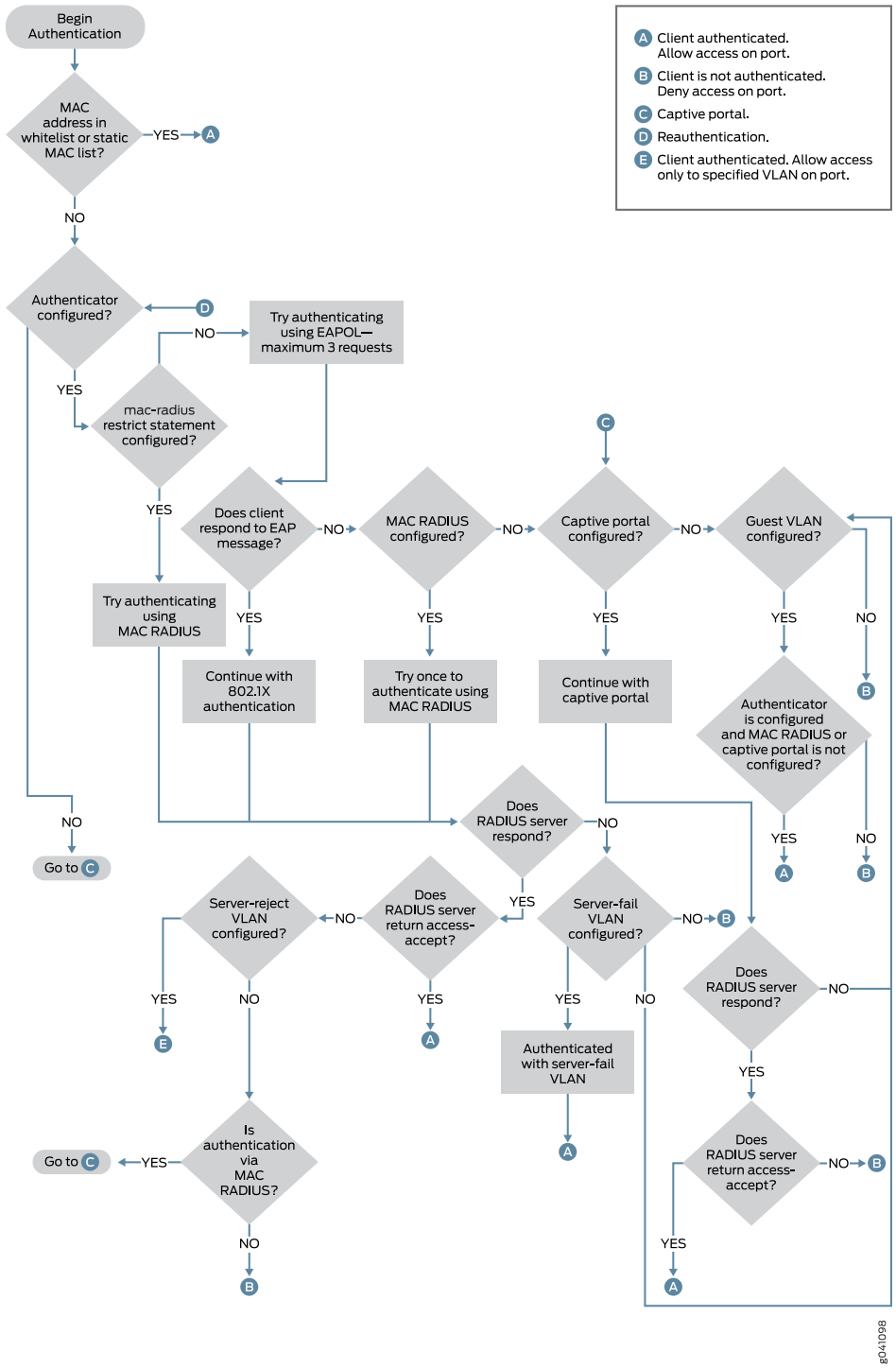
- Configuring Captive Portal Authentication (CLI Procedure) on page 378
- Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication (CLI Procedure) on page 368

Understanding Access Control on Switches

You can control access to your network through a switch by using several different authentication methods—including 802.1X, MAC RADIUS, or captive portal.

Figure 6 on page 275 illustrates the authentication process:

Figure 6: Authentication Process Flow for Switches



See Also • Understanding Server Fail Fallback and Authentication on Switches on page 286

- Understanding Guest VLANs for 802.1X on Switches on page 308
- Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 307
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373

Understanding Authentication Session Timeout

Information about authentication sessions—including the associated interfaces and VLANs for each MAC address that is authenticated—is stored in the authentication session table. The authentication session table is tied to the Ethernet switching table (also called the MAC table). Each time the switch detects traffic from a MAC address, it updates the timestamp for that network node in the Ethernet switching table. A timer on the switch periodically checks the timestamp and if its value exceeds the user-configured **mac-table-aging-time** value, the MAC address is removed from the Ethernet switching table. When a MAC address ages out of the Ethernet switching table, the entry for that MAC address is also removed from the authentication session table, with the result that the session ends.

When the authentication session ends due to MAC address aging, the host must re-attempt authentication. To limit the downtime resulting from re-authentication, you can control the timeout of authentication sessions in the following ways:

- For 802.1X and MAC RADIUS authentication sessions, disassociate the authentication session table from the Ethernet switching table by using the no-mac-table-binding statement. This setting prevents the termination of the authentication session when the associated MAC address ages out of the Ethernet switching table.
- For captive portal authentication sessions, configure a keep-alive timer using the **user-keepalive** statement. With this option configured, when the associated MAC address ages out of the Ethernet switching table, the keep-alive timer is started. If traffic is received within the keep-alive timeout period, the timer is deleted. If there is no traffic within the keep-alive timeout period, the session is deleted.

You can also specify timeout values for authentication sessions to end the session before the MAC aging timer expires. After the session times out, the host must re-attempt authentication.

- For 802.1X and MAC RADIUS authentication sessions, the duration of the session before timeout depends on the value of the **reauthentication** statement. If the MAC aging timer expires before the session times out, and the **no-mac-table-binding** statement is not configured, the session is ended, and the host must re-authenticate.
- For captive portal authentication sessions, the duration of the session depends on the value configured for the session-expiry statement. If the MAC aging timer expires before the session times out, and the **user-keepalive** statement is not configured, the session is ended, and the host must re-authenticate.

NOTE: If the authentication server sends an authentication session timeout to the client, this takes priority over the value configured locally using either the reauthentication statement of the session-expiry statement. The session timeout value is sent from the server to the client as an attribute of the RADIUS Access-Accept message. For information about configuring the authentication server to send an authentication session timeout, see the documentation for your server.

See Also

- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- *Configuring MAC Table Aging on Switches*

Controlling Authentication Session Timeouts (CLI Procedure)

The expiration of an authentication session can result in downtime because the host must re-attempt authentication. You can limit this downtime by controlling the timeout period for authentication sessions.

An authentication session can end when the MAC address associated with the authenticated host ages out of the Ethernet switching table. When the MAC address is cleared from the Ethernet switching table, the authenticated session for that host ends, and the host must re-attempt authentication.

To prevent the authentication session from ending when the MAC address ages out of the Ethernet switching table:

- For sessions authenticated using 802.1X or MAC RADIUS authentication, you can prevent authentication session timeouts due to MAC address aging by disassociating the authentication session table from the Ethernet switching table using the no-mac-table-binding statement:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator no-mac-table-binding;
  ```

- For sessions authenticated using captive portal authentication, you can prevent authentication session timeouts due to MAC address aging by extending the timeout period using the user-keepalive statement:

  ```
  [edit]
  user@switch# set services captive-portal interface interface-name user-keepalive minutes;
  ```

You can also configure timeout values for authentication sessions to end an authenticated session before the MAC aging timer expires.

NOTE: Configuring the session timeout for an authentication session does not extend the session after the MAC aging timer expires. You must configure either the **no-mac-table-binding** statement for 802.1X and MAC RADIUS authentication, or the **user-keepalive** statement for captive portal authentication, to prevent session timeout due to MAC aging.

For 802.1X and MAC RADIUS authentication sessions, configure the timeout value using the **reauthentication** statement.

- To configure the timeout value on a single interface:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name reauthentication seconds;
```

- To configure the timeout value on all interfaces:

```
[edit]
user@switch# set protocols dot1x authenticator interface all reauthentication seconds;
```

For captive portal authentication sessions, configure the timeout value using the **session-expiry** statement.

- To configure the timeout value on a single interface:

```
[edit]
user@switch# set services captive-portal interface interface-name session-expiry minutes;
```

- To configure the timeout value on all interfaces:

```
[edit]
user@switch# set services captive-portal interface all session-expiry minutes;
```

NOTE: If the authentication server sends an authentication session timeout to the client, this takes priority over the value configured using the **reauthentication** statement or the **session-expiry** statement. The session timeout value is sent from the server to the client as an attribute of the RADIUS Access-Accept message.

See Also

- *Configuring MAC Table Aging on Switches*
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337

Related Documentation

- 802.1X Authentication on page 289
- 802.1X and RADIUS Accounting on page 332

- MAC RADIUS Authentication on page 324

Preventing Unauthorized Access to EX Series Switches Using Unattended Mode for U-Boot

Junos OS allows you to configure anattended mode for U-Boot to prevent unauthorized access to the switch during the boot process. When you configure unattended mode, an user can access the CLI during the boot process by supplying the boot-loader password. This prevents unauthorized access during boot process. Read this topic for more information.

- Understanding Unattended Mode for U-Boot on EX Series Switches on page 279
- Using Unattended Mode for U-Boot to Prevent Unauthorized Access on page 280

Understanding Unattended Mode for U-Boot on EX Series Switches

Unattended mode for U-Boot can be configured to prevent unauthorized access to the switch that can occur during the boot process. After the CPU has been reset, there are several known methods of accessing the system before the JUNOS OS login prompt appears that do not require the user to enter authorization credentials. By gaining unauthorized access, the user can view, modify, or corrupt the switch configuration, or make the switch unavailable on the network.

When unattended mode is configured, the user can access the CLI during the boot process only by pressing <Ctrl+c> and entering the correct password, which is known as the boot-loader password. The boot-loader password must have been previously configured on the switch. Entering the correct boot-loader password will place the user in the U-Boot CLI. If the password is incorrect, or if no password is entered within one minute, access to the U-Boot CLI is blocked and the boot process continues automatically.

Access to the bootstrap loader command prompt (**loader>**) is blocked in unattended mode, which prevents the use of the following recovery mechanisms: root password recovery by using single-user mode, and booting the switch by using a software package stored on a USB flash drive.

NOTE: If the root password is lost while the switch is in unattended mode, the switch must be reset to the factory default configuration using the LCD panel. For more information see *Reverting to the Default Factory Configuration for the EX Series Switch*.

If unattended mode is not configured, but a boot-loader password has been configured, the user must enter the correct password to access the U-Boot CLI. If a boot-loader password has not been configured, the user can access the U-Boot CLI without entering a password. In either case, the user can access the bootstrap loader command prompt, which enables root password recovery by using single-user mode as well as booting from a USB flash drive.

Unattended mode is not enabled by default. When configured, unattended mode is turned on and will block unauthorized access to the switch. Table 19 on page 280 summarizes the behaviors for U-Boot mode.

Table 19: Unattended Mode Behavior

Unattended Mode	Boot-loader password	Behavior
On	Set	• Access to U-Boot CLI is allowed only after entering correct password. • Access to loader command prompt is blocked. • Booting from USB is blocked. • Root password recovery by using single-user mode is blocked.
On	Not Set	• Access to U-Boot CLI is blocked. • Access to loader command prompt is blocked. • Booting from USB is blocked. • Root password recovery by using single-user mode is blocked.
Off	Set	• Access to U-Boot CLI is allowed only after entering correct password. • Access to loader command prompt is allowed. • Booting from USB is allowed. • Root password recovery by using single-user mode is allowed.
Off	Not Set	• Access to U-Boot CLI is allowed. • Access to loader command prompt is allowed. • Booting from USB is allowed. • Root password recovery by using single-user mode is allowed.

See Also • Root Password on page 139

Using Unattended Mode for U-Boot to Prevent Unauthorized Access

Unattended mode for U-Boot can be used to prevent unauthorized access to the switch that can occur during the boot process. When unattended mode is configured, the user can access the CLI during the boot process only by entering the correct password, which is known as the boot-loader password. The boot-loader password must have been previously configured on the switch.

When unattended mode is configured, access to the bootstrap loader command prompt (**loader>**) is blocked, which prevents the use of the following recovery mechanisms: root password recovery by using single-user mode, and booting the switch by using a software package stored on a USB flash drive.

WARNING: On EX2200 switches, if both the root and unattended mode password are lost while the switch is in unattended mode, there is no alternative recovery method available. The switch must be returned to Juniper

Networks. For more information, see *Returning an EX2200 Switch or Component for Repair or Replacement*.

To use unattended mode, follow the following procedures:

- Configuring the Boot Loader Password on page 281
- Configuring Unattended Mode for U-Boot on page 282
- Accessing the U-Boot CLI on page 282

Configuring the Boot Loader Password

To configure the boot loader password, you can use either a plain-text password that the system encrypts for you, or a password that has already been encrypted. If you use a plain-text password, Junos OS displays the password as an encrypted string so that users viewing the configuration cannot see it. As you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password. Plain-text passwords are hidden and marked as ## SECRET-DATA in the configuration.

To configure the boot-loader password:

1. Enter either a plain-text password or an encrypted password by using the **set system boot-loader authentication** command.
   - To enter a plain-text password, use the **plain-text-password** option, and re-enter the password when prompted:

     ```
     [edit]
     root@# set system boot-loader-authentication plain-text-password
     New Password: type password here
     Retype new password: retype password here
     ```

   - To enter a password that is already encrypted, use the **encrypted-password** option:

     ```
     [edit]
     root@# set system boot-loader-authentication encrypted-password password
     ```

2. Commit the changes.

   ```
   [edit]
   root@# commit
   ```

3. To view the encrypted password entries, use the configuration mode **show** command. For example:

   ```
   [edit]
   root@# show system boot-loader-authentication
   encrypted-password “$ABC123”; ## SECRET-DATA
   ```

Configuring Unattended Mode for U-Boot

Before enabling unattended mode for U-Boot, you must download and install the jloader firmware package **/volume/build/junos/13.2/service/13.2X51-D20.2/ship/jloader-ex-2200-13.2X51-D20.2-signed.tgz**, as described in TSB16425.

Unattended mode for U-Boot is not enabled by default. Use the following procedure to configure unattended mode:

1. Configure unattended mode.

```
[edit]
root@# set system unattended-boot
```

2. Commit the changes.

```
[edit]
root@# commit
```

Accessing the U-Boot CLI

When unattended mode for U-Boot is configured and the boot-loader password has been set, you can access the U-Boot CLI during the boot process by pressing <Ctrl+c> and entering the password at the prompt:

```
Press Ctrl-C in next 1 seconds to enter u-boot prompt...
Enter password:
password correct...
=>
```

The correct password must be entered within one minute after the prompt appears. If the password is not entered within one minute, or if the password is incorrect or has not been configured, access to the U-Boot CLI will be blocked, and the boot process will continue. For more information about unattended mode behavior, see "Understanding Unattended Mode for U-Boot on EX Series Switches" on page 279.

See Also

- unattended-boot on page 1583
- boot-loader-authentication on page 911

Related Documentation

- Access Control and Authentication on Switching Devices on page 267

RADIUS Server Configuration for Authentication

Juniper Networks Ethernet Switches use 802.1X, MAC RADIUS, or captive portal authentication to provide access control to the devices or users. When 802.1X, MAC

RADIUS, or captive portal authentications are configured on the switch, end devices are evaluated at the initial connection by an authentication (RADIUS) server. To use 802.1X or MAC RADIUS authentication, you must specify the connections on the switch for each RADIUS server to which you want to connect. Read this topic for more information.

Specifying RADIUS Server Connections on Switches (CLI Procedure)

IEEE 802.1X and MAC RADIUS authentication both provide network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from devices at the interface until the supplicant's credentials or MAC address are presented and matched on the *authentication server* (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

To use 802.1X or MAC RADIUS authentication, you must specify the connections on the switch for each RADIUS server to which you will connect.

To configure a RADIUS server on the switch:

1. Define the IP address of the RADIUS server, the RADIUS server authentication port number, and the secret password. You can define more than one RADIUS server. The secret password on the switch must match the secret password on the server:

   ```
   [edit access]
   user@switch# set radius-server server-address port 1812 secret password
   ```

   NOTE: Specifying the authentication port is optional, and port 1812 is the default. However, we recommend that you configure it in order to avoid confusion as some RADIUS servers might refer to an older default.

2. (Optional) Specify the IP address by which the switch is identified by the RADIUS server. If you do not specify the IP address, the RADIUS server uses the address of the interface that sends the RADIUS request. We recommend that you specify this IP address because if the request gets diverted on an alternate route to the RADIUS server, the interface relaying the request might not be an interface on the switch.

   ```
   [edit access]
   user@switch# set access radius-server source-address source-address
   ```

3. Configure the authentication order, making **radius** the first method of authentication:

```
[edit access]
user@switch# set profile profile-name authentication-order (Access Profile) radius
```

4. Create a profile and specify the list of RADIUS servers to be associated with the profile. For example, you might choose to group your RADIUS servers geographically by city. This feature enables easy modification whenever you want to change to a different sent of authentication servers.

   ```
   [edit access profile profile-name]
   user@switch# set radius authentication-server server-address server-address
   ```

5. Specify the group of servers to be used for 802.1X or MAC RADIUS authentication by identifying the profile name:

   ```
   [edit]
   user@switch# set protocols dot1x authenticator authentication-profile-name
   access-profile-name
   ```

6. Configure the IP address of the switch in the list of clients on the RADIUS server. For information about configuring the RADIUS server, consult the documentation for your server.

See Also

- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- *Configuring 802.1X Authentication (J-Web Procedure)*
- Configuring MAC RADIUS Authentication (CLI Procedure) on page 325
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335

Configuring MS-CHAPv2 to Provide Password-Change Support (CLI Procedure)

Junos OS for EX Series switches enables you to configure the Microsoft Corporation implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the switch to provide password-change support. Configuring MS-CHAPv2 on the switch provides users accessing a switch the option of changing the password when the password expires, is reset, or is configured to be changed at next login.

See RFC 2433, *Microsoft PPP CHAP Extensions*, for information about MS-CHAP.

Before you configure MS-CHAPv2 to provide password-change support, ensure that you have:

- Configured RADIUS server authentication. Configure users on the authentication server and set the first-tried option in the authentication order to radius. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.

To configure MS-CHAPv2, specify the following:

```
[edit system radius-options]
user@switch# set password-protocol mschap-v2
```

You must have the required access permission on the switch in order to change your password.

See Also

- *Managing Users (J-Web Procedure)*
- For more about configuring user access, see the *Junos OS Access Privilege Configuration Guide*.

Configuring MS-CHAPv2 for Password-Change Support

You can configure the Microsoft implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the router or switch to support changing of passwords. This feature provides users accessing a router or switch the option of changing the password when the password expires, is reset, or is configured to be changed at next logon.

Before you configure MS-CHAPv2 for password-change support, ensure that you have done the following:

- Configured RADIUS server authentication parameters.
- Set the first tried option in the authentication order to RADIUS server.

To configure MS-CHAP-v2, include the following statements at the **[edit system radius-options]** hierarchy level:

```
[edit system radius-options]
password-protocol mschap-v2;
```

The following example shows statements for configuring the MS-CHAPv2 password protocol, password authentication order, and user accounts:

```
[edit]
system {
   authentication-order [ radius password ];
   radius-server {
      192.168.69.149 secret "$9$G-j.5Qz6tpBk.1hrlXxUjiq5Qn/C"; ## SECRET-DATA
   }
   radius-options {
      password-protocol mschap-v2;
   }
   login {
      user bob {
```

```
        class operator;
    }
  }
}
```

See Also

- *Configuring Access Profiles for L2TP or PPP Parameters*

Understanding Server Fail Fallback and Authentication on Switches

Juniper Networks Ethernet Switches use authentication to implement access control in an enterprise network. If 802.1X, MAC RADIUS, or captive portal authentication is configured on the switch, end devices are evaluated at the initial connection by an authentication (RADIUS) server. If the end device is configured on the authentication server, the device is granted access to the LAN and the EX Series switch opens the interface to permit access.

Server fail fallback enables you to specify how end devices connected to the switch are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message. Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by an end device's first attempt at authentication through the RADIUS server.

Server fail fallback enables you to specify one of four actions to be taken for end devices awaiting authentication when the server is timed out. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN. The VLAN must already be configured on the switch. The configured VLAN name overrides any attributes sent by the server.

- *Permit* authentication, allowing traffic to flow from the end device through the interface as if the end device were successfully authenticated by the RADIUS server.
- *Deny* authentication, preventing traffic from flowing from the end device through the interface. This is the default.
- *Move* the end device to a specified VLAN if the switch receives a RADIUS access-reject message. The configured VLAN name overrides any attributes sent by the server. (The VLAN must already exist on the switch.)
- *Sustain* authenticated end devices that already have LAN access and *deny* unauthenticated end devices. If the RADIUS servers time out during reauthentication, previously authenticated end devices are reauthenticated and new users are denied LAN access.

See Also

- 802.1X for Switches Overview on page 289
- Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 309

- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292

Configuring RADIUS Server Fail Fallback (CLI Procedure)

You can configure authentication fallback options to specify how end devices connected to a switch are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

When you set up 802.1X or MAC RADIUS authentication on the switch, you specify a primary authentication server and one or more backup authentication servers. If the primary authentication server cannot be reached by the switch and the secondary authentication servers are also unreachable, a RADIUS server timeout occurs. If this happens, because it is the authentication server that grants or denies access to the end devices awaiting authentication, the switch does not receive access instructions for end devices attempting access to the LAN, and normal authentication cannot be completed.

You can configure the server fail fallback feature to specify an action that the switch applies to end devices when the authentication servers are unavailable. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN.

You can also configure the server reject fallback feature for end devices that receive a RADIUS access-reject message from the authentication server. The server reject fallback feature provides limited access to a LAN, typically only to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials.

Server fail fallback is supported for voice traffic starting in Release 14.1X53-D40 and Release 15.1R4. To configure server fail fallback actions for VoIP clients sending voice traffic, use the **server-fail-voip** statement. For all data traffic, use the **server-fail** statement. The switch determines the fallback method to use based on the type of traffic sent by the client. Untagged data frames are subject to the action configured with **server-fail**, even if they are sent by a VoIP client. Tagged VoIP VLAN frames are subject to the action configured with **server-fail-voip**. If **server-fail-voip** is not configured, the voice traffic is dropped.

NOTE: Server reject fallback is not supported for VoIP VLAN tagged traffic. If a VoIP client starts authentication by sending untagged data traffic to a VLAN while server reject fallback is in effect, the VoIP client is allowed to access the fallback VLAN. If the same client subsequently sends tagged voice traffic, the voice traffic is dropped.

If a VoIP client starts authentication by sending tagged voice traffic while server reject fallback is in effect, the VoIP client is denied access to the fallback VLAN.

You can use the following procedure to configure server fail actions for data clients. To configure server fail fallback for VoIP clients sending voice traffic, use the **server-fail-voip** statement in place of the **server-fail** statement.

To configure server fail fallback actions:

- Configure an interface to allow traffic to flow from a supplicant to the LAN if a RADIUS server timeout occurs (as if the end device had been successfully authenticated by a RADIUS server):

  ```
  [edit protocols dot1x authenticator]
  user@switch# set interface interface-name server-fail permit
  ```

- Configure an interface to prevent traffic flow from an end device to the LAN (as if the end device had failed authentication and had been denied access by the RADIUS server):

  ```
  [edit protocols dot1x authenticator]
  user@switch# set interface interface-name server-fail deny
  ```

- Configure an interface to move an end device to a specified VLAN if a RADIUS server timeout occurs:

  ```
  [edit protocols dot1x authenticator]
  user@switch# set interface interface-name server-fail vlan-name
  ```

- Configure an interface to recognize already connected end devices as reauthenticated if there is a RADIUS timeout during reauthentication (new end devices are denied access):

  ```
  [edit protocols dot1x authenticator]
  user@switch# set interface interface-name server-fail use-cache
  ```

You can configure an interface that receives a RADIUS access-reject message from the authentication server to move end devices attempting LAN access on the interface to a server-reject VLAN, a specified VLAN already configured on the switch.

To configure a server reject fallback VLAN:

- ```
  [edit protocols dot1x authenticator]
  user@switch# set interface interface-name server-reject-vlan vlan-sf
  ```

See Also

- Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 309
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- Monitoring 802.1X Authentication on page 320
  ```

Release History Table

Release	Description
14.1X53-D40	Server fail fallback is supported for voice traffic starting in Release 14.1X53-D40 and Release 15.1R4.

Related Documentation

- Access Control and Authentication on Switching Devices on page 267
- 802.1X Authentication on page 289
- 802.1X and RADIUS Accounting on page 332
- MAC RADIUS Authentication on page 324

802.1X Authentication

IEEE 802.1X standard for port-based network access control and protects Ethernet LANs from unauthorized user access. It blocks all traffic to and from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the authentication server (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant. Read this topic for more information.

- 802.1X for Switches Overview on page 289
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- Understanding RADIUS-Initiated Changes to an Authorized User Session on page 294
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 297
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Understanding Dynamic Filters Based on RADIUS Attributes on page 306
- Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 307
- Understanding Guest VLANs for 802.1X on Switches on page 308
- Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 309
- Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 315
- Monitoring 802.1X Authentication on page 320
- Verifying 802.1X Authentication on page 321
- Troubleshooting Authentication of End Devices on EX Series Switches on page 322

802.1X for Switches Overview

How 802.1X Authentication Works

802.1X authentication works by using an authenticator port access entity (the switch) to block ingress traffic from a supplicant (end device) at the port until the supplicant's

credentials are presented and match on the authentication server (a RADIUS server). When authenticated, the switch stops blocking traffic and opens the port to the supplicant.

The end device is authenticated in *single supplicant* mode, *single-secure supplicant* mode, or *multiple supplicant* mode:

- single supplicant—Authenticates only the first end device. All other end devices that connect later to the port are allowed full access without any further authentication. They effectively *piggyback* on the first end device's authentication.
- single-secure supplicant—Allows only one end device to connect to the port. No other end device is allowed to connect until the first device logs out.
- multiple supplicant—Allows multiple end devices to connect to the port. Each end device is authenticated individually.

Network access can be further defined by using VLANs and firewall filters, both of which act as filters to separate and match groups of end devices to the areas of the LAN they require. For example, you can configure VLANs to handle different categories of authentication failures depending upon:

- Whether or not the end device is 802.1X-enabled.
- Whether or not MAC RADIUS authentication is configured on the switch interfaces to which the hosts are connected.
- Whether the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message. See "Configuring RADIUS Server Fail Fallback (CLI Procedure)" on page 287.

802.1X Features Overview

The following 802.1X features are supported on Juniper Networks Ethernet Switches:

- Guest VLAN—Provides limited access to a LAN, typically only to the Internet, for nonresponsive end devices that are not 802.1X-enabled when MAC RADIUS authentication is not configured on the switch interfaces to which the hosts are connected. Also, a guest VLAN can be used to provide limited access to a LAN for guest users. Typically, the guest VLAN provides access only to the Internet and to other guests' end devices.
- Server-reject VLAN—Provides limited access to a LAN, typically only to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials. If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is not allowed.
- Server-fail VLAN—Provides limited access to a LAN, typically only to the Internet, for 802.1X end devices during a RADIUS server timeout.
- Dynamic VLAN—Enables an end device, after authentication, to be a member of a VLAN dynamically.
- Private VLAN—Enables configuration of 802.1X authentication on interfaces that are members of private VLANs (PVLANs).

- Dynamic changes to a user session—Enables the switch administrator to terminate an already authenticated session. This feature is based on support of the RADIUS Disconnect Message defined in RFC 3576.
- VoIP VLAN—Supports IP telephones. The implementation of a voice VLAN on an IP telephone is vendor-specific. If the phone is 802.1X-enabled, it is authenticated as any other supplicant is. If the phone is not 802.1X-enabled, but has another 802.1X-compatible device connected to its data port, that device is authenticated, and then VoIP traffic can flow to and from the phone (provided that the interface is configured in single supplicant mode and not in single-secure supplicant mode).

NOTE: **Configuring a VoIP VLAN on private VLAN (PVLAN) interfaces is not supported.**

- RADIUS accounting—Sends accounting information to the RADIUS accounting server. Accounting information is sent to the server whenever a subscriber logs in or logs out and whenever a subscriber activates or deactivates a subscription.
- RADIUS server attributes for 802.1X—The **Juniper-Switching-Filter** is a vendor-specific attribute (VSA) that can be configured on the RADIUS server to further define a supplicant's access during the 802.1X authentication process. Centrally configuring attributes on the authentication server obviates the need to configure these same attributes in the form of firewall filters on every switch in the LAN to which the supplicant might connect to the LAN. This feature is based on RLI 4583, AAA RADIUS BRAS VSA Support.

The following features are supported to authenticate devices that are not 802.1X-enabled:

- Static MAC bypass—Provides a bypass mechanism to authenticate devices that are not 802.1X-enabled (such as printers). Static MAC bypass connects these devices to 802.1X-enabled ports, bypassing 802.1X authentication.
- MAC RADIUS authentication—Provides a means to permit hosts that are not 802.1X-enabled to access the LAN. MAC-RADIUS simulates the supplicant functionality of the client device, using the MAC address of the client as username and password.

802.1X Authentication on Trunk Ports

Starting in Junos OS Release 18.4R1, you can configure 802.1X authentication on trunk interfaces, which allows the network access device (NAS) to authenticate an access point (AP) or another connected Layer 2 device. An AP or switch connected to the NAS will support multiple VLANs, so must connect to a trunk port. Enabling 802.1X authentication on the trunk interface protects the NAS from a security breach in which an attacker might disconnect the AP and connect a laptop to get free access to network for all the configured VLANs.

Please note the following caveats when configuring 802.1X authentication on trunk interfaces.

- Only single and single-secure supplicant modes are supported on trunk interfaces.
- You must configure 802.1X authentication locally on the trunk interface. If you configure 802.1X authentication globally using the **set protocol dot1x interface all** command, the configuration is not applied to the trunk interface.
- Dynamic VLANS are not supported on trunk interfaces.
- Guest VLAN and server-reject VLAN are not supported on trunk interfaces.
- Server fail fallback for VoIP clients is not supported on trunk interfaces (**server-fail-voip**).
- Authentication on trunk port is not supported using captive portal.
- Authentication on trunk port is not supported on aggregated interfaces.
- Configuration of 802.1X authentication on interfaces that are members of private VLANs (PVLANs) is not supported on trunk ports.

See Also

- Understanding Authentication on Switches on page 268
- Understanding 802.1X and VoIP on EX Series Switches on page 406
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518
- Understanding 802.1X and RADIUS Accounting on Switches on page 332
- Understanding Server Fail Fallback and Authentication on Switches on page 286

Configuring 802.1X Interface Settings (CLI Procedure)

IEEE 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the *authentication server* (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

NOTE:

- You can also specify an 802.1X exclusion list to specify supplicants that can bypass authentication and be automatically connected to the LAN. See "Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication (CLI Procedure)" on page 368.
- You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.

Before you begin, specify the RADIUS server or servers to be used as the authentication server. See "Specifying RADIUS Server Connections on Switches (CLI Procedure)" on page 283.

To configure 802.1X on an interface:

1. Configure the supplicant mode as **single** (authenticates the first supplicant), **single-secure** (authenticates only one supplicant), or **multiple** (authenticates multiple supplicants):

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface interface-name supplicant multiple
   ```

   NOTE: Multiple supplicant mode is not supported on trunk interfaces.

2. Enable reauthentication and specify the reauthentication interval:

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface interface-name reauthentication interval seconds
   ```

3. Configure the interface timeout value for the response from the supplicant:

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface interface-name supplicant-timeout seconds
   ```

4. Configure the timeout for the interface before it resends an authentication request to the RADIUS server:

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface interface-name server-timeout seconds
   ```

5. Configure how long, in seconds, the interface waits before retransmitting the initial EAPOL PDUs to the supplicant:

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface interface-name transmit-period seconds
   ```

6. Configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out:

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface interface-name maximum-requests number
   ```

7. Configure the number of times the switch attempts to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt.

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface interface-name retries number
   ```

   NOTE: This setting specifies the number of attempts before the switch puts the interface in a *HELD* state.

See Also

- *Configuring 802.1X Authentication (J-Web Procedure)*
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Configuring LLDP (CLI Procedure) on page 512
- Understanding Authentication on Switches on page 268

Understanding RADIUS-Initiated Changes to an Authorized User Session

When using an authentication service that is based on a client/server RADIUS model, requests are typically initiated by the client and sent to the RADIUS server. There are instances in which a request might be initiated by the server and sent to the client in order to dynamically modify an authenticated user session already in progress. The client that receives and processes the messages is the switch, which acts as the network access server, or NAS. The server can send the switch a Disconnect message requesting to terminate a session, or a Change of Authorization (CoA) message requesting to modify the session authorization attributes.

The switch listens for unsolicited RADIUS requests on UPD port 3799, and accepts requests only from a trusted source. Authorization to send a Disconnect or CoA request is determined based on the source address and the corresponding shared secret, which must be configured on the switch as well as on the RADIUS server. For more information about configuring the source address and shared secret on the switch, see "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.

- Disconnect Messages on page 294
- Change of Authorization Messages on page 295
- CoA Request Port Bounce on page 295
- Error-Cause Codes on page 296

Disconnect Messages

The RADIUS server sends a Disconnect-Request message to the switch in order to terminate a user session and discard all associated session context. The switch responds to a Disconnect-Request packet with a Disconnect-ACK message if the request is successful, that is, all associated session context is discarded and the user session is no longer connected, or with a Disconnect-NAK packet if the request fails, that is, the authenticator is unable to disconnect the session and discard all associated session context.

In Disconnect-Request messages, RADIUS attributes are used to uniquely identify the switch (NAS) and the user session. The combination of NAS identification attributes and session identification attributes included in the message must match at least one session for the request to be successful; otherwise, the switch responds with a Disconnect-NAK message. A Disconnect-Request message can contain only NAS and session identification attributes; if any other attributes are included, the switch responds with a Disconnect-NAK message.

Change of Authorization Messages

Change of Authorization (CoA) messages contain information for dynamically modifying the authorization attributes for a user session to change the authorization level. This occurs as part of a two-step authentication process, in which the endpoint is first authenticated using MAC RADIUS authentication, and is then profiled based on the type of device. The CoA message is used to apply an enforcement policy that is appropriate for the device, typically by changing the data filters or the VLAN.

The switch responds to a CoA message with a CoA-ACK message if the authorization change is successful, or a with CoA-NAK message if the change is unsuccessful. If one or more authorization changes specified in a CoA-Request message cannot be carried out, the switch responds with a CoA-NAK message.

In CoA-Request messages, RADIUS attributes are used to uniquely identify the switch (acting as the NAS) and the user session. The combination of NAS identification attributes and session identification attributes included in the message must match the identification attributes of at least one session for the request to be successful; otherwise, the switch responds with a CoA-NAK message.

CoA-Request packets also include the session authorization attributes that will be modified if the request is accepted. The supported session authorization attributes are listed below. The CoA message can contain any or all of these attributes. If any attribute is not included as part of the CoA-Request message, the NAS assumes that the value for that attribute is to remain unchanged.

- Filter-ID
- Tunnel-Private-Group-ID
- Juniper-Switching-Filter
- Juniper-VoIP-VLAN
- Session-Timeout

CoA Request Port Bounce

When a CoA message is used to change the VLAN for an authenticated host, end devices such as printers do not have a mechanism to detect the VLAN change, so they do not renew the lease for their DHCP address in the new VLAN. Starting in Junos OS Release 17.3, the port bounce feature can be used to force the end device to initiate DHCP re-negotiation by causing a link flap on the authenticated port.

The command to bounce the port is sent from the RADIUS server using a Juniper Networks vendor-specific attribute (VSA). The port is bounced if the following VSA attribute-value pair is received in the CoA message from the RADIUS server:

- Juniper-AV-Pair = “Port-Bounce”

To enable the port bounce feature, you must update the Junos dictionary file (**juniper.dct**) on the RADIUS server with the Juniper-AV-Pair VSA. Locate the dictionary file and add the following text to the file:

```
ATTRIBUTE Juniper-AV-Pair  Juniper-VSA(52, string) r
```

For more information about adding the VSA, consult the FreeRADIUS documentation.

You can disable the feature by configuring the ignore-port-bounce statement at the [**edit protocols dot1x authenticator interface interface-name mac-radius**] hierachy level.

Error-Cause Codes

When a disconnect or CoA operation is unsuccessful, an Error-Cause attribute (RADIUS attribute 101) can be included in the response message sent by the NAS to the server to provide detail about the cause of the problem. If the detected error does not map to one of the supported Error-Cause attribute values, the router sends the message without an error-cause attribute. See Table 20 on page 296 for descriptions of error-cause codes that can be included in response messages sent from the NAS.

Table 20: Error-Cause Codes (RADIUS Attribute 101)

Code	Value	Description
201	Residual session context removed	Sent in response to a Disconnect-Request message if one or more user sessions are no longer active, but residual session context was found and successfully removed. This code is sent only within a Disconnect-ACK message.
401	Unsupported attribute	The request contains an attribute that is not supported (for example, a third-party attribute).
402	Missing attribute	A critical attribute (for example, the session identification attribute) is missing from a request.
403	NAS identification mismatch	Request contains one or more NAS identification attributes that do not match the identity of the NAS receiving the request.
404	Invalid request	Some other aspect of the request is invalid—for example, if one or more attributes are not formatted properly.
405	Unsupported service	The Service-Type attribute included with the request contains an invalid or unsupported value.
406	Unsupported extension	The entity receiving the request (either an NAS or a RADIUS proxy) does not support RADIUS-initiated requests.
407	Invalid attribute value	The request contains an attribute with an unsupported value.

Table 20: Error-Cause Codes (RADIUS Attribute 101) (continued)

Code	Value	Description
501	Administratively prohibited	The NAS is configured to prohibit honoring of Disconnect-Request or CoA-Request messages for the specified session.
503	Session context not found	The session context identified in the request does not exist on the NAS.
504	Session context not removable	The subscriber identified by attributes in the request is owned by a component that is not supported. This code is sent only within a Disconnect-NAK message.
506	Resources unavailable	A request could not be honored because of lack of available NAS resources (such as memory).
507	Request initiated	The CoA-Request message includes a Service-Type attribute with a value of Authorize Only.
508	Multiple session selection unsupported	The session identification attributes included in the request match multiple sessions, but the NAS does not support requests that apply to multiple sessions.

Filtering 802.1X Supplicants by Using RADIUS Server Attributes

There are two ways to configure the a RADIUS server with port firewall filters (Layer 2 firewall filters):

- Include one or more filter terms in the Juniper-Switching-Filter attribute. The Juniper-Switching-Filter attribute is a vendor-specific attribute (VSA) listed under attribute ID number 48 in the Juniper dictionary on the RADIUS server. Use this VSA to configure simple filter conditions for 802.1X authenticated users. Nothing needs to be configured on the switch; all of the configuration is on the RADIUS server.
- Configure a local firewall filter on each switch and apply that firewall filter to users authenticated through the RADIUS server. Use this method for more complex filters. The firewall filter must be configured on each switch.

NOTE: **If the firewall filter configuration is modified after users are authenticated using the 802.1X authentication, then the established 802.1X authentication session must be terminated and re-established for the firewall filter configuration changes to take effect.**

This topic includes the following tasks:

1. Configuring Firewall Filters on the RADIUS Server on page 298
2. Applying a Locally Configured Firewall Filter from the RADIUS Server on page 301

Configuring Firewall Filters on the RADIUS Server

You can configure simple filter conditions by using the Juniper-Switching-Filter attribute in the Juniper dictionary on the RADIUS server. These filters are sent to a switch whenever a new user is authenticated successfully. The filters are created and applied on all EX Series switches that authenticate users through that RADIUS server without the need for you to configure anything on each individual switch.

NOTE: This procedure describes using FreeRADIUS software to configure the Juniper-Switching-Filter VSA. For specific information about configuring your server, consult the AAA documentation included with your server.

To configure the Juniper-Switching-Filter attribute, enter one or more filter terms by using the CLI for the RADIUS server. Each filter term consists of match conditions with a corresponding action. Enter the filter terms enclosed within quotation marks (" ") by using the following syntax:

```
Juniper-Switching-Filter = “match <destination-mac mac-address> <source-vlan
  vlan-name> <source-dot1q-tag tag> <destination-ip ip-address> <ip-protocol
  protocol-id> <source-port port> <destination-port port> action (allow | deny)
  <forwarding-class class-of-service> <loss-priority (low | medium | high)>”
```

More than one match condition can be included in a filter term. When multiple conditions are specified in a filter term, they must all be fulfilled for the packet to match the filter term. For example, the following filter term requires a packet to match *both* the destination IP address and the destination MAC address to meet the term criteria:

```
Juniper-Switching-Filter = “match destination-ip 10.10.10.8 destination-mac
  00:00:00:01:02:03 action allow”
```

Multiple filter terms should be separated with commas—for example:

```
Juniper-Switching-Filter = “match destination-mac 00:00:00:01:02:03 action allow,
  match destination-port 80 destination-mac 00:aa:bb:cc:dd:ee action allow”
```

See “Juniper-Switching-Filter VSA Match Conditions and Actions” on page 197 for definitions of match conditions and actions.

NOTE: On EX9200 switches, and in a Junos Fusion Enterprise with EX9200 as the aggregate device, the dynamic firewall filter is strictly applied for all IP packets. If the filter is configured to allow only a specific destination IP address, packets with other IP addresses as the destination IP will be dropped per the filter rules. This includes any IP protocol packets, such as DHCP, IGMP and ARP packets.

To configure match conditions on the RADIUS server:

1. Verify that the Juniper dictionary is loaded on your RADIUS server and includes the filtering attribute **Juniper-Switching-Filter** (attribute ID 48):

```
[root@freeradius]# cat /usr/local/share/freeradius/dictionary.juniper

#  dictionary.juniper
#
# Version:      $Id: dictionary.juniper,v 1.2.6.1 2005/11/30 22:17:25 aland
Exp
$
#  VENDOR          Juniper                          2636
BEGIN-VENDOR    Juniper
ATTRIBUTE       Juniper-Local-User-Name                 1       string
ATTRIBUTE       Juniper-Allow-Commands                  2       string
ATTRIBUTE       Juniper-Deny-Commands                   3       string
ATTRIBUTE       Juniper-Allow-Configuration             4       string
ATTRIBUTE       Juniper-Deny-Configuration              5       string
ATTRIBUTE       Juniper-Switching-Filter                48      string
<–
```

2. Enter the match conditions and actions. For example:

   - To deny authentication based on the 802.1Q tag (here, the 802.1Q tag is **10**):

     ```
     [root@freeradius]#
     cd /usr/local/etc/raddb
     vi users
     ```

     For each relevant user, add the **Juniper-Switching-Filter** attribute:

     Juniper-Switching-Filter = "Match Source-dot1q-tag 10 Action deny"

   - To deny access based on a destination IP address:

     ```
     [root@freeradius]# cd /usr/local/etc/raddb
     vi users
     ```

     For each relevant user, add the **Juniper-Switching-Filter** attribute:

     Juniper-Switching-Filter = “Match Destination-ip 192.168.1.0/31 Action deny”

   - To set the packet loss priority (PLP) to **high** based on a destination MAC address and the IP protocol:

     ```
     [root@freeradius]# cd /usr/local/etc/raddb
     vi users
     ```

     For each relevant user, add the **Juniper-Switching-Filter** attribute:

     Juniper-Switching-Filter = "Match Destination-mac 00:04:0f:fd:ac:fe, Ip-protocol 2, forwarding-class high, Action loss-priority high"

NOTE: For the forwarding-class option to be applied, the forwarding class must be configured on the switch and the packet loss priority specified. If it is not configured on the switch, this option is ignored. You must specify both the forwarding class and the packet loss priority.

3. Stop and restart the RADIUS process to activate the configuration.

Applying a Locally Configured Firewall Filter from the RADIUS Server

You can apply a port firewall filter (Layer 2 firewall filter) to user policies centrally from the RADIUS server. The RADIUS server can then specify the firewall filters that are to be applied to each user that requests authentication, reducing the need to configure the same firewall filter on multiple switches. Use this method when the firewall filter contains a large number of conditions or you want to use different conditions for the same filter on different switches. The firewall filters must be configured on each switch.

For more information about firewall filters, see *Firewall Filters for EX Series Switches Overview*.

To apply a port firewall filter centrally from the RADIUS server:

NOTE: If port firewall filters are also configured locally for the interface, then the firewall filters configured by using VSAs take precedence if they conflict with the locally configured port firewall filters. If there is no conflict, they are merged.

1. Create the firewall filter on the local switch. See *Configuring Firewall Filters (CLI Procedure)* for more information on configuring a port firewall filter.

2. On the RADIUS server, open the **users** file to display the local user profiles of the end devices to which you want to apply the filter:

   ```
   [root@freeradius]#
   cat /usr/local/etc/raddb/usersvi users
   ```

3. Apply the filter to each user profile by adding the Filter-ID attribute with the filter name as the attribute value:

   Filter-Id =*filter-name*

   For example, the user profile below for **supplicant1** includes the Filter-ID attribute with the filter name **filter1**:

   ```
   [root@freeradius]# cat /usr/local/etc/raddb/users

   supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
           Tunnel-Type = VLAN,
           Tunnel-Medium-Type = IEEE-802,
           Tunnel-Private-Group-Id = "1005",
           Filter-Id = "filter1"
   ```

   NOTE: Multiple filters are not supported on a single interface. However, you can support multiple filters for multiple users that are connected to

the switch on the same interface by configuring a single filter with policies for each of those users.

4. Stop and restart the RADIUS process to activate the configuration.

See Also

- Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch on page 349
- *Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches*

Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch

802.1X is the IEEE standard for port-based network access control (PNAC). You use 802.1X to control network access. Only users and devices providing credentials that have been verified against a user database are allowed access to the network. You can use a RADIUS server as the user database for 802.1X authentication, as well as for MAC RADIUS authentication.

This example describes how to connect a RADIUS server to an EX Series switch, and configure it for 802.1X:

Requirements

This example uses the following software and hardware components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support*

. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

NOTE: For more about ELS, see *Using the Enhanced Layer 2 Software CLI*.

- Configured users on the RADIUS authentication server.

Overview and Topology

The EX Series switch acts as an authenticator PAE. It blocks all traffic and acts as a control gate until the supplicant (client) is authenticated by the server. All other users and devices are denied access.

Figure 7 on page 304 shows one EX4200 switch that is connected to the devices listed in Table 21 on page 304.

Figure 7: Topology for Configuration

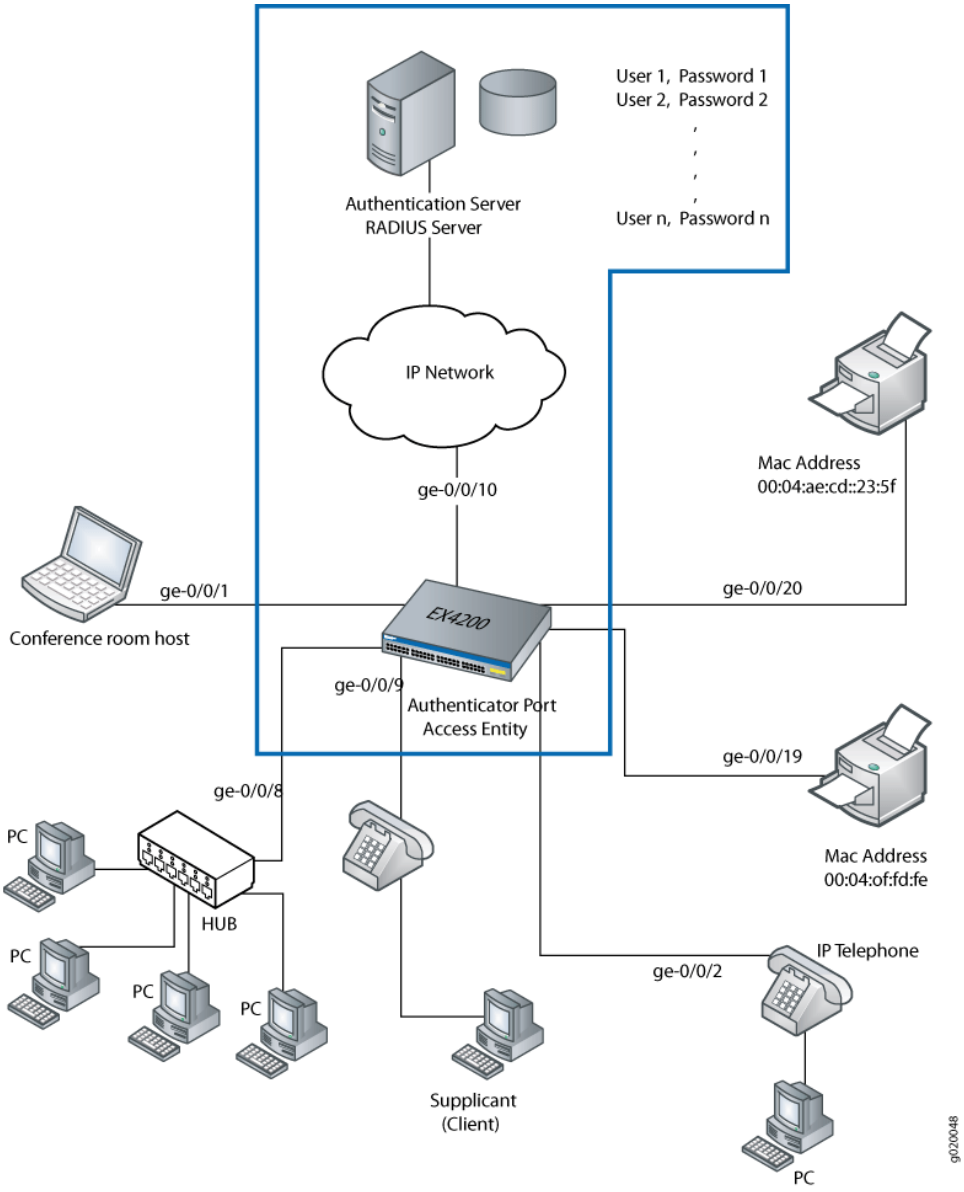


Table 21: Components of the Topology

Property	Settings
Switch hardware	EX4200 access switch, 24 Gigabit Ethernet ports: 8 PoE ports (ge-0/0/0 through ge-0/0/7) and 16 non-PoE ports (ge-0/0/8 through ge-0/0/23)
VLAN name	default
One RADIUS server	Backend database with an address **10.0.0.100** connected to the switch at port **ge-0/0/10**

In this example, connect the RADIUS server to access port ge-0/0/10 on the EX4200 switch. The switch acts as the authenticator and forwards credentials from the supplicant to the user database on the RADIUS server. You must configure connectivity between the EX4200 and the RADIUS server by specifying the address of the server and configuring the secret password. This information is configured in an access profile on the switch.

NOTE: For more information about authentication, authorization, and accounting (AAA) services, see the *Junos OS System Basics Configuration Guide*.

Configuration

CLI Quick Configuration

To quickly connect the RADIUS server to the switch, copy the following commands and paste them into the switch terminal window:

```
[edit]
set access radius-server 10.0.0.100 secret juniper
set access radius-server 10.0.0.200 secret juniper
set access profile profile1 authentication-order radius
set access profile profile1 radius authentication-server [10.0.0.100 10.0.0.200]
```

Step-by-Step Procedure

To connect the RADIUS server to the switch:

1. Define the address of the servers, and configure the secret password. The secret password on the switch must match the secret password on the server:

   ```
   [edit]
   user@switch# set access radius-server 10.0.0.100 secret juniper
   user@switch# set access radius-server 10.0.0.200 secret juniper
   ```

2. Configure the authentication order, making **radius** the first method of authentication:

   ```
   [edit]
   user@switch# set access profile profile1 authentication-order radius
   ```

3. Configure a list of server IP addresses to be tried in sequential order to authenticate the supplicant:

   ```
   [edit]
   user@switch# set access profile profile1 radius authentication-server [10.0.0.100
   10.0.0.200]
   ```

Results

Display the results of the configuration:

```
user@switch> show configuration access
radius-server {
   10.0.0.100
      port 1812;
      secret "$ABC123"; ## SECRET-DATA
      }
```

```
    }
    profile profile1{
      authentication-order radius;
      radius {
        authentication-server 10.0.0.100 10.0.0.200;
      }
    }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verify That the Switch and RADIUS Server Are Properly Connected on page 306

Verify That the Switch and RADIUS Server Are Properly Connected

Purpose Verify that the RADIUS server is connected to the switch on the specified port.

Action Ping the RADIUS server to verify the connection between the switch and the server:

```
user@switch> ping 10.0.0.100
PING 10.0.0.100 (10.0.0.100): 56 data bytes
64 bytes from 10.93.15.218: icmp_seq=0 ttl=64 time=9.734 ms
64 bytes from 10.93.15.218: icmp_seq=1 ttl=64 time=0.228 ms
```

Meaning ICMP echo request packets are sent from the switch to the target server at 10.0.0.100 to test whether the server is reachable across the IP network. ICMP echo responses are being returned from the server, verifying that the switch and the server are connected.

See Also

- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 343
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335

Understanding Dynamic Filters Based on RADIUS Attributes

You can use RADIUS server attributes to implement port firewall filters on a RADIUS authentication server. These filters can be dynamically applied to supplicants that request authentication through that server. RADIUS server attributes are clear-text fields encapsulated in Access-Accept messages sent from the authentication server to the switch when a supplicant connected to the switch is successfully authenticated. The

switch, acting as the authenticator, uses the information in the RADIUS attributes to apply the related filters to the supplicant. Dynamic filters can be applied to multiple ports on the same switch, or to multiple switches that the use same authentication server, providing centralized access control for the network.

You can define firewall filters directly on the RADIUS server by using the Juniper-Switching-Filter attribute, which is a RADIUS attribute specific to Juniper Networks, also known as a vendor-specific attribute (VSA). VSAs are described in RFC 2138, *Remote Authentication Dial In User Service* (RADIUS). The Juniper-Switching-Filter VSA is listed under attribute ID number 48 in the Juniper dictionary on the RADIUS server, with the vendor ID set to the Juniper Networks ID number 2636. Using this attribute, you define filters on the authentication server, which are applied on all switches that authenticate supplicants through that server. This method eliminates the need to configure the same filters on multiple switches.

Alternatively, you can apply a port firewall filter to multiple ports on the same switch by using the Filter-ID attribute, which is RADIUS attribute ID number 11. To use the Filter-ID attribute, you must first configure a filter on the switch, and then add the filter name to user policies on the RADIUS server as the value of the Filter-ID attribute. When a supplicant defined in one of those policies is authenticated by the RADIUS server, the filter is applied to the switch port that has been authenticated for the supplicant. Use this method when the firewall filter has complex conditions, or if you want to use different conditions for the same filter on different switches. The filter named in the Filter-ID attribute must be configured locally on the switch at the [**edit firewall family ethernet-switching filter**] hierarchy level.

VSAs are supported only for 802.1X single supplicant configurations and multiple supplicant configurations.

See Also

- Understanding Authentication on Switches on page 268
- Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch on page 349
- *Configuring Firewall Filters (CLI Procedure)*
- Juniper-Switching-Filter VSA Match Conditions and Actions on page 197

Understanding Dynamic VLAN Assignment Using RADIUS Attributes

VLANs can be dynamically assigned by a RADIUS server to supplicants requesting 802.1X authentication through that server. You configure the VLAN on the RADIUS server using RADIUS server attributes, which are clear-text fields encapsulated in messages sent from the authentication server to the switch when a supplicant connected to the switch requests authentication. The switch, acting as the authenticator, uses the information in the RADIUS attributes to assign the VLAN to the supplicant. Based on the results of the authentication, a supplicant that began authentication in one VLAN might be assigned to another VLAN.

Successful authentication requires that the VLAN ID or VLAN name is configured on the switch acting as 802.1X authenticator, and that it matches the VLAN ID or VLAN name

sent by the RADIUS server during authentication. If neither exists, the end device is not authenticated. If a guest VLAN is established, the unauthenticated end device is automatically moved to the guest VLAN.

The RADIUS server attributes used for dynamic VLAN assignment described in RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*.

- Tunnel-Type—Defined as RADIUS attribute type 64. The value should be set to **VLAN**.
- Tunnel-Medium-Type—Defined as RADIUS attribute type 65. The value should be set to **IEEE-802**.
- Tunnel-Private-Group-ID—Defined as RADIUS attribute type 81. The value should be set to the VLAN ID or the VLAN name.

For more information about configuring dynamic VLANs on your RADIUS server, see the documentation for your RADIUS server.

See Also
- Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 326
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 343

Understanding Guest VLANs for 802.1X on Switches

Guest VLANs can be configured on switches that are using 802.1X authentication to provide limited access—typically only to the Internet—for:

- Corporate guests
- End devices that are not 802.1X-enabled
- Nonresponsive end devices when MAC RADIUS authentication has not been configured on the switch interfaces to which the hosts are connected

A guest VLAN is not used for supplicants that send incorrect credentials. Those supplicants are directed to the server-reject VLAN instead.

For end devices that are not 802.1X-enabled, a guest VLAN can allow limited access to a server from which the non-802.1X-enabled end device can download the supplicant software and attempt authentication again.

A guest VLAN is not used when MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected.

See Also
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 343
- Understanding Authentication on Switches on page 268

Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch

Server fail fallback enables you to specify how 802.1X supplicants connected to the switch are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

You use 802.1X to control network access. Only users and devices (supplicants) providing credentials that have been verified against a user database are allowed access to the network. You use a RADIUS server as the user database.

This example describes how to configure an interface to move a supplicant to a VLAN in the event of a RADIUS server timeout:

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.3 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*. For all other switches, see*Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

  NOTE: For more about ELS, see *Using the Enhanced Layer 2 Software CLI*.

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.

- Configured users on the authentication server.

Overview and Topology

A RADIUS server timeout occurs if no authentication RADIUS servers are reachable when a supplicant logs in and attempts to access the LAN. Using server fail fallback, you configure alternative options for supplicants attempting LAN access. You can configure the switch to accept or deny access to supplicants or to maintain the access already granted to supplicants before the RADIUS server timeout. Additionally, you can configure the switch to move supplicants to a specific VLAN if a RADIUS timeout occurs or if the RADIUS server sends an EAP Access-Reject message.

Figure 8 on page 311 shows the topology used for this example. The RADIUS server is connected to the EX4200 switch on access port **ge-0/0/10**. The switch acts as the authenticator port access entity (PAE) and forwards credentials from the supplicant to the user database on the RADIUS server. The switch blocks all traffic and acts as a control gate until the supplicant is authenticated by the authentication server. A supplicant is connected to the switch through interface ge-0/0/1.

NOTE: This figure also applies to QFX5100 switches.

Figure 8: Topology for Configuring 802.1X Options

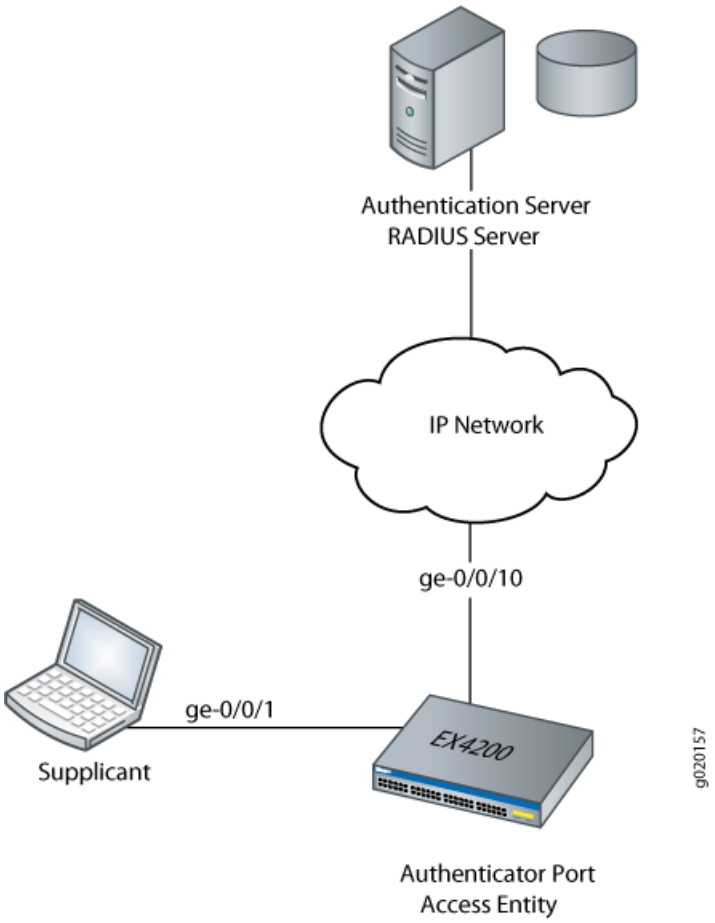


Table 22 on page 311 describes the components in this topology.

Table 22: Components of the Topology

Property	Settings
Switch hardware	EX4200 access switch, 24 Gigabit Ethernet ports: 16 non-PoE ports and 8 PoE ports.
VLAN names	**default** VLAN **vlan-sf** VLAN
Supplicant	Supplicant attempting access on interface **ge-0/0/1**
One RADIUS server	Backend database with an address of **10.0.0.100** connected to the switch at port **ge-0/0/10**

In this example, configure interface ge-0/0/1 to move a supplicant attempting access to the LAN during a RADIUS timeout to another VLAN. A RADIUS timeout prevents the normal exchange of EAP messages that carry information from the RADIUS server to the

switch and permit the authentication of a supplicant. The default VLAN is configured on interface ge-0/0/1. When a RADIUS timeout occurs, supplicants on the interface will be moved from the default VLAN to the VLAN named vlan-sf.

Configuration

CLI Quick Configuration

To quickly configure server fail fallback on the switch, copy the following commands and paste them into the switch terminal window:

```
[edit protocols dot1x authenticator]
set interface ge-0/0/1 server-fail vlan-name vlan-sf
```

Step-by-Step Procedure

To configure an interface to divert supplicants to a specific VLAN when a RADIUS timeout occurs (here, the VLAN is **vlan-sf**):

1. Define the VLAN to which supplicants are diverted:

```
[edit protocols dot1x authenticator]
user@switch# set interface ge-0/0/1 server-fail vlan-name vlan-sf
```

Results

Display the results of the configuration:

```
user@switch> show configuration
  interfaces {
    ge-0/0/1 {
      unit 0 {
        family ethernet-switching {
          vlan {
            members default;
          }
        }
      }
    }
  protocols {
    dot1x {
      authenticator {
        interface {
          ge-0/0/1.0 {
            server-fail vlan-name vlan-sf;
          }
        }
      }
    }
  }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That the Supplicants Are Moved to an Alternative VLAN During a RADIUS Timeout on page 313

Verifying That the Supplicants Are Moved to an Alternative VLAN During a RADIUS Timeout

Purpose Verify that the interface moves supplicants to an alternative VLAN during a RADIUS timeout.

NOTE: On switches running Junos OS for EX Series with support for ELS, the output for the **show vlans** command will contain additional information. If your switch runs software that supports ELS, see *show vlans*. For ELS details, see *Using the Enhanced Layer 2 Software CLI*

Action Display the VLANs configured on the switch; the interface **ge-0/0/1.0** is a member of the **default** VLAN:

```
user@switch> show vlans
Name            Tag     Interfaces
default
                        ge-0/0/0.0, ge-0/0/1.0*, ge-0/0/5.0*, ge-0/0/10.0,
                        ge-0/0/12.0*, ge-0/0/14.0*, ge-0/0/15.0, ge-0/0/20.0
v2              77
                        None
vlan-sf         50
                        None
mgmt
                        me0.0*
```

Display 802.1X protocol information on the switch to view supplicants that are authenticated on interface **ge-0/0/1.0**:

```
user@switch> show dot1x interface brief
802.1X Information:
Interface     Role           State           MAC address          User
ge-0/0/1.0    Authenticator  Authenticated   00:00:00:00:00:01    abc
ge-0/0/10.0   Authenticator  Initialize
ge-0/0/14.0   Authenticator  Connecting
ge-0/0/15.0   Authenticator  Initialize
ge-0/0/20.0   Authenticator  Initialize
```

A RADIUS server timeout occurs. Display the Ethernet switching table to show that the supplicant with the MAC address **00:00:00:00:00:01** previously accessing the LAN through the **default** VLAN is now being learned on the VLAN named **vlan-sf**:

```
user@switch> show ethernet-switching table
Ethernet-switching table: 3 entries, 1 learned
  VLAN              MAC address       Type         Age Interfaces
  v1                *                 Flood          - All-members
  vlan-sf           00:00:00:00:00:01 Learn       1:07 ge-0/0/1.0
  default           *                 Flood          - All-members
```

Display 802.1X protocol information to show that interface **ge-0/0/1.0** is connecting and will open LAN access to supplicants:

```
user@switch> show dot1x interface brief

802.1X Information:
Interface     Role           State           MAC address          User
ge-0/0/1.0    Authenticator  Connecting
ge-0/0/10.0   Authenticator  Initialize
ge-0/0/14.0   Authenticator  Connecting
ge-0/0/15.0   Authenticator  Initialize
ge-0/0/20.0   Authenticator  Initialize
```

Meaning The **show vlans** command displays interface **ge-0/0/1.0** as a member of the **default** VLAN. The **show dot1x interface brief** command shows that a supplicant (**abc**) is authenticated on interface **ge-0/0/1.0** and has the MAC address **00:00:00:00:00:01**. A RADIUS server timeout occurs, and the authentication server cannot be reached by the switch. The **show-ethernet-switching table** command shows that MAC address **00:00:00:00:00:01** is learned on VLAN **vlan-sf**. The supplicant has been moved from the **default** VLAN to the **vlan-sf** VLAN. The supplicant is then connected to the LAN through the VLAN named **vlan-sf**.

See Also

- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Configuring RADIUS Server Fail Fallback (CLI Procedure) on page 287
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335
- Understanding Server Fail Fallback and Authentication on Switches on page 286

Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients

For 802.1X user authentication, EX Series switches support RADIUS authentication servers that are using Extensible Authentication Protocol–Tunneled TLS (EAP-TTLS) to authenticate Odyssey Access Client (OAC) supplicants. OAC networking software runs on endpoint computers (desktop, laptop, or notepad computers and supported wireless devices) and provides secure access to both wired and wireless networks.

This example describes how to configure an 802.1X-enabled interface on the switch to provide fallback support for OAC users who have entered incorrect login credentials:

Requirements

This example uses the following software and hardware components:

NOTE: **This example also applies to QFX5100 switches.**

- Junos OS Release 11.2 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.

- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.
- One OAC end device acting as a supplicant.

Before you begin configuring the fallback option, ensure that you have:

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.
- Configured EAP-TTLS on the server. See your RADIUS server documentation.
- Configured users on the RADIUS server. See your RADIUS server documentation.

Overview and Topology

OAC is networking software that runs on endpoint computers (desktop, laptop, or notepad) and supported wireless devices. OAC provides full support for EAP, which is required for secure wireless LAN access.

In this topology, OAC is deployed with an 802.1X-enabled switch and a RADIUS server. The switch functions as an enforcement point in the network security architecture. This topology:

- Ensures that only authorized users can connect.
- Maintains privacy of login credentials.
- Maintains data privacy over the wireless link.

This example includes the configuration of a server-reject VLAN on the switch, which can be used to prevent accidental lockout for users who have entered incorrect login credentials. These users can be given limited LAN access.

However, this fallback configuration is complicated by the fact that the OAC supplicant and RADIUS server are using EAP-TTLS. EAP-TTLS creates a secure encrypted tunnel between the server and the end device to complete the authentication process. When the user enters incorrect login credentials, the RADIUS server sends EAP failure messages directly to the client through this tunnel. The EAP failure message causes the client to restart the authentication procedure, so that the switch's 802.1X authentication process tears down the session that was established with the switch using the server-reject VLAN. You can enable the remedial connection to continue by configuring:

- **eapol-block**—Enable the EAPoL block timer on the 802.1X interface that is configured to belong to the server-reject VLAN. The block timer causes the authentication port access entity to ignore EAP start messages from the client, attempting to restart the authentication procedure.

NOTE: The EAPoL block timer is triggered only after the configured number of allowed reattempts (using the **retries** option) on the 802.1X interface have been exhausted. You can configure **retries** to specify the number of times the switch attempts to authenticate the port after an initial failure. The default is three retries.

- **block-interval**—Configure the amount of time that you want the EAPoL block timer to continue to ignore EAP start messages. If you do not configure the block interval, the EAPoL block timer defaults to 120 seconds.

When the 802.1X interface ignores the EAP start messages from the client, the switch allows the existing remedial session that was established through the server-reject VLAN to remain open.

These configuration options apply to single, single-secure, and multiple supplicant authentication modes. In this example, the 802.1X interface is configured in single supplicant mode.

Figure 9 on page 317 shows an EX Series switch connecting an OAC end device to a RADIUS server, and indicates the protocols being used to connect the network entities.

NOTE: This figure also applies to QFX5100 switches.

Figure 9: EX Series Switch Connecting OAC to RADIUS Server Using EAP-TTLS Authentication

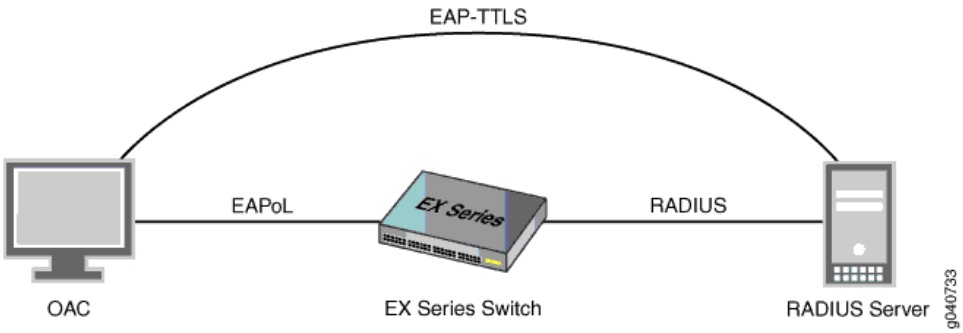


Table 23 on page 317 describes the components in this OAC deployment:.

Table 23: Components of the OAC Deployment

Property	Settings
Switch hardware	EX Series switch
VLANs	**default** **server-reject-vlan**: VLAN name is **remedial** and VLAN ID is **700**
802.1X interface	**ge-0/0/8**

Table 23: Components of the OAC Deployment (continued)

Property	Settings
OAC supplicant	EAP-TTLS
One RADIUS authentication server	EAP-TTLS

Configuration

CLI Quick Configuration

To quickly configure the fallback options for EAP-TTLS and OAC supplicants, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans remedial vlan-id 700
set protocols dot1x authenticator interface ge-0/0/8 retries 4
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan remedial
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan eapol-block
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan block-interval 130
```

Step-by-Step Procedure

To configure the fallback options for EAP-TTLS and OAC supplicants:

TIP: In this example, the switch has only one server-reject VLAN. Therefore, the configuration specifies **eapol-block** and **block-interval** directly after **server-reject-vlan**. However, if you have configured multiple VLANs on the switch, you must include the VLAN name or VLAN ID directly after **server-reject-vlan** to indicate which VLAN is being modified.

1. Configure a VLAN that will function as the server-reject VLAN to provide limited LAN access for users who have entered incorrect login credentials:

   ```
   [edit]
   user@switch# set vlans remedial vlan-id 700
   ```

2. Configure the number of times for the client to be prompted for username and password before an incorrect login is directed to the server-reject VLAN:

   ```
   [edit protocols dot1x authenticator interface ge-0/0/8]
   user@switch# set retries 4
   ```

3. Configure the 802.1X authenticator interface to use the server-reject VLAN as a fallback for incorrect logins:

   ```
   [edit protocols dot1x authenticator interface ge-0/0/8]
   user@switch# set server-reject-vlan remedial
   ```

4. Enable the EAPoL block timer on the 802.1X interface that is configured to belong to the server-reject VLAN.

   ```
   [edit protocols dot1x authenticator interface ge-0/0/8]
   ```

```
user@switch# set server-reject-vlan eapol-block
```

5. Configure the amount of time for the EAPoL block to remain in effect:

```
[edit protocols dot1x authenticator interface ge-0/0/8]
user@switch# set server-reject-vlan block-interval 130
```

Results

Check the results of the configuration:

```
user@switch> show configuration
  protocols {
    dot1x {
      authenticator {
        interface {
          ge-0/0/8.0 {
            supplicant single;
            retries 4;
            server-reject-vlan remedial block-interval 130 eapol-block;
          }
```

Verification

To confirm that the configuration and the fallback options are working correctly, perform this task:

- Verifying the Configuration of the 802.1X Interface on page 319

Verifying the Configuration of the 802.1X Interface

Purpose Verify that the 802.1X interface is configured with the desired options.

Action `user@switch>` **show dot1x interface ge-0/0/8.0 detail**

```
ge-0/0/8.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 4
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 120 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPoL requests: 2
  Guest VLAN member: guest
  Number of connected supplicants: 1
    Supplicant: tem, 2A:92:E6:F2:00:00
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Radius
      Authenticated VLAN: remedial
      Session Reauth interval: 120 seconds
      Reauthentication due in 68 seconds
```

Meaning The **show dot1x ge-0/0/8 detail** command output shows that the **ge-0/0/8** interface is in the **Authenticated** state and that it is using the **remedial** VLAN.

See Also

- Understanding Authentication on Switches on page 268

Monitoring 802.1X Authentication

Purpose

NOTE: This topic applies only to the J-Web Application package.

J-Web Application package Release 14.1X53-A2 does not support 802.1X authentication on EX4600 switches.

Use the monitoring feature to display details of authenticated users and users that failed authentication.

Action To display authentication details in the J-Web interface, select **Monitoring** > **Security** > **802.1X**.

To display authentication details in the CLI, enter the following commands:

- **show dot1x interface detail | display xml**
- **show dot1x interface detail** *<interface>* **| display xml**

- **show dot1x auth-failed-users**

Meaning The details displayed include:

- A list of authenticated users.
- The number of connected users.
- A list of users that failed authentication.

You can also specify an interface for which the details must be displayed.

See Also
- *Configuring 802.1X Authentication (J-Web Procedure)*
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337

Verifying 802.1X Authentication

Purpose Verify that supplicants are being authenticated on an interface on a switch with the interface configured for 802.1X authentication, and display the method of authentication being used.

Action Display detailed information about an interface configured for 802.1X (here, the interface is ge-0/0/16):

```
user@switch> show dot1x interface ge-0/0/16.0 detail
ge-0/0/16.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Strict: Disabled
  Reauthentication: Enabled Reauthentication interval: 40 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 1
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user5, 00:30:48:8C:66:BD
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: v200
      Reauthentication due in 17 seconds
```

Meaning The sample output from the **show dot1x interface detail** command shows that the **Number of connected supplicants** is 1. The supplicant that was authenticated and is now connected

to the LAN is known as **user5** on the RADIUS server and has the MAC address **00:30:48:8C:66:BD**. The supplicant was authenticated by means of the 802.1X authentication method called RADIUS authentication, as indicated by **Radius** in the output. When RADIUS authentication is used, the supplicant is configured on the RADIUS server, the RADIUS server communicates this to the switch, and the switch opens LAN access on the interface to which the supplicant is connected. The sample output also shows that the supplicant is connected to VLAN **v200**.

Other 802.1X authentication methods supported on EX Series switches in addition to RADIUS authentication are:

- Guest VLAN—A nonresponsive host is granted Guest-VLAN access.
- MAC Radius—A nonresponsive host is authenticated based on its MAC address. The MAC address is configured as permitted on the RADIUS server, the RADIUS server notifies the switch that the MAC address is a permitted address, and the switch grants LAN access to the nonresponsive host on the interface to which it is connected.
- Server-fail deny—If the RADIUS servers time out, all supplicants are denied access to the LAN, preventing traffic from the supplicant from traversing through the interface. This is the default.
- Server-fail permit—When the RADIUS server is unavailable, a supplicant is still permitted access to the LAN as if the supplicant were successfully authenticated by the RADIUS server.
- Server-fail use-cache—If the RADIUS servers time out during reauthentication, previously authenticated supplicants are granted LAN access, but new supplicants are denied LAN access.
- Server-fail VLAN—A supplicant is configured to be moved to a specified VLAN if the RADIUS server is unavailable to reauthenticate the supplicant. (The VLAN must already exist on the switch.)

See Also

- *Configuring 802.1X Authentication (J-Web Procedure)*
- Configuring MAC RADIUS Authentication (CLI Procedure) on page 325
- Configuring RADIUS Server Fail Fallback (CLI Procedure) on page 287

Troubleshooting Authentication of End Devices on EX Series Switches

Problem **Description:** End devices configured using static MAC addresses lose connection to the switch after the clear dot1x interface command is run to clear all learned MAC addresses.

Before clearing MAC addresses:

```
user@switch# run show ethernet-switching table
Ethernet-switching table: 3 entries, 1 learned, 0 persistent entries
  VLAN              MAC address       Type         Age Interfaces
  vlan100           *                 Flood          - All-members
  default           *                 Flood          - All-members
  default           00:a0:d4:00:03:00 Learn          0 ge-3/0/16.0
```



```
user@switch> show dot1x authentication-bypassed-users
MAC address        Interface         VLAN
00:a0:d4:00:03:00  ge-3/0/16.0       configured/default
```

To clear MAC addresses:

```
user@switch> clear dot1x interface
```

After clearing MAC addresses:

```
user@switch> show ethernet-switching table
Ethernet-switching table: 2 entries, 0 learned, 0 persistent entries
  VLAN              MAC address       Type         Age Interfaces
  vlan100           *                 Flood          - All-members
  default           *                 Flood          - All-members

user@switch> show dot1x authentication-bypassed-users
```

Note that there are no end devices on the authentication bypass list.

Cause Static MAC addresses are treated the same as other learned MAC addresses on an interface. When the clear dot1x interface command is run, it clears all learned MAC addresses from the interface, including the static MAC bypass list (also known as the exclusion list).

Solution If you run the clear dot1x interfaces command for an interface that has static MAC addresses configured for authentication bypass, re-add the static MAC addresses to the static MAC bypass list.

See Also

- clear dot1x on page 1659
- Understanding Authentication on Switches on page 268

Release History Table

Release	Description
18.4R1	Starting in Junos OS Release 18.4R1, you can configure 802.1X authentication on trunk interfaces, which allows the network access device (NAS) to authenticate an access point (AP) or another connected Layer 2 device.
17.3R1	Starting in Junos OS Release 17.3, the port bounce feature can be used to force the end device to initiate DHCP re-negotiation by causing a link flap on the authenticated port.
14.1X53-A2	J-Web Application package Release 14.1X53-A2 does not support 802.1X authentication on EX4600 switches.

Related Documentation

- RADIUS Server Configuration for Authentication on page 282
- 802.1X and RADIUS Accounting on page 332
- MAC RADIUS Authentication on page 324
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 343

MAC RADIUS Authentication

You can control access to your network through a switch by using several different authentication. Junos OS switches support 802.1X, MAC RADIUS, and captive portal as an authentication methods to devices requiring to connect to a network.

You can configure MAC RADIUS authentication on the switch interfaces to which the hosts are connected to provide LAN access. For more information, read this topic.

- Configuring MAC RADIUS Authentication (CLI Procedure) on page 325
- Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 326

Configuring MAC RADIUS Authentication (CLI Procedure)

You can permit devices that are not 802.1X-enabled LAN access by configuring MAC RADIUS authentication on the switch interfaces to which the hosts are connected.

NOTE: You can also allow non-802.1X-enabled devices to access the LAN by configuring their MAC address for static MAC bypass of authentication.

You can configure MAC RADIUS authentication on an interface that also allows 802.1X authentication, or you can configure either authentication method alone.

If both MAC RADIUS and 802.1X authentication are enabled on the interface, the switch first sends the host three EAPoL requests to the host. If there is no response from the host, the switch sends the host's MAC address to the RADIUS server to check whether it is a permitted MAC address. If the MAC address is configured as permitted on the RADIUS server, the RADIUS server sends a message to the switch that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected.

If MAC RADIUS authentication is configured on the interface but 802.1X authentication is not (by using the **mac-radius restrict** option), the switch attempts to authenticate the MAC address with the RADIUS server without delaying by attempting 802.1X authentication first.

Before you configure MAC RADIUS authentication, be sure you have:

- Configured basic access between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.

To configure MAC RADIUS authentication by using the CLI:

- On the switch, configure the interfaces to which the nonresponsive hosts are attached for MAC RADIUS authentication, and add the **restrict** qualifier for interface **ge-0/0/20** to have it use only MAC RADIUS authentication:

```
[edit]
user@switch#  set protocols dot1x authenticator interface ge-0/0/19 mac-radius
user@switch#  set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
```

- On a RADIUS authentication server, create user profiles for each nonresponsive host using the MAC address (without colons) of the nonresponsive host as the username and password (here, the MAC addresses are **00:04:0f:fd:ac:fe** and **00:04:ae:cd:23:5f**):

```
[root@freeradius]#
edit /etc/raddb
vi users
00040ffdacfe Auth-type:=Local, User-Password = "00040ffdacfe"
0004aecd235f Auth-type:=Local, User-Password = "0004aecd235f"
```

See Also
- Understanding Authentication on Switches on page 268

Example: Configuring MAC RADIUS Authentication on an EX Series Switch

To permit hosts that are not 802.1X-enabled to access a LAN, you can configure MAC RADIUS authentication on the switch interfaces to which the non-802.1X-enabled hosts are connected. When MAC RADIUS authentication is configured, the switch will attempt to authenticate the host with the RADIUS server by using the host's MAC address.

This example describes how to configure MAC RADIUS authentication for two non-802.1X-enabled hosts:

Requirements

This example uses the following software and hardware components:

NOTE: **This example also applies to QFX5100 switches.**

- Junos OS Release 9.3 or later for EX Series switches.
- An EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- A RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you configure MAC RADIUS authentication, be sure you have:

- Configured basic access between the EX Series switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

NOTE: **For more about ELS, see: *Using the Enhanced Layer 2 Software CLI***

- Performed basic 802.1X configuration. See "Configuring 802.1X Interface Settings (CLI Procedure)" on page 292.

Overview and Topology

IEEE 802.1X port-based network access control (PNAC) authenticates and permits devices access to a LAN if the devices can communicate with the switch by using the 802.1X protocol (that is, the devices are 802.1X-enabled). To permit non-802.1X-enabled end devices to access the LAN, you can configure MAC RADIUS authentication on the interfaces to which the end devices are connected. When the MAC address of the end device appears on the interface, the switch consults the RADIUS server to check whether it is a permitted MAC address. If the MAC address of the end device is configured as permitted on the RADIUS server, the switch opens LAN access to the end device.

You can configure both MAC RADIUS authentication and 802.1X authentication methods on an interface configured for multiple supplicants. Additionally, if an interface is connected only to a non-802.1X-enabled host, you can enable MAC RADIUS and not enable 802.1X authentication by using the **mac-radius restrict** option, and thus avoid the delay that occurs while the switch determines that the device is does not respond to EAP messages.

Figure 10 on page 328 shows the two printers connected to the switch.

NOTE: This figure also applies to QFX5100 switches.

Figure 10: Topology for MAC RADIUS Authentication Configuration

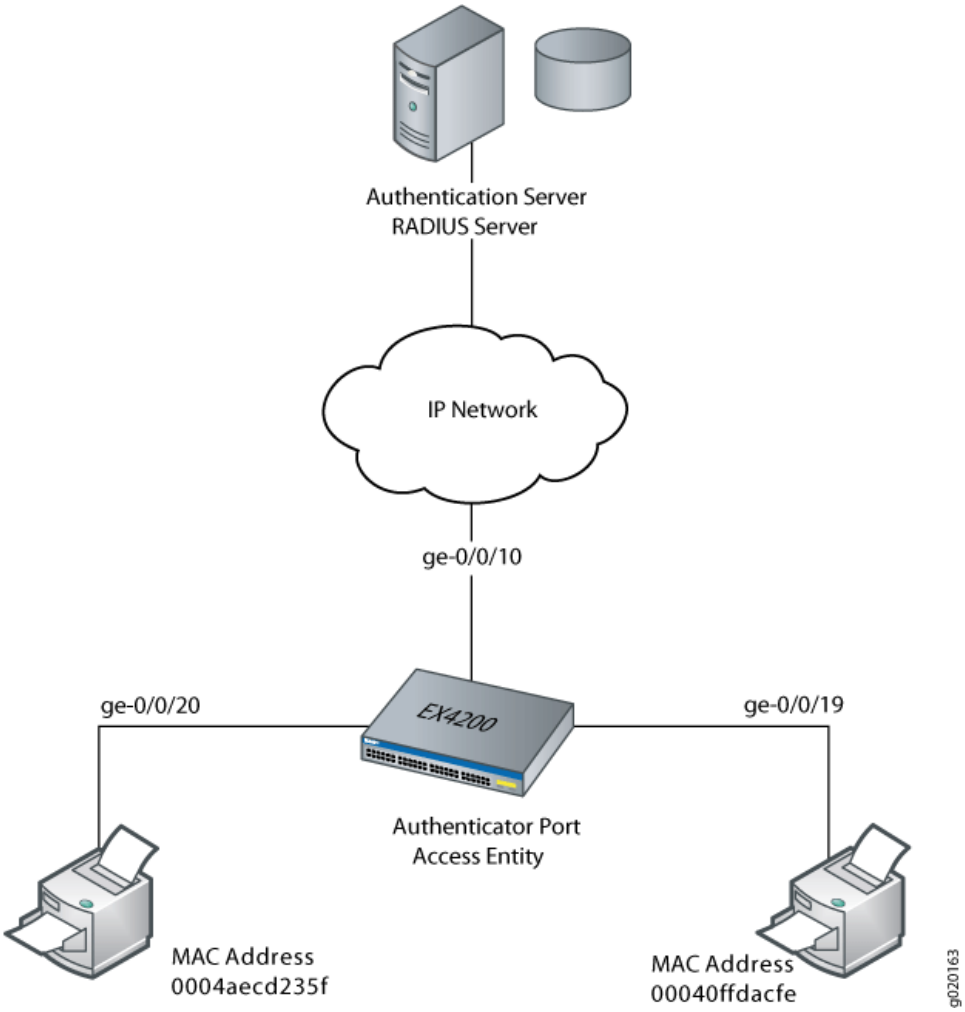


Table 24 on page 328 shows the components in the example for MAC RADIUS authentication.

Table 24: Components of the MAC RADIUS Authentication Configuration Topology

Property	Settings
Switch hardware	EX4200 ports (ge-0/0/0 through ge-0/0/23)
VLAN name	sales
Connections to printers (no PoE required)	ge-0/0/19, MAC address 00040ffdacfe ge-0/0/20, MAC address 0004aecd235f
RADIUS server	Connected to the switch on interface **ge-0/0/10**

The printer with the MAC address 00040ffdacfe is connected to access interface ge-0/0/19. A second printer with the MAC address 0004aecd235f is connected to access interface ge-0/0/20. In this example, both interfaces are configured for MAC RADIUS authentication on the switch, and the MAC addresses (without colons) of both printers are configured on the RADIUS server. Interface ge-0/0/20 is configured to eliminate the normal delay while the switch attempts 802.1X authentication; MAC RADIUS authentication is enabled and 802.1X authentication is disabled using the **mac radius restrict** option.

Configuration

CLI Quick Configuration

To quickly configure MAC RADIUS authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator interface ge-0/0/19 mac-radius
set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
```

NOTE: You must also configure the two MAC addresses as usernames and passwords on the RADIUS server, as is done in step 2 of the Step-by-Step Procedure.

Step-by-Step Procedure

Configure MAC RADIUS authentication on the switch and on the RADIUS server:

1. On the switch, configure the interfaces to which the printers are attached for MAC RADIUS authentication, and configure the restrict option on interface ge-0/0/20, so that only MAC RADIUS authentication is used:

   ```
   [edit]
   user@switch#  set protocols dot1x authenticator interface ge-0/0/19 mac-radius
   user@switch#  set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
   ```

2. On the RADIUS server, configure the MAC addresses 00040ffdacfe and 0004aecd235f as usernames and passwords:

   ```
   [root@freeradius]#
   edit /etc/raddb
   vi users
   00040ffdacfe Auth-type:=EAP, User-Password = "00040ffdacfe"
   0004aecd235f Auth-type:=EAP, User-Password = "0004aecd235f"
   ```

Results

Display the results of the configuration on the switch:

```
user@switch> show configuration
protocols {
  dot1x {
    authenticator {
      authentication-profile-name profile52;
```

```
        interface {
          ge-0/0/19.0 {
            mac-radius;
          }
          ge-0/0/20.0 {
            mac-radius {
              restrict;
            }
          }
        }
      }
    }
}
```

Verification

Verify that the supplicants are authenticated:

- Verifying That the Supplicants Are Authenticated on page 330

Verifying That the Supplicants Are Authenticated

Purpose After supplicants are configured for MAC RADIUS authentication on the switch and on the RADIUS server, verify that they are authenticated and display the method of authentication.

Action Display information about the 802.1X-configured interfaces ge-0/0/19 and ge-0/0/20:

```
user@switch> show dot1x interface ge-0/0/19.0 detail
ge-0/0/19.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

```
user@switch> show dot1x interface ge-0/0/20.0 detail
ge-0/0/20.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Enabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user102, 00:04:ae:cd:23:5f
      Operational state: Authenticated
      Authentcation method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning The sample output from the **show dot1x interface detail** command displays the MAC address of the connected end device in the **Supplicant** field. On interface ge-0/0/19, the MAC address is **00:04:0f:fd:ac:fe**, which is the MAC address of the first printer configured for MAC RADIUS authentication. The **Authentication method** field displays the

authentication method as **Radius**. On interface **ge-0/0/20**, the MAC address is **00:04:ae:cd:23:5f**, which is the MAC address of the second printer configured for MAC RADIUS authentication. The **Authentication method** field displays the authentication method as **Radius**.

Related Documentation

- Interfaces Enabled for 802.1X or MAC RADIUS Authentication on page 349
- Static MAC Bypass of 802.1X and MAC RADIUS Authentication on page 367

802.1X and RADIUS Accounting

EX Series Switches support RADIUS accounting. You can configure RADIUS accounting on an EX Series switch to collect statistical data about users logging in to or out of a LAN and send that data to a RADIUS accounting server. The data gathered is used for network monitoring purpose.

- Understanding 802.1X and RADIUS Accounting on Switches on page 332
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335

Understanding 802.1X and RADIUS Accounting on Switches

Juniper Networks EX Series Ethernet Switches support IETF RFC 2866, *RADIUS Accounting*. By configuring RADIUS accounting on an EX Series switch, you can collect statistical data about users logging in to or out of a LAN and send that data to a RADIUS accounting server. The statistical data gathered can be used to perform general network monitoring, to analyze and track usage patterns, or to bill a user based on the amount of time or type of services accessed.

- RADIUS Accounting Process on page 332
- Supported RADIUS Attributes on page 333

RADIUS Accounting Process

RADIUS accounting is based on a client/server model in which the switch, operating as the network access server (NAS), is the client. The client forwards user accounting statistics to a designated RADIUS accounting server. The RADIUS accounting server must send a response to the client when it has successfully received and recorded the accounting statistics.

The RADIUS accounting process between a switch and a RADIUS server is based on the exchange of two types of RADIUS messages—Accounting-Request and Accounting-Response. Accounting-Request messages are sent from the switch to the server and convey information used to account for a service provided to a user. Accounting-Response messages are sent from the server to acknowledge receipt of the Accounting-Request packets. The exchange of messages between the switch and the server proceeds as follows:

1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. For example, on FreeRADIUS, the default port is 1813.

2. When a supplicant is authenticated through 802.1X authentication and then connected to the LAN, the switch forwards an Accounting-Request message with a record of the event to the accounting server. The Accounting-Request message sent by the switch includes the RADIUS attribute Acct-Status-Type with a value of Start, which indicates the beginning of user service for this supplicant. The accounting server records this event in the accounting log file as a start record.

3. The accounting server sends an Accounting-Response message back to the switch confirming that it received the accounting request. If the switch does not receive a response from the server, it continues to send accounting requests until an accounting response is returned from the accounting server.

4. The switch might send an interim message to the accounting server to periodically update the server with information pertaining to a specific session. Interim messages are sent as Accounting-Request messages with the Acct-Status-Type attribute value of Interim-Update. The accounting server sends an Accounting-Response messae back to the switch to confirm receipt of an interim update.

5. When the supplicant's session ends, the switch forwards an Accounting-Request message with the Acct-Status-Type attribute value set to Stop, indicating the end of user service. The accounting server records this event in the accounting log file as a stop record that contains session information and the length of the session.

The statistics collected through this process can be displayed from the RADIUS server. To view those statistics, the user needs to access the accounting log file configured to receive them. On FreeRADIUS, the filename is the server's address—for example, 122.69.1.250.

Supported RADIUS Attributes

RADIUS accounting statistics are conveyed through the attributes included in each Accounting-Request message sent from the NAS to the server. Table 25 on page 333 list the RADIUS attributes supported for Accounting-Request messages.

Table 25: RADIUS Accounting Request Attributes

Type	Attribute	Description
1	User-Name	The name of the authenticated user.
5	NAS-Port	The physical port number of the NAS that authenticates the user. Either NAS-Port or NAS-Port-ID must be contained in the packet.

Table 25: RADIUS Accounting Request Attributes (continued)

Type	Attribute	Description
8	Framed-IP-Address	The IP address of the authenticated user. NOTE: The Framed-IP-Address attribute is sent only if a valid DHCP binding exists for the host in the DHCP snooping table.
11	Filter-ID	The name of the filter list for the user.
12	Framed-MTU	The maximum transmission unit that can be configured for the user.
26	Client-System-Name	Vendor-specific attribute (VSA) used to indicate the client's hostname. Supported for LLDP-capable devices only.
27	Session-Timeout	Sets the maximum time (in seconds) that a session stays active before it terminates or a prompt is issued notifying its termination.
28	Idle-Timeout	The maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.
30	Called-Station-ID	Enables the NAS to identify the phone number that the user called, using Dialed Number Identification (DNIS) or a similar technology.
31	Calling-Station-ID	Enables the NAS to identify the phone number that the call came from, using Automatic Number Identification (ANI) or a similar technology.
32	NAS-Identifier	Contains a string identifying the NAS originating the Accounting-Request message.
40	Acct-Status-Type	Indicates whether this Accounting-Request message marks the beginning (Start) or the end (Stop) of the user session. Can also be used for an interim update (Interim-Update).
44	Acct-Session-ID	A unique ID for a specific accounting session that can be used to match start and stop records for a session in the log file.
45	Acct-Authentic	Indicates whether the user was authenticated locally, by the RADIUS server, or by another remote authentication protocol.
55	Event-Timestamp	Records the time an event occurred.
87	NAS-Port-ID	Text string that identifies the port that authenticates the user. Either NAS-Port or NAS-Port-ID must be present in the packet.

See Also

- 802.1X for Switches Overview on page 289
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302

- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335

Configuring 802.1X RADIUS Accounting (CLI Procedure)

RADIUS accounting enables statistical data about users logging in to or out of a LAN to be collected and sent to a RADIUS accounting server. The statistical data gathered can be used to perform general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

RADIUS accounting is based on a client/server model in which the switch, operating as the network access server (NAS), is the client. The client is responsible for forwarding user accounting statistics to a designated RADIUS accounting server. To configure RADIUS accounting, specify one or more RADIUS accounting servers to receive the statistical data from the switch, and select the type of accounting data to be collected.

The RADIUS accounting server you specify can be the same server used for RADIUS authentication, or it can be a separate RADIUS server. You can specify a list of RADIUS accounting servers. If the primary server (the first one configured) is unavailable, then each RADIUS server in the list is tried in the order in which the servers are configured in Junos OS.

To configure RADIUS accounting by using the CLI:

1. Configure an access profile and specify the accounting servers to which the switch forwards accounting statistics:

   ```
   [edit access]
   user@switch# set profile profile-name radius accounting-server [server-addresses]
   ```

2. Define the address of RADIUS accounting servers and configure the secret password (the secret password on the switch must match the secret password on the server):

   ```
   [edit access]
   user@switch# set radius-server server-address secret password
   ```

3. Enable accounting for the access profile:

   ```
   [edit access]
   user@switch# set profile profile-name accounting
   ```

4. Configure the accounting order, making RADIUS the first method for sending accounting messages and updates:

   ```
   [edit access]
   user@switch# set profile profile-name accounting order radius
   ```

5. Configure the statistics to be collected on the switch and forwarded to the accounting server:

   ```
   [edit access]
   user@switch# set profile profile-name accounting accounting-stop-on-access-deny
   user@switch# set profile profile-name accounting accounting-stop-on-failure
   ```

6. (Optional) Configure the switch to send periodic updates for a user session at a specified interval to the accounting server:

```
[edit access]
user@switch# set profile profile-name accounting update-interval minutes
```

7. Display accounting statistics collected on the switch using the **show network-access aaa statistics accounting** command, for example:

```
user@switch> show network-access aaa statistics accounting
Accounting module statistics
  Requests received: 1
  Accounting Response failures: 0
  Accounting Response Success: 1
  Requests timedout: 0
```

8. Open an accounting log on the RADIUS accounting server by using the server's address, and view accounting statistics, for example:

```
[root@freeradius]# cd /usr/local/var/log/radius/radacct/192.168.0.1
[root@freeradius 192.168.0.1]# ls

detail-20071214

[root@freeradius 192.168.0.1]# vi details-20071214

        User-Name = "000347e1bab9"
        NAS-Port = 67
        Acct-Status-Type = Stop
        Acct-Session-Id = "802.1x811912"
        Acct-Input-Octets = 17454
        Acct-Output-Octets = 4245
        Acct-Session-Time = 1221041249
        Acct-Input-Packets = 72
        Acct-Output-Packets = 53
        Acct-Terminate-Cause = Lost-Carrier
        Acct-Input-Gigawords = 0
        Acct-Output-Gigawords = 0
        Called-Station-Id = "00-19-e2-50-52-60"
        Calling-Station-Id = "00-03-47-e1-ba-b9"
        Event-Timestamp = "Sep 10 2008 16:52:39 PDT"
        NAS-Identifier = "esp48t-1b-01"
        NAS-Port-Type = Virtual

        User-Name = "000347e1bab9"
        NAS-Port = 67
        Acct-Status-Type = Start
        Acct-Session-Id = "802.1x811219"
        Called-Station-Id = "00-19-e2-50-52-60"
        Calling-Station-Id = "00-03-47-e1-ba-b9"
        Event-Timestamp = "Sep 10 2008 18:58:52 PDT"
        NAS-Identifier = "esp48t-1b-01"
        NAS-Port-Type = Virtual
```

See Also
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302

Related Documentation
- RADIUS Server Configuration for Authentication on page 282

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch

802.1x port-based network access control (PNAC) authentication on EX Series switches provides three types of authentication to meet the access needs of your enterprise LAN:

- Authenticate the first end device (supplicant) on an authenticator port, and allow all other end devices also connecting to have access to the LAN.
- Authenticate only one end device on an authenticator port at one time.
- Authenticate multiple end devices on an authenticator port. Multiple supplicant mode is used in VoIP configurations.

This example configures an EX Series switch to use IEEE 802.1X to authenticate end devices that use three different administrative modes.

Requirements

This example uses the following software and hardware components:

NOTE: **This example also applies to QFX5100 switches.**

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from end devices until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for end devices (supplicants) that have permission to connect to the network.

Before you configure the ports for 802.1X authentication, be sure you have:

- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a

switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

NOTE: For more about ELS, see *Using the Enhanced Layer 2 Software CLI*.

- Configured users on the authentication server.

Overview and Topology

As shown in Figure 11 on page 339, the topology contains an EX4200 access switch connected to the authentication server on port ge-0/0/10. Interfaces ge-0/0/8, ge-0/0/9, and ge-0/0/11 will be configured for three different administrative modes.

NOTE: This figure also applies to QFX5100 switches.

Figure 11: Topology for Configuring Supplicant Modes

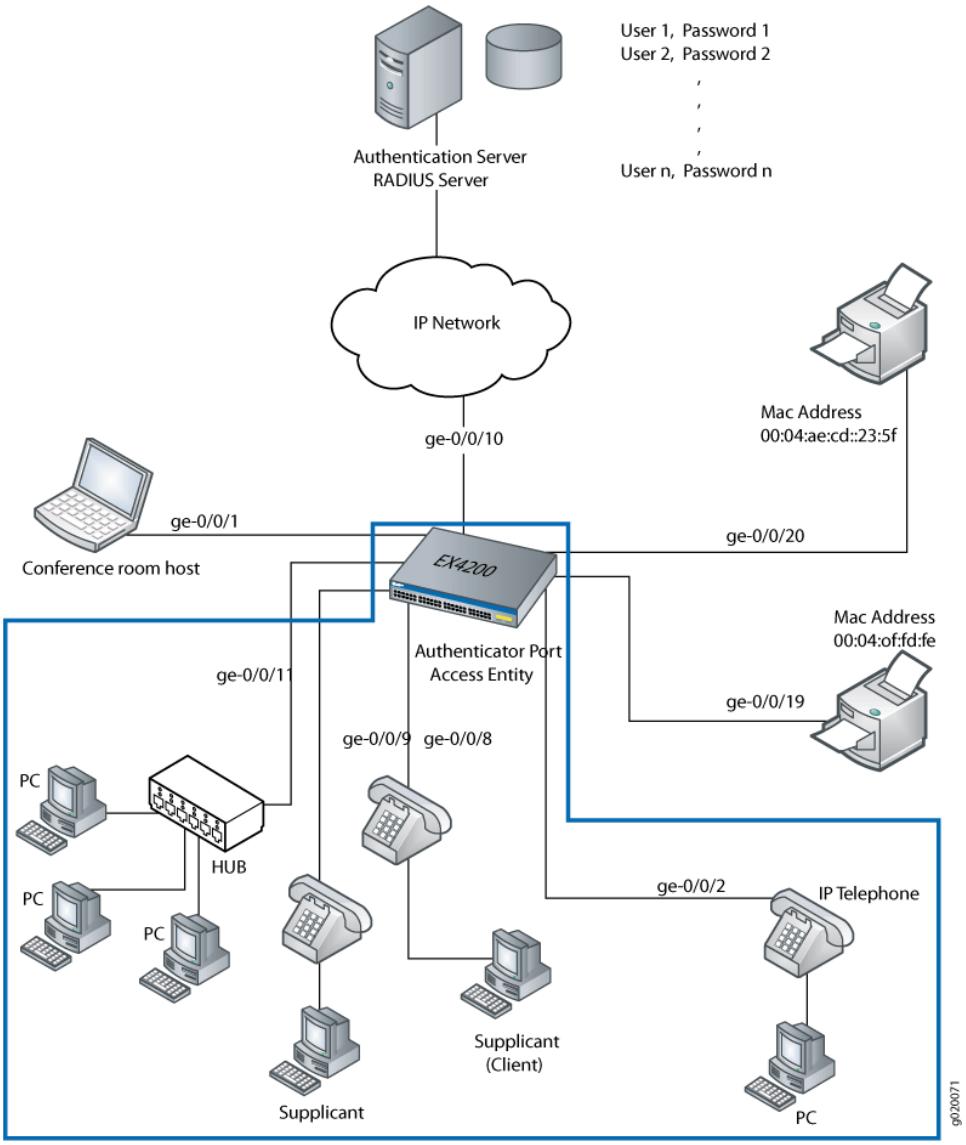


Table 26: Components of the Supplicant Mode Configuration Topology

Property	Settings
Switch hardware	EX4200 switch, 24 Gigabit Ethernet ports: 8 PoE ports (ge-0/0/0 through ge-0/0/7) and 16 non-PoE ports (ge-0/0/8 through ge-0/0/23)
Connections to Avaya phones—with integrated hub, to connect phone and desktop PC to a single port; (requires PoE)	ge-0/0/8, ge-0/0/9, and ge-0/0/11

To configure the administrative modes to support supplicants in different areas of the Enterprise network:

- Configure access port ge-0/0/8 for single supplicant mode authentication.
- Configure access port ge-0/0/9 for single secure supplicant mode authentication.
- Configure access port ge-0/0/11 for multiple supplicant mode authentication.

Single supplicant mode authenticates only the first end device that connects to an authenticator port. All other end devices connecting to the authenticator port after the first has connected successfully, whether they are 802.1X-enabled or not, are permitted access to the port without further authentication. If the first authenticated end device logs out, all other end devices are locked out until an end device authenticates.

Single-secure supplicant mode authenticates only one end device to connect to an authenticator port. No other end device can connect to the authenticator port until the first logs out.

Multiple supplicant mode authenticates multiple end devices individually on one authenticator port. If you configure a maximum number of devices that can be connected to a port through port security, the lesser of the configured values is used to determine the maximum number of end devices allowed per port.

Configuration of 802.1X to Support Multiple Supplicant Modes

CLI Quick Configuration

To quickly configure the ports with different 802.1X authentication modes, copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator interface ge-0/0/8 supplicant single
set protocols dot1x authenticator interface ge-0/0/9 supplicant single-secure
set protocols dot1x authenticator interface ge-0/0/11 supplicant multiple
```

Step-by-Step Procedure

Configure the administrative mode on the interfaces:

1. Configure the supplicant mode as single on interface ge-0/0/8:

   ```
   [edit protocols]
   user@switch# set dot1x authenticator interface ge-0/0/8 supplicant single
   ```

2. Configure the supplicant mode as single secure on interface ge-0/0/9:

   ```
   [edit protocols]
   user@switch# set dot1x authenticator interface ge-0/0/9 supplicant single-secure
   ```

3. Configure multiple supplicant mode on interface ge-0/0/11:

   ```
   [edit protocols]
   user@switch# set dot1x authenticator interface ge-0/0/11 supplicant multiple
   ```

Results

Check the results of the configuration:

```
[edit]
user@access-switch> show configuration
protocols {
   dot1x {
      authenticator {
         interface {
            ge-0/0/8.0 {
               supplicant single;
            )
            ge-0/0/9.0 {
               supplicant single-secure;
            )
            ge-0/0/11.0 {
               supplicant multiple;
            )
         }
      }
   }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying the 802.1X Configuration on page 341

Verifying the 802.1X Configuration

Purpose Verify the 802.1X configuration on interfaces ge-0/0/8, ge-0/0/9, and ge-0/0/5.

Action Verify the 802.1X configuration by issuing the operational mode command **show dot1x interface**:

```
user@switch> show dot1x interface ge-0/0/8.0 detail
ge-0/0/8.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
```

```
user@switch> show dot1x interface ge-0/0/9.0 detail
ge-0/0/9.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single-Secure
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 0
```

```
user@switch> show dot1x interface ge-0/0/11.0 detail
ge-0/0/11.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 0
```


Meaning The **Supplicant mode** output field displays the configured administrative mode for each interface. Interface **ge-0/0/8.0** displays **Single** supplicant mode. Interface **ge-0/0/9.0** displays **Single-Secure** supplicant mode. Interface **ge-0/0/11.0** displays **Multiple** supplicant mode.

Related Documentation

- Controlling Authentication Session Timeouts (CLI Procedure) on page 277
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 343
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 297
- Understanding Authentication on Switches on page 268

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch

802.1X on EX Series switches provides LAN access to users who do not have credentials in the RADIUS database. These users, referred to as *guests*, are authenticated and typically provided with access to the Internet.

This example describes how to create a guest VLAN and configure 802.1X authentication for it.

Requirements

This example uses the following software and hardware components:

NOTE: **This example also applies to QFX5100 switches.**

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as a port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.

- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you configure guest VLAN authentication, be sure you have:

- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

NOTE: For more about ELS, see: *Using the Enhanced Layer 2 Software CLI*

Overview and Topology

As part of IEEE 802.1X port-based network access control (PNAC), you can provide limited network access to supplicants who do not belong to a VLAN authentication group by configuring authentication for a guest VLAN. Typically, guest VLAN access is used to provide Internet access to visitors to a corporate site. However, you can also use the guest VLAN feature to provide access to a VLAN with limited resources to supplicants that fail 802.1X authentication on a corporate LAN.

NOTE: This figure also applies to QFX5100 switches.

Figure 12 on page 345 shows the conference room connected to the switch at interface ge-0/0/1.

Figure 12: Topology for Guest VLAN Example

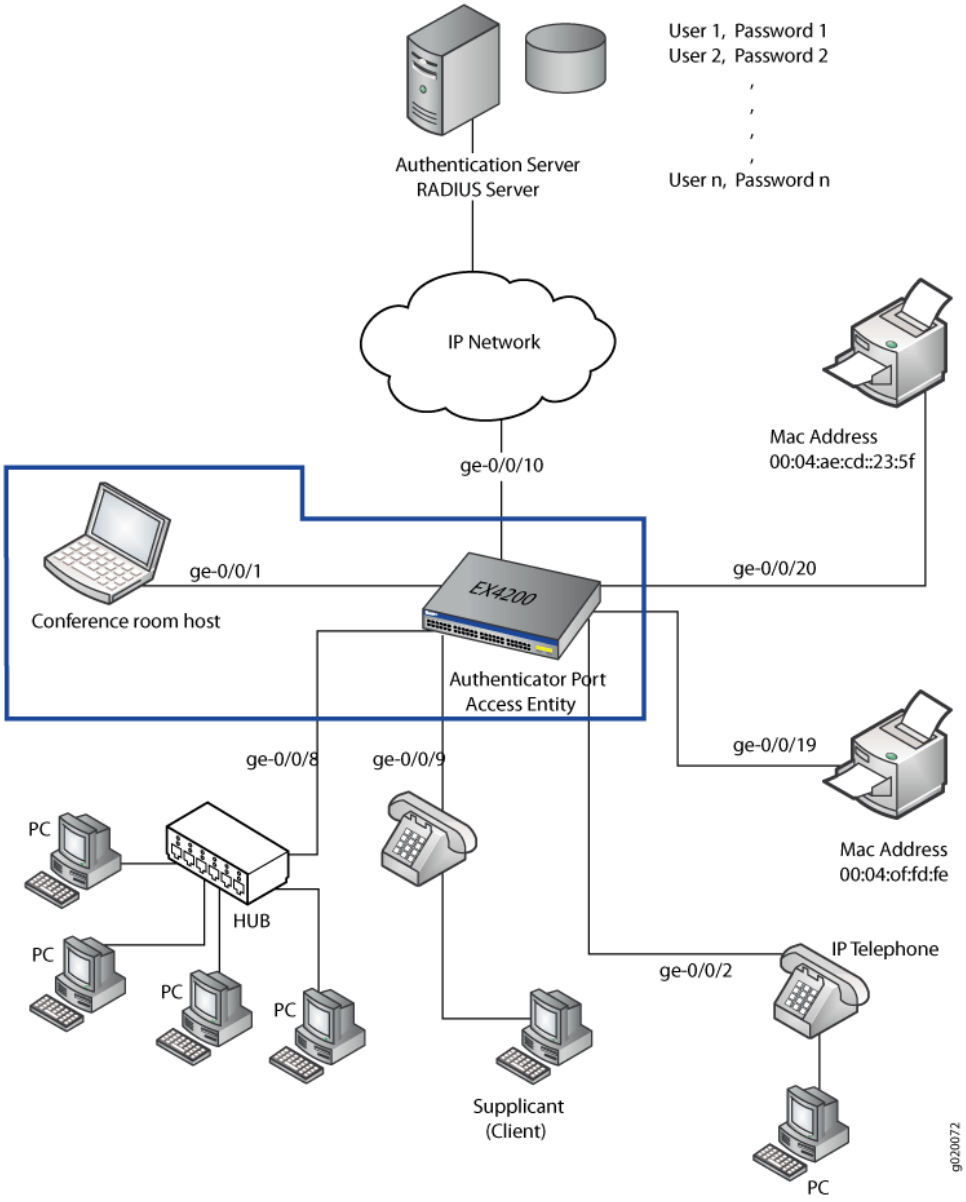


Table 27: Components of the Guest VLAN Topology

Property	Settings
Switch hardware	EX4200 switch, 24 Gigabit Ethernet interfaces: 8 PoE interfaces (**ge-0/0/0** through **ge-0/0/7**) and 16 non-PoE interfaces (**ge-0/0/8** through **ge-0/0/23**)
VLAN names and tag IDs	**sales**, tag **100** **support**, tag **200** **guest-vlan**, tag **300**
One RADIUS server	Backend database connected to the switch through interface **ge-0/0/10**

In this example, access interface **ge-0/0/1** provides LAN connectivity in the conference room. Configure this access interface to provide LAN connectivity to visitors in the conference room who are not authenticated by the corporate VLAN.

Configuration of a Guest VLAN That Includes 802.1X Authentication

CLI Quick Configuration

To quickly configure a guest VLAN, with 802.1X authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans guest-vlan vlan-id 300
set protocols dot1x authenticator interface all guest-vlan guest-vlan
```

Step-by-Step Procedure

To configure a guest VLAN that includes 802.1X authentication on an EX Series switch:

1. Configure the VLAN ID for the guest VLAN:

   ```
   [edit]
   user@switch# set vlans guest-vlan vlan-id 300
   ```

2. Configure the guest VLAN under **dot1x** protocol:

   ```
   [edit]
   user@switch# set protocols dot1x authenticator interface all guest-vlan guest-vlan
   ```

Results

Check the results of the configuration:

```
user@switch> show configuration
protocols {
  dot1x {
    authenticator {
      interface {
        all {
          guest-vlan {
            guest-vlan;
          }
        }
      }
    }
  }
}
vlans {
  guest-vlan {
    vlan-id 300;
  }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That the Guest VLAN Is Configured on page 347

Verifying That the Guest VLAN Is Configured

Purpose Verify that the guest VLAN is created and that an interface has failed authentication and been moved to the guest VLAN.

NOTE: On switches running Junos OS for EX Series with support for ELS, the output for the show vlans command will contain additional information. If your switch runs software that supports ELS, see *show vlans*. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

Action Issue the operational mode commands:

```
user@switch> show vlans

Name            Tag     Interfaces
default
                        ge-0/0/3.0*
dynamic         40
                        None
guest           30
                        None
guest-vlan      300
                        ge-0/0/1.0*
vlan_dyn
                        None
```

```
user@switch> show dot1x interface ge-0/0/1.0 detail
ge-0/0/1.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: guest-vlan
  Number of connected supplicants: 1
    Supplicant: user1, 00:00:00:00:13:23
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning The output of the **show vlans** command shows **guest-vlan** as the the name of the VLAN and the VLAN ID as **300**.

The output of the **show dot1x interface ge-0/0/1.0 detail** command displays the **Guest VLAN membership** field, indicating that a supplicant at this interface failed 802.1X authentication and was passed through to the **guest-vlan**.

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292

Interfaces Enabled for 802.1X or MAC RADIUS Authentication

EX Series switches support port firewall filters. Port firewall filters are configured on a single EX Series switch, but in order for them to operate throughout an enterprise, they must be configured on multiple switches. To reduce the need to configure the same port firewall filter on multiple switches, you can instead apply the filter centrally on the RADIUS server by using RADIUS server attributes. Terms are applied after a device is successfully authenticated through 802.1X. For more information, read this topic.

- Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch on page 349
- Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on page 356
- Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on EX Series Switches with ELS Support on page 362

Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch

You can use RADIUS server attributes and a port firewall filter to centrally apply terms to multiple supplicants (end devices) connected to an EX Series switch in your enterprise. Terms are applied after a device is successfully authenticated through 802.1X. If the firewall filter configuration is modified after end devices are authenticated using the 802.1X authentication, then the established 802.1X authentication session must be terminated and re-established for the firewall filter changes to take effect.

EX Series switches support port firewall filters. Port firewall filters are configured on a single EX Series switch, but in order for them to operate throughout an enterprise, they must be configured on multiple switches. To reduce the need to configure the same port firewall filter on multiple switches, you can instead apply the filter centrally on the RADIUS server by using RADIUS server attributes.

The following example uses FreeRADIUS to apply a port firewall filter on a RADIUS server. For information about configuring your server, consult the documentation that was included with your RADIUS server.

This example describes how to configure a port firewall filter with terms, create counters to count packets for the supplicants, apply the filter to user profiles on the RADIUS server, and display the counters to verify the configuration:

- Requirements on page 350
- Overview and Topology on page 350
- Configuring the Port Firewall Filter and Counters on page 353

Requirements

This example uses the following software and hardware components:

NOTE: **This example also applies to QFX5100 switches.**

- Junos OS Release 9.3 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.
- Configured 802.1X authentication on the switch, with the supplicant mode for interface ge-0/0/2 set to **multiple**. See "Configuring 802.1X Interface Settings (CLI Procedure)" on page 292 and "Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch" on page 337.
- Configured users on the RADIUS authentication server (in this example, the user profiles for Supplicant 1 and Supplicant 2 in the topology are modified on the RADIUS server).

Overview and Topology

When the 802.1X configuration on an interface is set to **multiple** supplicant mode, you can apply a single port firewall filter configured through the Junos OS CLI on the EX Series switch to any number of end devices (supplicants) by adding the filter centrally to the RADIUS server. Only a single filter can be applied to an interface; however, the filter can contain multiple terms for separate end devices.

For more information about firewall filters, see *Firewall Filters for EX Series Switches Overview* or *Overview of Firewall Filters*.

RADIUS server attributes are applied to the port where the end device is connected after the device is successfully authenticated using 802.1X. To authenticate an end device, the switch forwards the end device's credentials to the RADIUS server. The RADIUS server matches the credentials against preconfigured information about the supplicant located in the supplicant's user profile on the RADIUS server. If a match is found, the RADIUS server instructs the switch to open an interface to the end device. Traffic then flows from and to the end device on the LAN. Further instructions configured in the port firewall filter

and added to the end device's user profile using a RADIUS server attribute further define the access that the end device is granted. Filtering terms configured in the port firewall filter are applied to the port where the end device is connected after 802.1X authentication is complete.

NOTE: If you modify the port firewall filter after an end device is successfully authenticated using 802.1X, you must terminate and re-establish the 802.1X authentication session for the firewall filter configuration changes to be effective.

Figure 13 on page 352 shows the topology used for this example. The RADIUS server is connected to an EX4200 switch on access port ge-0/0/10. Two end devices (supplicants) are accessing the LAN on interface ge-0/0/2. Supplicant 1 has the MAC address 00:50:8b:6f:60:3a. Supplicant 2 has the MAC address 00:50:8b:6f:60:3b.

NOTE: This figure also applies to QFX5100 switches.

Figure 13: Topology for Firewall Filter and RADIUS Server Attributes Configuration

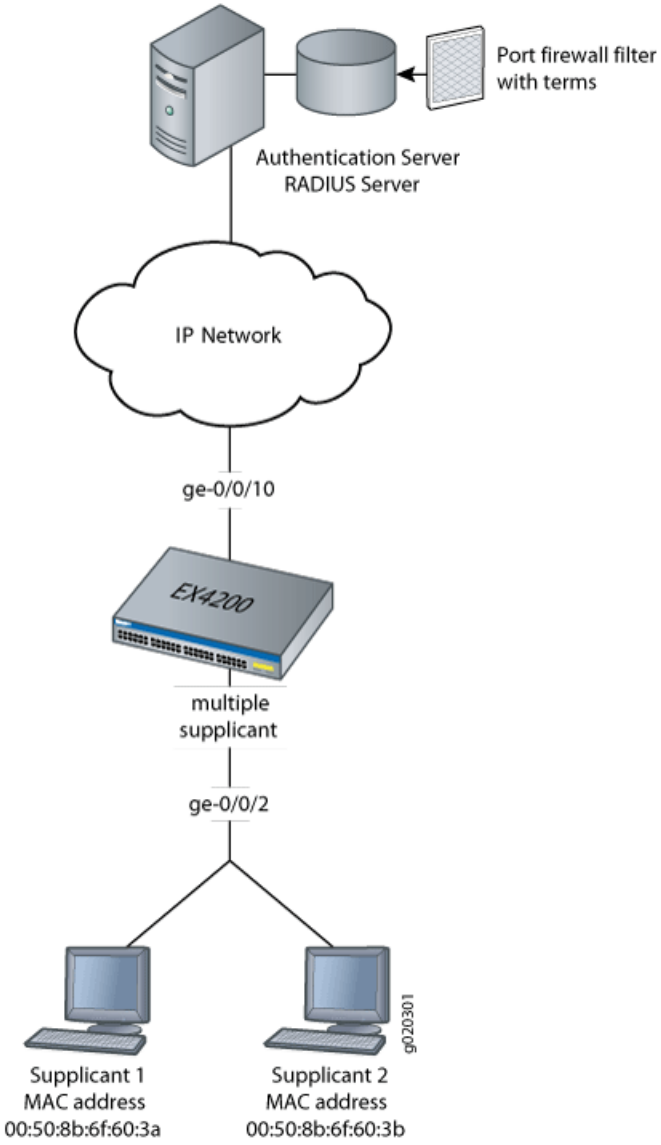


Table 28 on page 352 describes the components in this topology.

Table 28: Components of the Firewall Filter and RADIUS Server Attributes Topology

Property	Settings
Switch hardware	EX4200 access switch, 24 Gigabit Ethernet ports: 16 non-PoE ports and 8 PoE ports.
One RADIUS server	Backend database with the address **10.0.0.100** connected to the switch at port **ge-0/0/10**.
802.1X supplicants connected to the switch on interface **ge-0/0/2**	• **Supplicant 1** has MAC address **00:50:8b:6f:60:3a**. • **Supplicant 2** has MAC address **00:50:8b:6f:60:3b**.

Table 28: Components of the Firewall Filter and RADIUS Server Attributes Topology (continued)

Property	Settings
Port firewall filter to be applied on the RADIUS server	**filter1**
Counters	**counter1** counts packets from Supplicant 1, and **counter2** counts packets from Supplicant 2.
Policer	**policer p1**
User profiles on the RADIUS server	• Supplicant 1 has the user profile **supplicant1**. • Supplicant 2 has the user profile **supplicant2**.

In this example, you configure a port firewall filter named **filter1**. The filter contains terms that will be applied to the end devices based on the MAC addresses of the end devices. When you configure the filter, you also configure the counters **counter1** and **counter2**. Packets from each end device are counted, which helps you verify that the configuration is working. Policer **p1** limits the traffic rate based on the values for **exceeding** and **discard** parameters. Then, you check to see that the RADIUS server attribute is available on the RADIUS server and apply the filter to the user profiles of each end device on the RADIUS server. Finally, you verify the configuration by displaying output for the two counters.

Configuring the Port Firewall Filter and Counters

CLI Quick Configuration

To quickly configure a port firewall filter with terms for Supplicant 1 and Supplicant 2 and create parallel counters for each supplicant, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter filter1 term supplicant1 from source-mac-address
00:50:8b:6f:60:3a
set firewall family ethernet-switching filter filter1 term supplicant2 from source-mac-address
00:50:8b:6f:60:3b
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall policer p1 then discard
set firewall family ethernet-switching filter filter1 term supplicant1 then count counter1
set firewall family ethernet-switching filter filter1 term supplicant1 then policer p1
set firewall family ethernet-switching filter filter1 term supplicant2 then count counter2
```

Step-by-Step Procedure

To configure a port firewall filter and counters on the switch:

1. Configure a port firewall filter (here, **filter1**) with terms for each end device based on the MAC address of each end device:

   ```
   [edit firewall family ethernet-switching]
   user@switch# set filter filter1 term supplicant1 from source-mac-address 00:50:8b:6f:60:3a
   user@switch# set filter filter1 term supplicant2 from source-mac-address 00:50:8b:6f:60:3b
   ```

2. Set policer definition:

```
[edit]
user@switch# set firewall policer p1 if-exceeding bandwidth-limit 1m
user@switch# set firewall policer p1 if-exceeding burst-size-limit 1k
user@switch# set firewall policer p1 then discard
```

3. Create two counters that will count packets for each end device and a policer that limits the traffic rate:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term supplicant1 then count counter1
user@switch# set filter filter1 term supplicant1 then policer p1
user@switch# set filter filter1 term supplicant2 then count counter2
```

Results Display the results of the configuration:

```
user@switch> show configuration
  firewall {
    family ethernet-switching {
      filter filter1 {
        term supplicant1 {
          from {
            source-mac-address {
              00:50:8b:6f:60:3a;
            }
          }
          then count counter1;
          then policer p1;
        }
        term supplicant2 {
          from {
            source-mac-address {
              00:50:8b:6f:60:3b;
            }
          }
          then count counter2;
        }
      }
    }
  }
  policer p1 {
    if-exceeding {
      bandwidth-limit 1m;
        burst-size-limit 1k;
      }
      then discard;
    }
```

Applying the Port Firewall Filter to the Supplicant User Profiles on the RADIUS Server

Step-by-Step Procedure

To verify that the RADIUS server attribute **Filter-ID** is on the RADIUS server and to apply the filter to the user profiles:

1. Display the dictionary **dictionary.rfc2865** on the RADIUS server, and verify that the attribute **Filter-ID** is in the dictionary:

   ```
   [root@freeradius]# cd usr/share/freeradius/dictionary.rfc2865
   ```

2. Close the dictionary file.

3. Display the local user profiles of the end devices to which you want to apply the filter (here, the user profiles are called **supplicant1** and **supplicant2**):

   ```
   [root@freeradius]# cat /usr/local/etc/raddb/users
   ```

   The output shows:

   ```
   supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
           Tunnel-Type = VLAN,
           Tunnel-Medium-Type = IEEE-802,
           Tunnel-Private-Group-Id = "1005"

   supplicant2 Auth-Type := EAP, User-Password == "supplicant2"
           Tunnel-Type = VLAN,
           Tunnel-Medium-Type = IEEE-802,
           Tunnel-Private-Group-Id = "1005"
   ```

4. Apply the filter to both user profiles by adding the line **Filter-Id = “filter1”** to each profile, and then close the file:

   ```
   [root@freeradius]# cat /usr/local/etc/raddb/users
   ```

   After you paste the line into the files, the files look like this:

   ```
   supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
           Tunnel-Type = VLAN,
           Tunnel-Medium-Type = IEEE-802,
           Tunnel-Private-Group-Id = "1005",
           Filter-Id = "filter1"

   supplicant2 Auth-Type := EAP, User-Password == "supplicant2"
           Tunnel-Type = VLAN,
           Tunnel-Medium-Type = IEEE-802,
           Tunnel-Private-Group-Id = "1005",
           Filter-Id = "filter1"
   ```

Verification

Verifying That the Filter Has Been Applied to the Supplicants

Purpose After the end devices are authenticated on interface ge-0/0/2, verify that the filter has been configured on the switch and includes the results for both supplicants:

Action

```
user@switch> show dot1x firewall
Filter: dot1x-filter-ge-0/0/2
Counters
counter1_dot1x_ge-0/0/2_user1 100
counter2_dot1x_ge-0/0/2_user2 400
```

Meaning The output of the **show dot1x firewall** command displays **counter1** and **counter2**. Packets from User_1 are counted using **counter1**, and packets from User 2 are counted using **counter2**. The output displays packets incrementing for both counters. The filter has been applied to both end devices.

See Also

- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- *Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches*
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335
- Understanding Authentication on Switches on page 268
- Understanding Dynamic Filters Based on RADIUS Attributes on page 306

Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication

On EX Series switches, firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server. The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.

This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

- Requirements on page 357
- Overview and Topology on page 357

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.5 or later for EX Series switches
- One EX Series switch
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

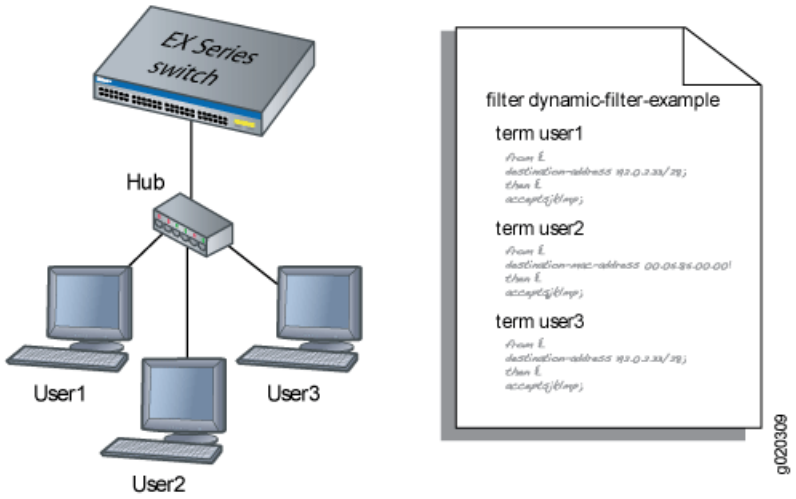
- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.
- Configured 802.1X authentication on the switch, with the authentication mode for interface **ge-0/0/2** set to **multiple**. See "Configuring 802.1X Interface Settings (CLI Procedure)" on page 292 and "Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch" on page 337.
- Configured users on the RADIUS authentication server.

Overview and Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines interface firewall filter with the user policies sent to the switch from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in Figure 14 on page 358, when User1 is authenticated by the EX Series switch, the system creates the firewall filter **dynamic-filter-example**. When User2 is authenticated, another term is added to the firewall filter, and so on.

Figure 14: Conceptual Model: Dynamic Filter Updated for Each New User

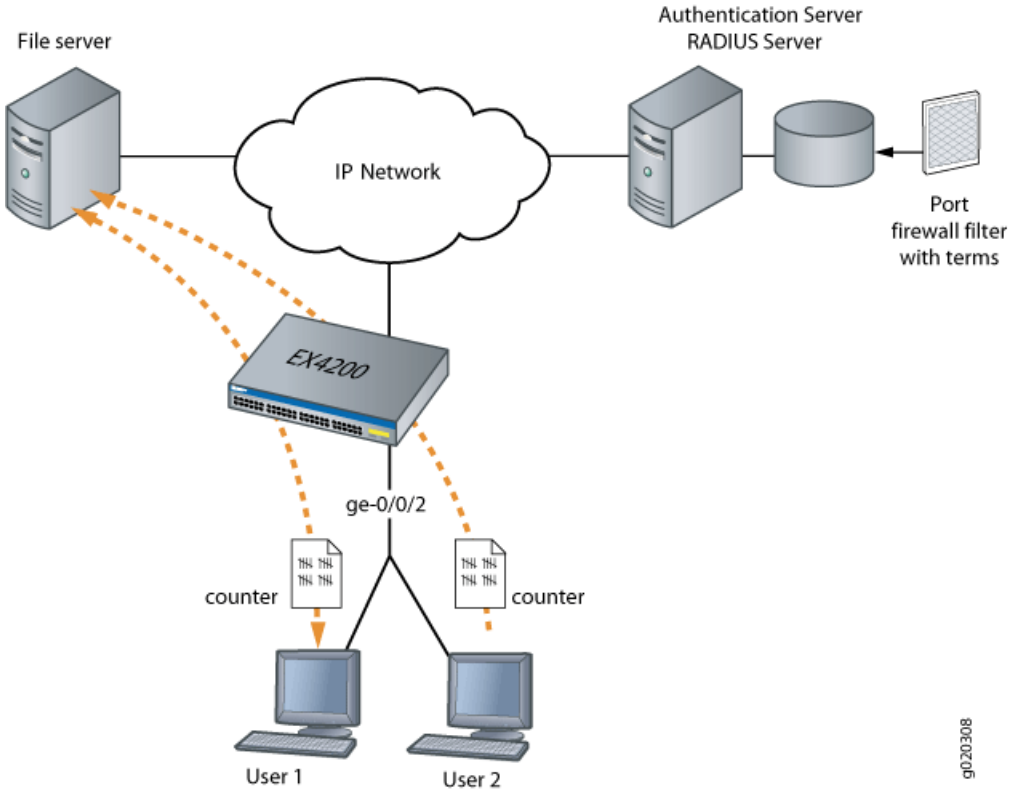


This is a conceptual model of the internal process—you cannot access or view the dynamic filter.

NOTE: If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface **ge-0/0/2** to the file server, which is located on subnet **192.0.2.16/28**, and set policer definitions to rate limit the traffic. Figure 15 on page 359 shows the network topology for this example.

Figure 15: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server



Configuration

To configure firewall filters for multiple supplicants on 802.1X-enabled interfaces:

- Configuring Firewall Filters on Interfaces with Multiple Supplicants on page 359

Configuring Firewall Filters on Interfaces with Multiple Supplicants

CLI Quick Configuration

To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator interface ge-0/0/2 supplicant multiple
set firewall family ethernet-switching filter filter1 term term1 from destination-address
192.0.2.16/28
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall family ethernet-switching filter filter1 term term1 then count counter1
set firewall family ethernet-switching filter filter1 term term2 then policer p1
```

Step-by-Step Procedure

To configure firewall filters on an interface enabled for multiple supplicants:

1. Configure interface **ge-0/0/2** for multiple supplicant mode authentication:

```
[edit protocols dot1x]
```

```
user@switch# set authenticator interface ge-0/0/2 supplicant multiple
```

2. Set policer definition:

```
user@switch# show policer p1 |display set
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall policer p1 then discard
```

3. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term term1 from destination-address 192.0.2.16/28
user@switch# set filter filter1 term term1 then count counter1
user@switch# set filter filter1 term term2 then policer p1
```

Results Check the results of the configuration:

```
user@switch> show configuration

firewall {
   family ethernet-switching {
      filter filter1 {
         term term1 {
            from {
               destination-address {
                  192.0.2.16/28;
               }
            }
            then count counter1;
            term term2 {
            from {
               destination-address {
                  192.0.2.16/28;
               }
            }
            then policer p1;
         }
      }
   }
   policer p1 {
      if-exceeding {
         bandwidth-limit 1m;
            burst-size-limit 1k;
         }
         then discard;
      }
}
protocols {
   dot1x {
```

```
    authenticator
      interface ge-0/0/2 {
        supplicant multiple;
      }
    }
  }
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying Firewall Filters on Interfaces with Multiple Supplicants on page 361

Verifying Firewall Filters on Interfaces with Multiple Supplicants

Purpose Verify that firewall filters are functioning on the interface with multiple supplicants.

Action

1. Check the results with one user authenticated on the interface. In this case, the user is authenticated on **ge-0/0/2**:

   ```
   user@switch> show dot1x firewall
   Filter: dot1x_ge-0/0/2
   Counters
   counter1_dot1x_ge-0/0/2_user1 100
   ```

2. When a second user, User2, is authenticated on the same interface, **ge-0/0/2**, you can verify that the filter includes the results for both of the users authenticated on the interface:

   ```
   user@switch> show dot1x firewall
   Filter: dot1x-filter-ge-0/0/0
   Counters
   counter1_dot1x_ge-0/0/2_user1 100
   counter1_dot1x_ge-0/0/2_user2 400
   ```

Meaning The results displayed by the **show dot1x firewall** command output reflect the dynamic filter created with the authentication of each new user. User1 accessed the file server located at the specified destination address 100 times, while User2 accessed the same file server 400 times.

See Also

- *Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches*
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 297

Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on EX Series Switches with ELS Support

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication" on page 356. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

On EX Series switches, firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server. The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.

This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 13.2 or later for EX Series switches
- One EX Series switch with support for ELS
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.
- Configured 802.1X authentication on the switch, with the authentication mode for the interface ge-0/0/2 set to **multiple**. See "Configuring 802.1X Interface Settings (CLI

Procedure)" on page 292 and "Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch" on page 337.

- Configured users on the RADIUS authentication server.

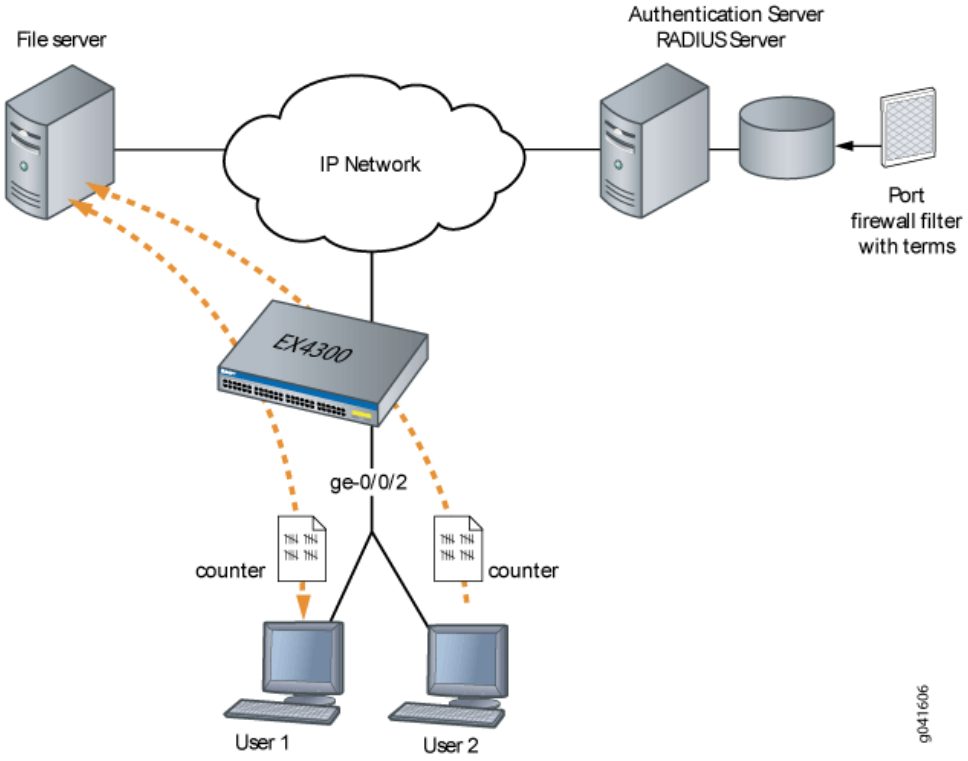
Overview and Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines the interface firewall filter with the user policies sent to the switch from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in Figure 16 on page 364, when User 1 is authenticated by the EX Series switch, the system adds a term to the firewall filter **dynamic-filter-example**. When User 2 is authenticated, another term is added to the firewall filter, and so on.

NOTE: This figure also applies to QFX5100 switches.

Figure 16: Conceptual Model: Dynamic Filter Updated for Each New User

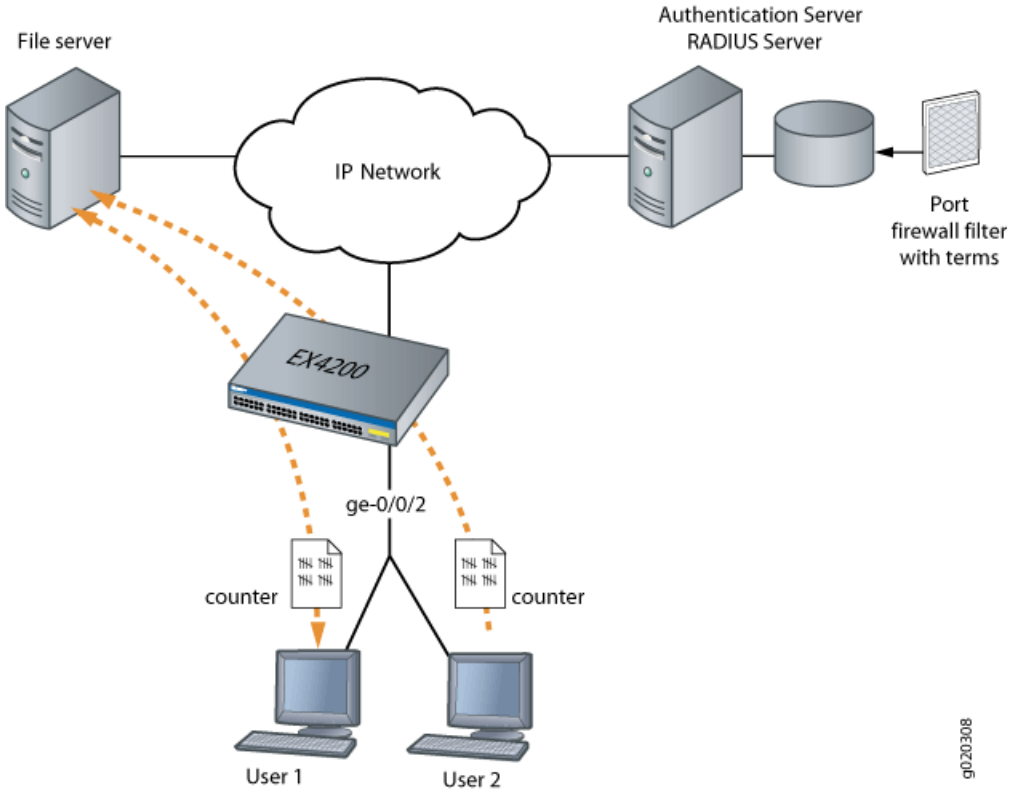


This is a conceptual model of the internal process—you cannot access or view the dynamic filter.

NOTE: If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface ge-0/0/2 to the file server, which is located on subnet 192.0.2.16/28, and set policer definitions to rate-limit the traffic. Figure 17 on page 365 shows the network topology for this example.

Figure 17: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server



Configuration

Configuring Firewall Filters on Interfaces with Multiple Supplicants

CLI Quick Configuration

To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter filter1 term term1 from ip-destination-address
192.0.2.16/28
set firewall family ethernet-switching filter filter1 term term2 from ip-destination-address
192.0.2.16/28
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1500
set firewall policer p1 then discard
set firewall family ethernet-switching filter filter1 term term1 then count counter1
set firewall family ethernet-switching filter filter1 term term2 then policer p1
```

Step-by-Step Procedure

To configure firewall filters on an interface enabled for multiple supplicants:

1. Set the policer definition:

```
user@switch# show policer p1 |display set
set firewall policer p1 if-exceeding bandwidth-limit 1m
```

```
set firewall policer p1 if-exceeding burst-size-limit 1500
set firewall policer p1 then discard
```

2. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term term1 from ip-destination-address 192.0.2.16/28
user@switch# set filter filter1 term term2 from ip-destination-address 192.0.2.16/28
user@switch# set filter filter1 term term1 then count counter1
user@switch# set filter filter1 term term2 then policer p1
```

Results Check the results of the configuration:

```
user@switch> show configuration

firewall {
    family ethernet-switching {
        filter filter1 {
            term term1 {
                from {
                    ip-destination-address {
                        192.0.2.16/28;
                    }
                }
                then count counter1;
                term term2 {
                from {
                    ip-destination-address {
                        192.0.2.16/28;
                    }
                }
                then policer p1;
            }
        }
    }
    policer p1 {
        if-exceeding {
            bandwidth-limit 1m;
                burst-size-limit 1500;
            }
            then discard;
        }
}
protocols {
    dot1x {
        authenticator
            interface ge-0/0/2 {
                supplicant multiple;
            }
        }
```

```
}
```

Verification

Verifying Firewall Filters on Interfaces with Multiple Supplicants

Purpose Verify that firewall filters are functioning on the interface with multiple supplicants.

Action

1. Check the results with one user authenticated on the interface. In this case, User 1 is authenticated on ge-0/0/2:

   ```
   user@switch> show dot1x firewall
   Filter: dot1x_ge-0/0/2
   Counters
   counter1_dot1x_ge-0/0/2_user1 100
   ```

2. When a second user, User 2, is authenticated on the same interface, ge-0/0/2, you can verify that the filter includes the results for both of the users authenticated on the interface:

   ```
   user@switch> show dot1x firewall
   Filter: dot1x-filter-ge-0/0/0
   Counters
   counter1_dot1x_ge-0/0/2_user1 100
   counter1_dot1x_ge-0/0/2_user2 400
   ```

Meaning The results displayed by the **show dot1x firewall** command output reflect the dynamic filter created with the authentication of each new user. User 1 accessed the file server located at the specified destination address **100** times, while User 2 accessed the same file server **400** times.

See Also

- *Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches*
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 297

Related Documentation

- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337

Static MAC Bypass of 802.1X and MAC RADIUS Authentication

Junos OS allows you to configure access to your LAN through 802.1X-configured interfaces without authentication, by configuring a static MAC bypass list on the EX Series switch. The static MAC bypass list, also known as the *exclusion list*, specifies MAC addresses

that are allowed on the switch without sending a request to an authentication server. For more information, read this topic.

- Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication (CLI Procedure) on page 368
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 368

Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication (CLI Procedure)

You can configure a static MAC bypass list (sometimes called the exclusion list) on the switch to specify MAC addresses of devices allowed access to the LAN without 802.1X or MAC RADIUS authentication requests to the RADIUS server.

To configure the static MAC bypass list:

- Specify a MAC address to bypass authentication:

```
[edit protocols dot1x]
user@switch# set authenticator static 00:04:0f:fd:ac:fe
```

- Configure a supplicant to bypass authentication if it is connected through a particular interface:

```
[edit protocols dot1x]
user@switch# set authenticator static 00:04:0f:fd:ac:fe interface ge-0/0/5
```

- Configure a supplicant to be moved to a specific VLAN after it is authenticated:

```
[edit protocols dot1x]
user@switch# set authenticator static 00:04:0f:fd:ac:fe interface ge-0/0/5 vlan-assignment
default-vlan
```

See Also

- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- *Configuring 802.1X Authentication (J-Web Procedure)*

Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch

To allow devices to access your LAN through 802.1X-configured interfaces without authentication, you can configure a static MAC bypass list on the EX Series switch. The static MAC bypass list, also known as the *exclusion list*, specifies MAC addresses that are allowed on the switch without sending a request to an authentication server.

You can use static MAC bypass of authentication to allow connection for devices that are not 802.1X-enabled, such as printers. If a host's MAC address is compared and matched against the static MAC address list, the nonresponsive host is authenticated and an interface opened for it.

This example describes how to configure static MAC bypass of authentication for two printers:

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.

Before you configure static MAC bypass of authentication, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

  For more about ELS, see: *Using the Enhanced Layer 2 Software CLI*.

- Specified the RADIUS server connections and configured an access profile on the switch. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.

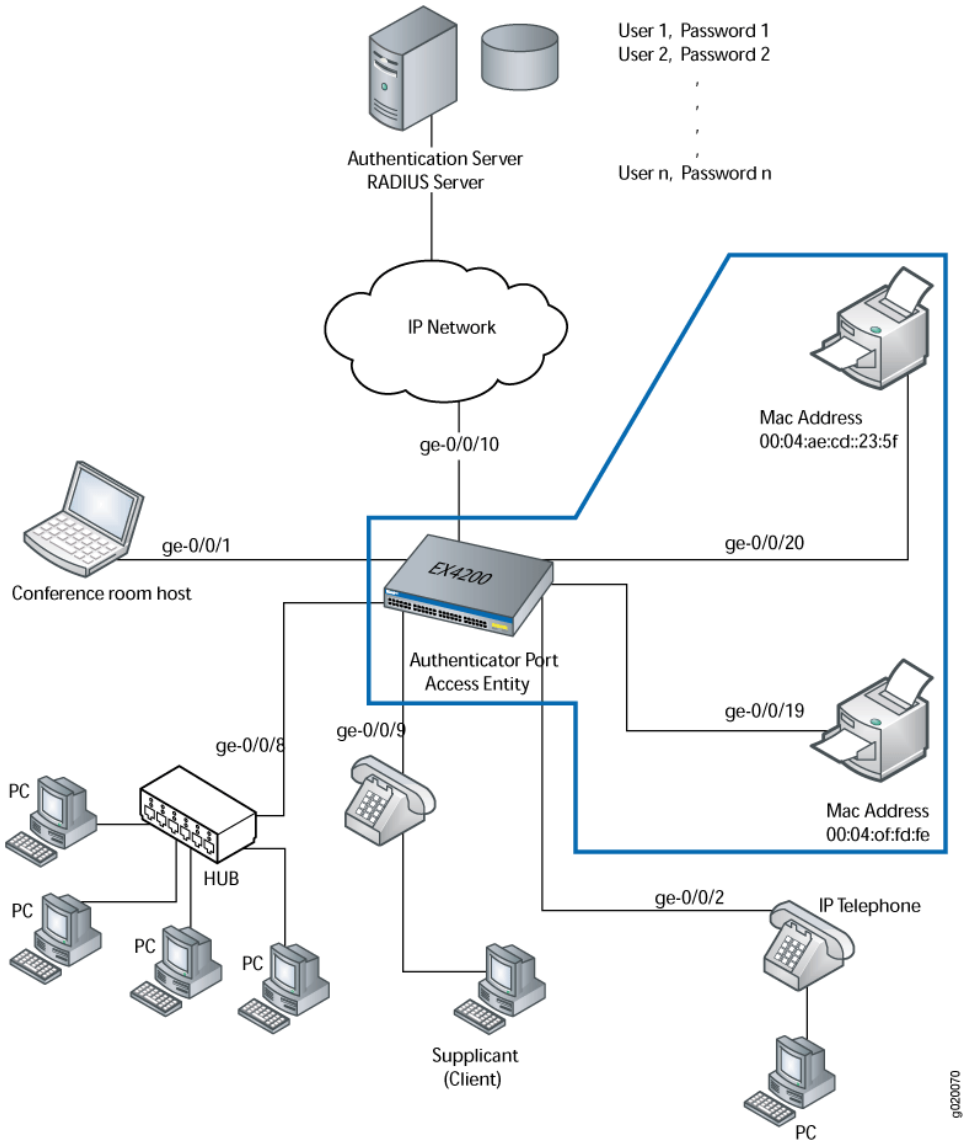
Overview and Topology

To permit printers access to the LAN, add them to the static MAC bypass list. The MAC addresses on this list are permitted access without authentication from the RADIUS server.

Figure 18 on page 370 shows the two printers connected to the EX4200.

NOTE: This figure also applies to QFX5100 switches.

Figure 18: Topology for Static MAC Bypass of Authentication Configuration



The interfaces shown in Table 29 on page 370 will be configured for static MAC bypass of authentication.

Table 29: Components of the Static MAC Bypass of Authentication Configuration Topology

Property	Settings
Switch hardware	EX4200, 24 Gigabit Ethernet ports: 16 non-PoE ports and 8 PoE ports (**ge-0/0/0** through **ge-0/0/23**)
VLAN name	**default**
Connections to integrated printer/fax/copier machines (no PoE required)	**ge-0/0/19**, MAC address 00:04:0f:fd:ac:fe **ge-0/0/20**, MAC address 00:04:ae:cd:23:5f

The printer with the MAC address 00:04:0f:fd:ac:fe is connected to access interface **ge-0/0/19**. A second printer with the MAC address 00:04:ae:cd:23:5f is connected to access interface **ge-0/0/20**. Both printers will be added to the static list and bypass 802.1X authentication.

Configuration

CLI Quick Configuration

To quickly configure the static MAC bypass list, copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
set protocols dot1x authenticator interface all supplicant multiple
set protocols dot1x authenticator authenticaton-profile-name profile1
```

Step-by-Step Procedure

Configure the static MAC bypass list:

1. Configure MAC addresses **00:04:0f:fd:ac:fe** and **00:04:ae:cd:23:5f** as static MAC addresses:

   ```
   [edit protocols]
   user@switch# set dot1x authenticator static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
   ```

2. Configure the 802.1X authentication method:

   ```
   [edit protocols]
   user@switch# set dot1x authenticator interface all supplicant multiple
   ```

3. Configure the authentication profile name (access profile name) to use for authentication:

   ```
   [edit protocols]
   user@switch# set dot1x authenticator authentication-profile-name profile1
   ```

NOTE: Access profile configuration is required only for 802.1X clients, not for static MAC clients.

Results

Display the results of the configuration:

```
user@switch> show
interfaces {
  ge-0/0/19 {
    unit 0 {
      family ethernet-switching {
        vlan members default;
      }
    }
  }
```

```
    ge-0/0/20 {
      unit 0 {
        family ethernet-switching {
          vlan members default;
        }
      }
    }
}
protocols {
    dot1x {
      authenticator {
        authentication-profile-name profile1
        static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f];
        interface {
          all {
            supplicant multiple;
          }
        }
      }
    }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying Static MAC Bypass of Authentication on page 372

Verifying Static MAC Bypass of Authentication

Purpose Verify that the MAC addresses of both printers are configured and associated with the correct interfaces.

Action Issue the operational mode command:

```
user@switch> show dot1x static-mac-address
```

```
MAC address           VLAN-Assignment          Interface
00:04:0f:fd:ac:fe     default                  ge-0/0/19.0
00:04:ae:cd:23:5f     default                  ge-0/0/20.0
```

Meaning The output field **MAC address** shows the MAC addresses of the two printers.

The output field **Interface** shows that the MAC address **00:04:0f:fd:ac:fe** can connect to the LAN through interface **ge-0/0/19.0** and that the MAC address **00:04:ae:cd:23:5f** can connect to the LAN through interface **ge-0/0/20.0**.

See Also

- *Configuring 802.1X Authentication (J-Web Procedure)*

- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- Understanding Authentication on Switches on page 268

Related Documentation

- Interfaces Enabled for 802.1X or MAC RADIUS Authentication on page 349
- 802.1X Authentication on page 289
- MAC RADIUS Authentication on page 324

Captive Portal Authentication

You can control access to your network through a switch by using several different authentication. Junos OS switches support 802.1X, MAC RADIUS, and captive portal as an authentication methods to devices requiring to connect to a network. You can set up captive portal authentication on a switch to redirect Web browser requests to a login page that requires the user to input a username and password. For more information, read this topic.

- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378
- Designing a Captive Portal Authentication Login Page on Switches on page 380
- Configuring Captive Portal Authentication (CLI Procedure) on an EX Series Switche with ELS Support on page 383
- Example: Setting Up Captive Portal Authentication on an EX Series Switch with ELS Support on page 384

Example: Setting Up Captive Portal Authentication on an EX Series Switch

You can set up captive portal authentication (hereafter referred to as captive portal) on a switch to redirect Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

This example describes how to set up captive portal on an EX Series switch:

- Requirements on page 373
- Overview and Topology on page 374
- Configuration on page 374
- Verification on page 377
- Troubleshooting on page 378

Requirements

This example uses the following hardware and software components:

- An EX Series switch that supports captive portal
- Junos OS Release 10.1 or later for EX Series switches

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.
- Generated an SSL certificate and installed it on the switch. See "Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)" on page 252.
- Designed your captive portal login page. See "Designing a Captive Portal Authentication Login Page on Switches" on page 380.

Overview and Topology

This example shows the configuration required on the switch to enable captive portal on an interface. To permit a printer connected to the captive portal interface to access the LAN without going through captive portal, add its MAC address to the authentication whitelist. The MAC addresses in this list are permitted access on the interface without captive portal.

The topology for this example consists of one EX Series switch connected to a RADIUS authentication server. One interface on the switch is configured for captive portal. In this example, the interface is configured in multiple supplicant mode.

Configuration

To configure captive portal on your switch:

CLI Quick Configuration

To quickly configure captive portal on the switch after completing the tasks in the Requirements section, copy the following commands and paste them into the switch terminal window:

```
[edit]
set access radius-server 10.204.96.165 port 1812
set access radius-server 10.204.96.165 secret "ABC123"
set access profile profile1 authentication-order radius
set access profile profile1 radius authentication-server 10.204.96.165
set system services web-management http
set system services web-management https local-certificate my-signed-cert
set services captive-portal secure-authentication https
set services captive-portal interface ge-0/0/10.0 supplicant multiple
set services captive-portal authentication-profile-name profile1
set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22
set services captive-portal custom-options post-authentication-url
http://www.my-home-page.com
```

Step-by-Step Procedure

To configure captive portal on the switch:

1. Define the server IP address, the server authentication port number, and configure the secret password. The secret password on the switch must match the secret password on the server:

```
[edit]
user@switch# set access radius-server 10.204.96.165 port 1812
[edit]
user@switch# set access radius-server 10.204.96.165 secret "ABC123"
```

2. Configure the authentication order, making **radius** the first method of authentication:

```
[edit]
user@switch# set access profile profile1 authentication-order radius
```

3. Configure the server IP address to be tried in order to authenticate the supplicant:

```
[edit]
user@switch# set access profile profile1 radius authentication-server 10.204.96.165
```

4. Enable HTTP access on the switch:

```
[edit]
user@switch# set system services web-management http
```

5. To create a secure channel for Web access to the switch, configure captive portal for HTTPS:

NOTE: You can enable HTTP without enabling HTTPS, but we recommend HTTPS for security purposes.

   a. Associate the security certificate with the Web server and enable HTTPS access on the switch:

```
[edit]
user@switch# set system services web-management https local-certificate
my-signed-cert
```

   b. Configure captive portal to use HTTPS:

```
[edit]
user@switch# set services captive-portal secure-authentication https
```

6. Enable an interface for captive portal:

```
[edit]
user@switch# set services captive-portal interface ge-0/0/10 supplicant multiple
```

7. Specify the name of the access profile to be used for captive portal authentication:

```
[edit]
user@switch# set services captive-portal authentication-profile-name profile1
```

8. (Optional) Allow specific clients to bypass captive portal:

NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the clear captive-portal mac-address *mac-address* command after adding its MAC address to the whitelist. Otherwise the new entry for the MAC address will not be added to the Ethernet switching table and authentication bypass will not be allowed.

```
[edit]
user@switch# set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22
```

NOTE: Optionally, you can use set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22 interface ge-0/0/10.0 to limit the scope to the interface.

9. (Optional) To redirect clients to a specified page rather than the page they originally requested, configure the post-authentication URL:

```
[edit]
user@switch# set services captive-portal custom-options post-authentication-url
http://www.my-home-page.com
```

Results Display the results of the configuration:

```
[edit]
user@switch> show
system {
   services {
      web-management {
         http;
         https {
            local-certificate my-signed-cert;
         }
      }
   }
}
security {
   certificates {
      local {
         my-signed-cert {
            "-----BEGIN RSA PRIVATE KEY-----ABC123
               ...
               ABC123-----END CERTIFICATE-----\n"; ## SECRET-DATA
         }
```

```
    }
  }
}
services {
  captive-portal {
    interface {
      ge-0/0/10.0 {
        supplicant multiple;
      }
    }
    secure-authentication https;
  }
}
ethernet-switching-options {
  authentication-whitelist {
    00:10:12:e0:28:22/48;
  }
}
```

Verification

To confirm that captive portal is configured and working properly, perform these tasks:

- Verifying That Captive Portal Is Enabled on the Interface on page 377
- Verify That Captive Portal Is Working Correctly on page 377

Verifying That Captive Portal Is Enabled on the Interface

Purpose Verify that captive portal is configured on interface ge-0/0/10.

Action Use the operational mode command **show captive-portal interface *interface-name* detail**:

```
user@switch> show captive-portal interface ge-0/0/10.0 detail
ge-0/0/10.0
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Configured CP session timeout: 3600 seconds
  Server timeout: 15 seconds
```

Meaning The output confirms that captive portal is configured on interface ge-0/0/10 with the default settings for number of retries, quiet period, CP session timeout, and server timeout.

Verify That Captive Portal Is Working Correctly

Purpose Verify that captive portal is working on the switch.

Action Connect a client to interface ge-0/0/10. From the client, open a Web browser and request a webpage. The captive portal login page that you designed should be displayed. After

you enter your login information and are authenticated against the RADIUS server, the Web browser should display either the page you requested or the post-authentication URL that you configured.

Troubleshooting

To troubleshoot captive portal, perform these tasks:

- Troubleshooting Captive Portal on page 378

Troubleshooting Captive Portal

Problem The switch does not return the captive portal login page when a user connected to a captive portal interface on the switch requests a Web page.

Solution You can examine the ARP, DHCP, HTTPS, and DNS counters—if one or more of these counters are not incrementing, this provides an indication of where the problem lies. For example, if the client cannot get an IP address, check the switch interface to determine whether the DHCP counter is incrementing—if the counter increments, the DHCP packet was received by the switch.

```
user@switch> show captive-portal firewall ge-0/0/10.0
ge-0/0/10.0
  Filter name: dot1x_ge-0/0/10
Counters:
Name                            Bytes              Packets
dot1x_ge-0/0/10_CP_arp           7616                  119
dot1x_ge-0/0/10_CP_dhcp             0                    0
dot1x_ge-0/0/10_CP_http             0                    0
dot1x_ge-0/0/10_CP_https            0                    0
dot1x_ge-0/0/10_CP_t_dns            0                    0
dot1x_ge-0/0/10_CP_u_dns            0                    0
```

Configuring Captive Portal Authentication (CLI Procedure)

Configure captive portal authentication (hereafter referred to as captive portal) on an EX Series switch so that users connected to the switch are authenticated before being allowed to access the network. When the user requests a web page, a login page is displayed that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.
- Generated an SSL certificate and installed it on the switch. See "Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)" on page 252.

- Configured basic access between the EX Series switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.
- Designed your captive portal login page. See "Designing a Captive Portal Authentication Login Page on Switches" on page 380.

This topic includes the following tasks:

Configuring Secure Access for Captive Portal

To configure secure access for captive portal:

1. Enable HTTP access on the switch:

```
[edit]
user@switch# set system services web-management http
```

2. Associate the security certificate with the Web server and enable HTTPS access on the switch:

```
[edit]
user@switch# set system services web-management https local-certificate my-signed-cert
```

NOTE: You can enable HTTP without HTTPS, but we recommend HTTPS for security purposes.

3. Configure captive portal to use HTTPS:

```
[edit]
user@switch# set services captive-portal secure-authentication https
```

Enabling an Interface for Captive Portal

To enable an interface for captive portal:

```
[edit]
user@switch# set services captive-portal interface interface-name
```

For example, to enable captive portal on the interface ge-0/0/10:

```
[edit]
user@switch# set services captive-portal interface ge-0/0/10
```

Configuring Bypass of Captive Portal Authentication

To allow specific clients to bypass captive portal:

```
[edit]
user@switch# set ethernet-switching-options authentication-whitelist mac-address
```

For example, to allow specific clients to bypass captive portal:

```
[edit]
user@switch# set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22
```

NOTE: Optionally, you can use **set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22 interface ge-0/0/10.0** to limit the scope to the interface.

NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the **clear captive-portal mac-address *mac-address*** command after adding its MAC address to the whitelist. Otherwise the new entry for the MAC address will not be added to the Ethernet switching table and authentication bypass will not be allowed.

Designing a Captive Portal Authentication Login Page on Switches

You can set up captive portal authentication on your switch to redirect all Web browser requests to a login page that requires users to input a username and password before they are allowed access. Upon successful authentication, users are allowed access to the network and redirected to the original page requested.

Junos OS provides a customizable template for the captive portal window that allows you to easily design and modify the look of the captive portal login page. You can modify the design elements of the template to change the look of your captive portal login page and to add instructions or information to the page. You can also modify any of the design elements of a captive portal login page.

The first screen displayed before the captive login page requires the user to read the terms and conditions of use. By clicking the Agree button, the user can access the captive portal login page.

Figure 19 on page 381 shows an example of a captive portal login page:

Figure 19: Example of a Captive Portal Login Page

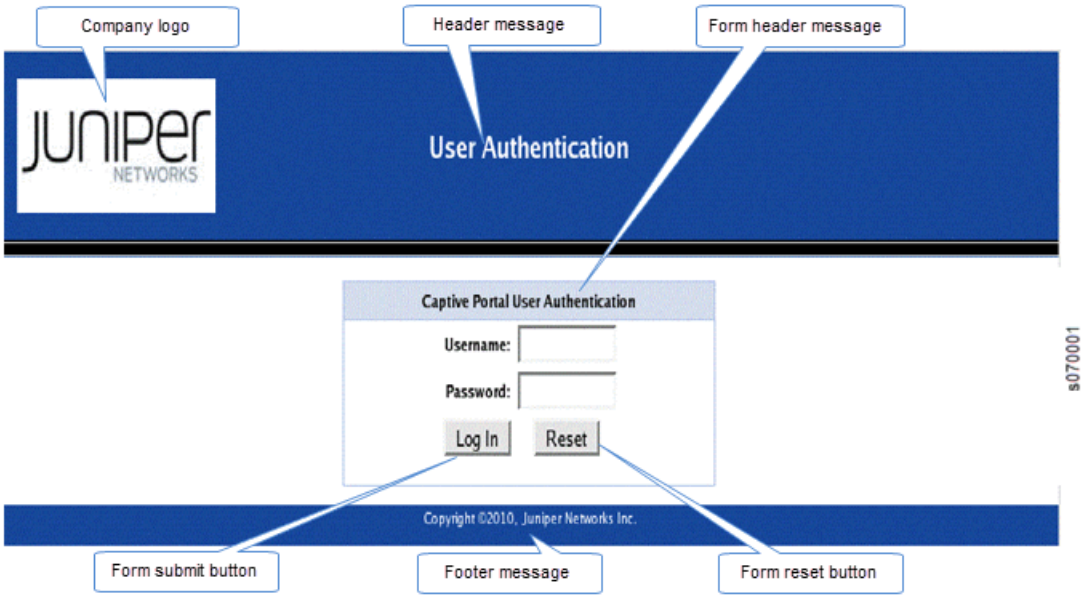


Table 30 on page 381 summarizes the configurable elements of a captive portal login page.

Table 30: Configurable Elements of a Captive Portal Login Page

Element	CLI Statement	Description
Footer background color	**footer-bgcolor** ***hex-color***	The HTML hexadecimal code for the background color of the captive portal login page footer.
Footer message	**footer-message** ***text-string***	Text displayed in the footer of the captive portal login page. You can include copyright information, links, and additional information such as help instructions, legal notices, or a privacy policy The default text shown in the footer is **Copyright @2010, Juniper Networks Inc.**
Footer text color	**footer- text-color** ***color***	Color of the text in the footer. The default color is white.
Form header background color	**form-header-bgcolor** ***hex-color***	The HTML hexadecimal code for the background color of the header bar across the top of the form area of the captive portal login page.
Form header message	**form-header-message** ***text-string***	Text displayed in the header of the captive portal login page. The default text is **Captive Portal User Authentication** .
Form header text color	**form-header- text- color** *color*	Color of the text in the form header. The default color is black.
Form reset button label	**form-reset-label** ***label-name***	Using the **Reset** button, the user can clear the username and password fields on the form.

Table 30: Configurable Elements of a Captive Portal Login Page (continued)

Element	CLI Statement	Description
Form submit button label	**form-submit-label** ***label-name***	Using the **Login** button, the user can submit the login information.
Header background color	**header-bgcolor** ***hex-color***	The HTML hexadecimal code for the background color of the captive portal login page header.
Header logo	**header-logo** ***filename***	Filename of the file containing the image of the logo that you want to appear in the header of the captive portal login page. The image file can be in GIF, JPEG, or PNG format. You can upload a logo image file to the switch. Copy the logo to the /var/tmp directory on the switch (during commit, the files are saved to persistent locations). If you do not specify a logo image, the Juniper Networks logo is displayed.
Header message	**header-message** ***text-string***	Text displayed in the page header. The default text is **User Authentication**.
Header text color	**header-text- color***color*	Color of the text in the header. The default color is white.
Post-authentication URL	**post-authentication-url** ***url***	URL to which the users are directed on successful authentication. By default, users are directed to the page they had originally requested.

To design the captive portal login page:

1. (Optional) Upload your logo image file to the switch:

   ```
   user@switch> file copy ftp://username:prompt@ftp.hostname.net/var/tmp/my-logo.jpeg
   ```

2. Configure the custom options to specify the background colors and text displayed in the captive portal page:

   ```
   [edit system services captive-portal]
   user@switch# set custom-options header-bgcolor #006600
   set custom-options header-message “Welcome to Our Network”
   set custom-options banner-message “Please enter your username and password”.The banner
   displays the message ”XXXXXXX” by default. The user can modify this message.
   set custom-options footer-message “Copyright ©2010, Our Network”
   ```

Now you can commit the configuration.

NOTE: For the custom options that you do not specify, the default value is used.

See Also

- Understanding Authentication on Switches on page 268
- captive-portal on page 920

Configuring Captive Portal Authentication (CLI Procedure) on an EX Series Switche with ELS Support

NOTE: This task uses Junos OS for switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Configuring Captive Portal Authentication (CLI Procedure)" on page 378. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

Configure captive portal authentication (hereafter referred to as captive portal) on a switch so that users connected to the switch are authenticated before being allowed to access the network. When the user requests a webpage, a login page is displayed that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* .
- Generated an SSL certificate and installed it on the switch. See "Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)" on page 252.
- Configured basic access between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.
- Designed your captive portal login page. See "Designing a Captive Portal Authentication Login Page on Switches" on page 380.

This topic includes the following tasks:

Configuring Secure Access for Captive Portal

To configure secure access for captive portal:

1. Associate the security certificate with the Web server and enable HTTPS on the switch:

```
[edit]
user@switch# set system services web-management https local-certificate certificate-name
```

NOTE: You can enable HTTP instead of HTTPS, but we recommend HTTPS for security purposes.

2. Configure captive portal to use HTTPS:

```
[edit]
user@switch# set services captive-portal secure-authentication https
```

Enabling an Interface for Captive Portal

To enable an interface for use with captive portal authentication:

```
[edit]
user@switch# set services captive-portal interface interface-name
```

Configuring Bypass of Captive Portal Authentication

You can allow specific clients to bypass captive portal authentication:

```
[edit]
user@switch# set switch-options authentication-whitelist mac-address
```

NOTE: Optionally, you can use **set switch-options authentication-whitelist** *mac-address* **interface** *interface-name* to limit the scope to the interface.

NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the **clear captive-portal mac-address** *session-mac-addr* command after adding its MAC address to the whitelist. Otherwise, the new entry for the MAC address is not added to the Ethernet switching table and the authentication bypass is not allowed.

Example: Setting Up Captive Portal Authentication on an EX Series Switch with ELS Support

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Example: Setting Up Captive Portal Authentication on an EX Series Switch" on page 373. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

You can set up captive portal authentication (hereafter referred to as captive portal) on a switch to redirect Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

This example describes how to set up captive portal on an EX Series switch:

Requirements

This example uses the following software and hardware components:

- Junos OS Release 13.2X50 or later for EX Series switches
- An EX Series switch with support for ELS

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* .
- Generated an SSL certificate and installed it on the switch. See "Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)" on page 252.
- Configured basic access between the EX Series switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.
- Designed your captive portal login page. See "Designing a Captive Portal Authentication Login Page on Switches" on page 380.

Overview and Topology

This example shows the configuration required on the switch to enable captive portal on an interface. To permit a printer connected to the captive portal interface to access the LAN, add its MAC address to the authentication whitelist and assign it to a VLAN, vlan1. The MAC addresses on this list are permitted access on the interface without captive portal authentication.

The topology for this example consists of one EX Series switch connected to a RADIUS authentication server. One interface on the switch is configured for captive portal. In this example, the interface is configured in multiple supplicant mode.

Configuration

To configure captive portal on your switch:

CLI Quick Configuration

To quickly configure captive portal on the switch after completing the tasks in the Requirements section, copy the following commands and paste them into the switch terminal window:

```
[edit]
set system services web-management https local-certificate my-signed-cert
set services captive-portal secure-authentication https
set services captive-portal interface ge-0/0/10.0 supplicant multiple
set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment vlan1
set custom-options post-authentication-url http://www.my-home-page.com
```

Step-by-Step Procedure

1. To create a secure channel for Web access to the switch, configure captive portal for HTTPS:

   a. Associate the security certificate with the Web server and enable HTTPS on the switch:

   ```
   [edit]
   user@switch# set system services web-management https local-certificate
   my-signed-cert
   ```

   NOTE: You can enable HTTP instead of HTTPS, but we recommend that you enable HTTPS for security purposes.

   b. Configure captive portal to use HTTPS:

   ```
   [edit]
   user@switch# set services captive-portal secure-authentication https
   ```

2. Enable an interface for captive portal:

   ```
   [edit]
   user@switch# set services captive-portal interface ge-0/0/10 supplicant multiple
   ```

3. (Optional) Allow specific clients to bypass captive portal authentication:

   NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the clear captive-portal mac-address *mac-address* command after adding its MAC address to the whitelist. Otherwise, the new entry for the MAC address will not be added to the Ethernet switching table and the authentication bypass will not be allowed.

   ```
   [edit]
   user@switch# set switch-options authentication-whitelist 00:10:12:e0:28:22
   vlan-assignment vlan1
   ```

   NOTE: Optionally, you can use **set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment vlan1 interface ge-0/0/10.0** to limit the scope to the interface.

4. (Optional) To redirect clients to a specified page rather than the page they originally requested, configure the post-authentication URL:

```
[edit services captive-portal]
user@switch# set custom-options post-authentication-url http://www.my-home-page.com
```

Results Display the results of the configuration:

```
[edit]
user@switch# show
system {
  services {
    web-management {
      https {
        local-certificate my-signed-cert;
      }
    }
  }
}
security {
  certificates {
    local {
      my-signed-cert {
        "-----BEGIN RSA PRIVATE KEY-----\ABC123
          ABC123ABC123ABC123 ... ABC123
          ----END CERTIFICATE-----\n"; ## SECRET-DATA
      }
    }
  }
}
services {
  captive-portal {
    interface {
      ge-0/0/10.0 {
        supplicant multiple;
      }
    }
    secure-authentication https;
    custom-options {
      post-authentication-url http://www.my-home-page.com;
    }
  }
}
switch-options {
  authentication-whitelist {
    00:10:12:e0:28:22/48 {
      vlan-assignment vlan1;
    }
  }
}
```

Verification

To confirm that captive portal authentication is configured and working properly, perform these tasks:

- Verifying That Captive Portal Is Enabled on the Interface on page 388
- Verify That Captive Portal Is Working Correctly on page 388

Verifying That Captive Portal Is Enabled on the Interface

Purpose Verify that captive portal is configured on the interface ge-0/0/10.

Action Use the operational mode command **show captive-portal interface *interface-name* detail**:

```
user@switch> show captive-portal interface ge-0/0/10.0 detail
ge-0/0/10.0
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Configured CP session timeout: 3600 seconds
  Server timeout: 15 seconds
```

Meaning The output confirms that captive portal is configured on the interface **ge-0/0/10**, with the default settings for number of retries, quiet period, CP session timeout, and server timeout.

Verify That Captive Portal Is Working Correctly

Purpose Verify that captive portal is working on the switch.

Action Connect a client to the interface ge-0/0/10. From the client, open a Web browser and request a webpage. The captive portal login page that you designed should be displayed. After you enter your login information and are authenticated against the RADIUS server, the Web browser should display either the page you requested or the post-authentication URL that you configured.

Troubleshooting

To troubleshoot captive portal, perform this task:

- Troubleshooting Captive Portal on page 388

Troubleshooting Captive Portal

Problem The switch does not return the captive portal login page when a user connected to a captive portal interface on the switch requests a webpage.

Solution You can examine the ARP, DHCP, HTTPS, and DNS counters—if one or more of these counters are not incrementing, this provides an indication of where the problem lies. For example, if the client cannot get an IP address, you might check the switch interface to determine whether the DHCP counter is incrementing—if the counter increments, the DHCP packet was received by the switch.

```
user@switch> show captive-portal firewall ge-0/0/10.0
ge-0/0/10.0
  Filter name: dot1x_ge-0/0/10
Counters:
Name                            Bytes              Packets
dot1x_ge-0/0/10_CP_arp           7616                  119
dot1x_ge-0/0/10_CP_dhcp             0                    0
dot1x_ge-0/0/10_CP_http             0                    0
dot1x_ge-0/0/10_CP_https            0                    0
dot1x_ge-0/0/10_CP_t_dns            0                    0
dot1x_ge-0/0/10_CP_u_dns            0                    0
```

Related Documentation

- Flexible Authentication Order on EX Series Switches on page 389
- Central Web Authentication on page 393
- Centralized Access Control to Network Resources on EX Series Switches on page 399

Flexible Authentication Order on EX Series Switches

Junos OS switches support 802.1X, MAC RADIUS, and captive portal as an authentication methods to devices requiring to connect to a network. You can use the flexible authentication order feature to specify the order of authentication methods that the switch uses when attempting to authenticate a client. If multiple authentication methods are configured on a single interface, when one authentication method fails, the switch falls back to another method. For more information, read this topic.

- Configuring Flexible Authentication Order on page 389
- Configuring EAPoL Block to Maintain an Existing Authentication Session on page 392

Configuring Flexible Authentication Order

You can use the flexible authentication order feature to specify the order of authentication methods that the switch uses when attempting to authenticate a client. If multiple authentication methods are configured on a single interface, when one authentication method fails, the switch falls back to another method.

By default, the switch attempts to authenticate a client by using 802.1X authentication first. If 802.1X authentication fails because there is no response from the client, and MAC RADIUS authentication is configured on the interface, the switch will attempt authentication using MAC RADIUS. If MAC RADIUS fails, and captive portal is configured on the interface, the switch attempts authentication using captive portal.

With a flexible authentication order, the sequence of authentication method used can be changed based on the type of clients connected to the interface. You can configure the **authentication-order** statement to specify whether 802.1X authentication or MAC RADIUS authentication must be the first authentication method tried. Captive portal is always the last authentication method tried.

If MAC RADIUS authentication is configured as the first authentication method in the order, then on receiving data from any client, the switch attempts to authenticate the client by using MAC RADIUS authentication. If MAC RADIUS authentication fails, then the switch uses 802.1X authentication to authenticate the client. If 802.1X authentication fails, and captive portal is configured on the interface, the switch attempts authentication using captive portal.

NOTE: If 802.1X authentication and MAC RADIUS authentication fail, and captive portal is not configured on the interface, the client is denied access to the LAN unless a server fail fallback method is configured. See "Configuring RADIUS Server Fail Fallback (CLI Procedure)" on page 287 for more information.

Different authentication methods can be used in parallel on an interface that is configured in multiple-supplicant mode. Therefore, if an end device is authenticated on the interface by using captive portal, another end device connected to that interface can still be authenticated using 802.1X or MAC RADIUS authentication.

Before you configure the flexible authentication order on an interface, make sure that the authentication methods are configured on that interface. The switch does not attempt authentication using a method that is not configured on the interface, even if that method is included in the authentication order; the switch ignores that method and attempts the next method in the authentication order that is enabled on that interface.

Use the following guidelines when configuring the **authentication-order** statement:

- The authentication order must include at least two methods of authentication.
- 802.1X authentication must be one of the methods included in the authentication order.
- If captive portal is included in the authentication order, it must be the last method in the order.
- If **mac-radius-restrict** is configured on an interface then the authentication order cannot be configured on that interface.

To configure a flexible authentication order, use one of the following valid combinations:

NOTE: The authentication order can be configured globally using the **interface all** option as well as locally using the individual interface name. If the authentication order is configured both for an individual interface and for all interfaces, the local configuration for that interface overrides the global configuration.

- To configure 802.1X authentication as the first authentication method, followed by MAC RADIUS authentication, and then captive portal:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface interface-name authentication-order
  [dot1x mac-radius captive-portal]
  ```

- To configure 802.1X authentication as the first authentication method, followed by captive portal:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface interface-name authentication-order
  [dot1x captive-portal]
  ```

- To configure 802.1X authentication as the first authentication method, followed by MAC RADIUS authentication:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface interface-name authentication-order
  [dot1x mac-radius]
  ```

- To configure MAC RADIUS authentication as the first authentication method, followed by 802.1X, followed by captive portal:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface interface-name authentication-order
  [mac-radius dot1x captive-portal]
  ```

After you configure the authentication order, you must use the **insert** command to make any modifications to the authentication order. Using the **set** command does not change the configured order.

To change the authentication order after initial configuration:

```
[edit]
user@switch# insert protocols dot1x authenticator interface interface-name authentication-order
authentication-method before authentication-method
```

For example, to change the order from **[mac-radius dot1x captive portal]** to **[dot1x mac-radius captive portal]**:

```
[edit]
user@switch# insert protocols dot1x authenticator interface interface-name authentication-order
dot1x before mac-radius
```

See Also

- Understanding Authentication on Switches on page 268
- Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 326

Configuring EAPoL Block to Maintain an Existing Authentication Session

When a switch acting as an 802.1X authenticator receives an EAP-Start message from an authenticated client, the switch tries to re-authenticate the client using the 802.1X method and typically returns an EAP-Request message, and waits for a response. If the client fails to respond, the switch attempts to re-authenticate the client using MAC RADIUS or captive portal method if these methods were configured. Clients that have been authenticated using MAC RADIUS or captive portal authentication are non-responsive, and traffic is dropped on the interface as the switch attempts re-authentication.

If you have configured flexible authentication order on the interface so that MAC RADIUS is the first method used to authenticate a client, the switch still reverts to using 802.1X for re-authentication if the client sends an EAP-Start message, even if the client was successfully authenticated using MAC RADIUS authentication. You can configure an EAPoL block with either a fixed or flexible authentication order. If you do not configure the **authentication-order** statement, the order is fixed by default. The **eapol-block** statement can be configured with or without configuring the **authentication-order** statement.

You can configure a switch to ignore EAP-Start messages sent from a client that has been authenticated using MAC RADIUS authentication or captive portal authentication using the **eapol-block** statement. With a block of EAPoL messages in effect, if the switch receives an EAP-Start message from the client, it does not return an EAP-Request message, and the existing authentication session is maintained.

NOTE: If the endpoint has not been authenticated with MAC RADIUS authentication or captive portal authentication, the EAPoL block does not take effect. The endpoint can authenticate using 802.1X authentication.

If **eapol-block** is configured with the **mac-radius** option, then once the client is authenticated with MAC RADIUS authentication or CWA (Central Web Authentication), the client remains in authenticated state even if it sends an EAP-Start message. If **eapol-block** is configured with the **captive-portal** option, then once the client is authenticated with captive portal, the client remains in authenticated state even if it sends an EAP-Start message.

NOTE: This feature is supported on EX4300 and EX9200 switches.

To configure a block of EAPoL messages to maintain an existing authentication session:

- To configure EAPoL block for a client authenticated using MAC RADIUS authentication:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name eapol-block
mac-radius
```

- To configure EAPoL block for a client authenticated using captive portal authentication:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name eapol-block
captive-portal
```

See Also
- Understanding Authentication on Switches on page 268

Related Documentation
- Access Control and Authentication on Switching Devices on page 267

Central Web Authentication

Web authentication provides access to network for users by redirecting the client's Web browser to a central Web authentication server (CWA server), which handles the complete login process. Web authentication can also be used as a fallback authentication method for regular network users who have 802.1X-enabled devices, but fail authentication because of other issues, such as expired network credentials.

- Understanding Central Web Authentication on page 393
- Configuring Central Web Authentication on page 396

Understanding Central Web Authentication

Web authentication redirects Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed access to the network. Web authentication is useful for providing network access to temporary users, such as visitors to a corporate site, who try to access the network using devices that are not 802.1X-enabled. Web authentication can also be used as a fallback authentication method for regular network users who have 802.1X-enabled devices, but fail authentication because of other issues, such as expired network credentials.

Web authentication can be done locally on the switch using captive portal, but this requires that the Web portal pages be configured on each switch used as a network access device. Central Web authentication (CWA) provides efficiency and scaling benefits

by redirecting the client's Web browser to a central Web authentication server (CWA server), which handles the complete login process.

Central Web Authentication Process

Central Web authentication is invoked after a host has failed MAC RADIUS authentication. The host can attempt authentication using 802.1X authentication first, but must then attempt MAC RADIUS authentication before attempting central Web authentication. The switch, operating as the authenticator, exchanges RADIUS messages with the authentication, authorization, and accounting (AAA) server. After MAC RADIUS authentication fails, the switch receives an Access-Accept message from the AAA server. This message includes a dynamic firewall filter and a redirect URL for central Web authentication. The switch applies the filter, which allows the host to receive an IP address, and uses the URL to redirect the host to the Web authentication page.

The host is prompted for login credentials and might also be asked to agree to an acceptable use policy. If Web authentication is successful, the AAA server sends a Change of Authorization (CoA) message, which updates the terms of the authorized session in progress. This enables the authenticator to update the filter or VLAN assignment applied to the controlled port, to allow the host to access the LAN.

The sequence of events in central Web authentication is as follows (see Figure 20 on page 395):

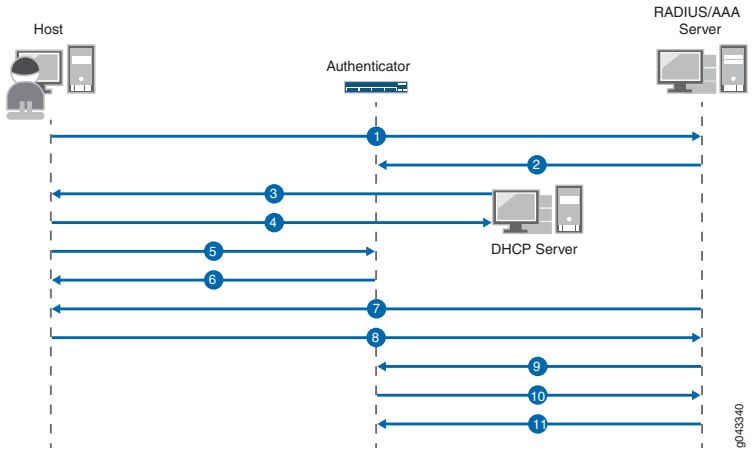
1. A host connected to the switch (authenticator) initiates MAC RADIUS authentication.
2. MAC RADIUS authentication fails. Instead of sending an Access-Reject message to the switch, the AAA server sends an Access-Accept message that includes a dynamic firewall filter and a CWA redirect URL.
3. The host is allowed by the terms of the filter to send DHCP requests.
4. The host receives an IP address and DNS information from the DHCP server. The AAA server initiates a new session that has a unique session ID.
5. The host opens a Web browser.
6. The authenticator sends the CWA redirect URL to the host.
7. The host is redirected to the CWA server and is prompted for login credentials.
8. The host provides the username and password.

9. After successful Web authentication, the AAA server sends a CoA message to udpate the filter or VLAN assignment applied on the controlled port, allowing the host to access the LAN.

10. The authenticator responds with a CoA-ACK message and sends a MAC RADIUS authentication request to the AAA server.

11. The AAA server matches the session ID to the appropriate access policy and sends an Access-Accept message to authenticate the host.

Figure 20: Central Web Authentication Process



Dynamic Firewall Filters for Central Web Authentication

Central Web authentication uses dynamic firewall filters, which are centrally defined on the AAA server and dynamically applied to supplicants that request authentication through that server. The filter allows the host to get an IP address dynamically using DHCP. You define the filters by using RADIUS attributes, which are included in the Access-Accept messages sent from the server. Filters can be defined using either the Juniper-Switching-Filter attribute, which is a vendor-specific attribute (VSA), or the Filter-ID attribute, which is an IETF RADIUS attribute.

To use the Juniper-Switching-Filter VSA for central Web authentication, you must configure the filter with the correct terms that allow the destination IP address of the CWA server. This configuration is done directly on the AAA server. To use the Filter-ID attribute for central web authentication, enter the value as JNPR_RSVD_FILTER_CWA on the AAA server. The filter terms for this attribute are internally defined for central Web authentication, because of which no additional configuration is required. For more information about configuring dynamic firewall filters for central web authentication, see “Configuring Central Web Authentication” on page 396.

Redirect URL for Central Web Authentication

In central Web authentication, the authenticator redirects the host’s Web browser request to the CWA server by using a redirect URL. After redirection, the CWA server completes

the login process. The redirect URL for central web authentication can be configured on the AAA server or on the authenticator. The redirect URL, along with the dynamic firewall filter, must be present to trigger the central web authentication process after the failure of MAC RADIUS authentication.

The redirect URL can be centrally defined on the AAA server by using the Juniper-CWA-Redirect VSA, which is attribute number 50 in the Juniper RADIUS dictionary. The URL is forwarded from the AAA server to the switch in the same RADIUS Access-Accept message that contains the dynamic firewall filter. You can also configure the redirect URL locally on the host interface by using the CLI statement **redirect-url** at the [**edit protocols dot1x authenticator interface *interface-name***] hierarchy level. For more information about configuring the redirect URL, see "Configuring Central Web Authentication" on page 396.

See Also

- Understanding Dynamic Filters Based on RADIUS Attributes on page 306
- Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 307
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 297

Configuring Central Web Authentication

Central Web authentication is a fallback method of authentication in which the host's Web browser is redirected to a central Web authentication (CWA) server. The CWA server provides a web portal where the user can enter a username and password. If these credentials are validated by the CWA server, the user is authenticated and is allowed access to the network.

Central Web authentication is invoked after a host has failed MAC RADIUS authentication. The switch, operating as the authenticator, receives a RADIUS Access-Accept message from the AAA server that includes a dynamic firewall filter and a redirect URL for central Web authentication. The dynamic firewall filter and the redirect URL must both be present for the central Web authentication process to be triggered.

- Configuring Dynamic Firewall Filters for Central Web Authentication on page 396
- Configuring the Redirect URL for Central Web Authentication on page 397
- Guidelines for Configuring Central Web Authentication on page 398

Configuring Dynamic Firewall Filters for Central Web Authentication

Dynamic firewall filters are used in central Web authentication to enable the host to get an IP address from a DHCP server, which allows the host to access the network. The filters are defined on the AAA server using RADIUS attributes, which are sent to the authenticator in an Access-Accept message. You can define the filter using either the Juniper-Switching-Filter attribute, which is a vendor-specific attribute (VSA), or the Filter-ID attribute, which is an IETF RADIUS attribute.

- To use the Juniper-Switching-Filter VSA for central Web authentication, you must configure the filter terms directly on the AAA server. The filter must include a term to match the destination IP address of the CWA server with the action **allow**.

For example:

```
001122334455 Auth-Type := EAP, Cleartext-Password :="001122334455"
        Session-Timeout = "300",
        Juniper-CWA-Redirect-URL = "https://10.10.10.10",
        Juniper-Switching-Filter = "Match Destination-ip 10.10.10.10 Action
allow, Match ip-protocol 17 Action allow, Match Destination-mac 00:01:02:33:44:55
 Action deny"
```

NOTE: The switch does not resolve the DNS queries for the redirect URL. You must configure the Juniper-Switching-Filter attribute to allow the destination IP address of the CWA server.

- To use the Filter-ID attribute for central Web authentication, enter JNPR_RSVD_FILTER_CWA as the value for the attribute on the AAA server. The filter terms for this attribute are internally defined for central Web authentication, because of which no additional configuration is required.

  For example:

```
001122334455 Auth-Type := EAP, Cleartext-Password :="001122334455"
        Session-Timeout = "300",
        Juniper-CWA-Redirect-URL = "https://10.10.10.10",
        Filter-Id = "JNPR_RSVD_FILTER_CWA",
```

For more information about configuring dynamic firewall filters on the AAA server, see the documentation for your AAA server.

Configuring the Redirect URL for Central Web Authentication

In central Web authentication, the authenticator redirects the host's Web browser request to the CWA server by using a redirect URL. The redirect URL for central Web authentication can be configured on the AAA server or locally on the host interface.

- To configure the redirect URL on the AAA server, use the Juniper-CWA-Redirect VSA, which is attribute number 50 in the Juniper RADIUS dictionary. The URL is forwarded from the AAA server to the switch in the same RADIUS Access-Accept message that contains the dynamic firewall filter.

  For example:

```
001122334455 Auth-Type := EAP, Cleartext-Password :="001122334455"
        Session-Timeout = "300",
        Juniper-CWA-Redirect-URL = "https://10.10.10.10",
        Filter-Id = "JNPR_RSVD_FILTER_CWA",
```

NOTE: When the special Filter-ID attribute JNPR_RSVD_FILTER_CWA is used for the dynamic firewall filter, the redirect URL must include the IP address of the AAA server, for example, https://10.10.10.10.

- To configure the redirect URL locally on the host interface, use the following CLI statement:

  ```
  [edit]
  user@switch#  set protocols dot1x authenticator interface interface-name redirect-url
  ```

  For example:

  ```
  user@switch# show protocols dot1x
  authenticator {
    authentication-name-profile auth1;
    interface {
      ge-0/0/1.0 {
        supplicant single;
        mac-radius;
        redirect-url https://10.10.10.10;
      }
    }
  }
  ```

Guidelines for Configuring Central Web Authentication

Central Web authentication is triggered after the failure of MAC RADIUS authentication when the redirect URL and dynamic firewall filter are both present. The redirect URL and dynamic firewall filter can be configured in any of the following combinations:

1. The AAA server sends both the CWA redirect URL and dynamic firewall filter to the authenticator. The redirect URL is configured on the AAA server by using the Juniper-CWA-Redirect VSA and the dynamic firewall filter is configured on the AAA server by using the Juniper-Switching-Filter VSA. The filter must be configured to allow the destination IP address of the CWA server in this case.
2. The AAA server sends the dynamic firewall filter to the authenticator and the redirect URL is configured locally on the host port. The redirect URL is configured on the authenticator by using the **redirect-url** CLI statement and the dynamic firewall filter is configured on the AAA server by using the Juniper-Switching-Filter VSA. The filter must be configured to allow the destination IP address of the CWA server in this case.
3. The AAA server sends both the CWA redirect URL and dynamic firewall filter to the authenticator. The redirect URL is configured on the AAA server by using the Juniper-CWA-Redirect VSA and the dynamic firewall filter is configured on the AAA server by using the Filter-ID attribute with the value JNPR_RSVD_FILTER_CWA. The redirect URL must contain the IP address of the CWA server in this case.
4. The AAA server sends the dynamic firewall filter to the authenticator and the redirect URL is configured locally on the host port. The redirect URL is configured on the authenticator by using the **redirect-url** CLI statement and the dynamic firewall filter is configured on the AAA server by using the Filter-ID attribute with the value JNPR_RSVD_FILTER_CWA. The redirect URL must contain the IP address of the CWA server in this case.

Related Documentation

- Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass

Centralized Access Control to Network Resources on EX Series Switches

Network access control (NAC) allows you to control access to network resources such as servers, applications, and stored data.

You can use Junos Pulse Access Control Service and the switches for a centralized end-to-end NAC system. The Access Control Service eliminates the need to configure firewall filters on each switch. Instead, you define resource access policies centrally on the NAC device. For more information, read this topic.

Understanding Centralized Network Access Control and EX Series Switches

Network access control (NAC) allows you to control who is admitted to the network and what resources—servers, applications, and stored data—those users are allowed to access. These controls include:

- Authentication—Pre-admission controls
- Authorization—Post-admission controls

You can use different methods to implement NAC on Juniper Networks EX Series Ethernet Switches.

This topic describes:

NAC Using Any RADIUS Server and Access Polices Defined on the Local Switch

For pre-admission controls, you can use the switch in combination with any RADIUS server as the *authentication server*. For additional information, see "Understanding Authentication on Switches" on page 268.

For post-admission controls, you can configure firewall filters to limit access to specific resources. For additional information, see *Firewall Filters for EX Series Switches Overview*.

Centralized NAC Using Junos Pulse Access Control Service

You can use Junos Pulse Access Control Service and the switches for a centralized end-to-end NAC system, including both pre-admission *authentication* and post-admission *authorization*.

When you configure such a system, the Juniper Networks MAG Series Junos Pulse Gateways or the Juniper Networks IC Series Unified Access Control Appliances NAC device functions as the authentication server. For messages relating to IEEE 802.1X and MAC RADIUS authentication, the NAC device communicates with the switch using the RADIUS protocol.

The Access Control Service also performs additional functions. It eliminates the need to configure firewall filters on each switch. Instead, you define resource access policies centrally on the NAC device. This centralized method is particularly helpful when you have multiple switches in your network.

The resource access policy on the Access Control Service defines which network resources are allowed and denied for a user, based upon the user's role. The NAC device distributes these policies to all connected switches. The NAC device thus functions as a centralized policy management server. For messages relating to access policies, the NAC device communicates with the switch using the Junos UAC Enforcer Protocol (JUEP). The switch converts the resource access policies into filter definitions and applies these to the appropriate port.

NOTE: With this solution, the EX Series switch serves as an *Infranet Enforcer*, that is, a policy enforcement point for the Access Control Service. The Access Control Service sends auth table entries and resource access policies when an endpoint successfully completes 802.1X authentication or MAC authentication (unmanaged devices). Access for any endpoint is governed by the resource access policies that you configure on the Access Control Service. Because resource access policies are employed, firewall filters are not required for the switch configuration.

This integrated solution of Access Control Service and EX Series switches is easier to implement and much more efficient than previous versions of Access Control Service and the switches. As soon the switch connects to the MAG Series or IC Series NAC device, the Access Control Service pushes the role-based policies to the switch via JUEP. This enables the user to access the network more quickly than previous implementations, because the policy is already available on the switch and does not need to be pushed from the centralized device at the time of user authentication. Moreover, the policy push happens only once, which utilizes network bandwidth efficiently and makes this implementation suitable for scaled environments.

If you change policies, the Access Control Service automatically pushes the updated policies to the connected switch. The switch applies the policies dynamically without taking users through another authentication transaction.

NOTE: Do not configure firewall filters on the switch and do not use RADIUS server attributes for firewall filters if you are configuring the switch to use the Access Control Service. Instead, specify or deny access to resources by using the Access Control Service resource access policies.

You create policies on the NAC device's administrative interface to control access to resources and services. Access is based on successful authentication, the user's assigned role, and the security compliance of the endpoint device. For example, you can provide full access to protected resources employee role and limited access for a contractor role.

Captive Portal Authentication

Captive portal authentication allows you to authenticate users on the switches by redirecting Web browser requests to a login page that requires users to input a username and password before they are allowed access to the network. The details of configuring captive portal authentication differ depending on whether you are using the Access Control Service:

- If you have connected the switch to the Access Control Service, use the Access Control Service NAC device as an external captive portal server for redirecting Web browser requests. When users try to access a protected network resource that is connected to the switch, the user must first sign in to the Access Control Service for authentication and endpoint security checking. The captive portal redirects the user to a login page located on the Access Control Service. When the sign-in page for the Access Control Service is displayed, the user signs in and the Access Control Service examines the endpoint for compliance with security policies. If the endpoint passes the security check, access is granted to the protected resource.

  See "Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure)" on page 404. You can use the same Access Control Service as the external captive portal server for more than one switch.

- If you are not using the Access Control Service, you can use captive portal to redirect users to a login page that you configure on the local switch. See "Designing a Captive Portal Authentication Login Page on Switches" on page 380 for information about designing a login page on your switch.

Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)

You can connect the switch to Junos Pulse Access Control Service to set up a centralized, end-to-end network access control (NAC) system, which allows you to control who is admitted to the network and what resources those users are allowed to access.

The Access Control Service functions both as an *authentication server* (RADIUS server) and as a *centralized policy management server*.

Before you begin configuring the switch to connect to the Access Control Service:

- Configure a resource access policy.

- Obtain the password of the Access Control Service.
- Obtain the IP address of the Access Control Service.

NOTE: Specify the same IP address for the authentication server, the RADIUS server, and the infranet controller (NAC device). These components refer to the same Access Control Service.

To configure the switch to work with the Access Control Service:

1. Configure the switch to use the Access Control Service for authentication and authorization:

   ```
   [edit ethernet-switching-options]
   user@switch# set uac-policy
   ```

2. Configure the access profile to specify the Access Control Service. The access profile contains the authentication and authorization configuration that aids in handling authentication and authorization requests, including the authentication method and sequence, and the Access Control Service address:

   a. Configure **radius** as the authentication method to be used when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches:

      ```
      [edit access profile]
      user@switch# set profile-name authentication-order radius
      ```

   b. Specify the IP address of the authentication server:

      NOTE: Specify the same IP address that you use for the RADIUS server and the NAC device.

      ```
      [edit access profile]
      user@switch# set profile-name radius authentication-server ip-address
      ```

3. Configure the RADIUS server to use the same IP address that you specified for the authentication server:

   ```
   [edit access]
   user@switch# set radius-server ip-address
   ```

4. Configure the password to use for connecting the switch with the RADIUS server:

   NOTE: The password specified here is used for RADIUS communications between the switch and the Access Control Service. It does not need to match the password that is specified on the Access Control Service through the administrative interface on the Access Control Service.

```
[edit access]
user@switch# set radius-server secret password
```

5. Configure the address of the Access Control Service MAG Series or the IC Series NAC device:

NOTE: Specify the hostname and IP address of the NAC device. This is the same IP address that you used for specifying the authentication server.

```
[edit services united-access-control infranet-controller hostname]
user@switch# set address ip-address
```

6. Configure the switch's management Ethernet interface for the NAC device:

```
[edit services united-access-control infranet-controller hostname]
user@switch# set interface me0.0
```

7. Configure the password for connecting the switch to the Access Control Service NAC device:

NOTE: This password must match the password specified on the Access Control Service though its administrative interface. It is used for Junos UAC Enforcer Protocol (JUEP) communications between the switch and the Access Control Service.

```
[edit services united-access-control infranet-controller hostname]
user@switch# set password password
```

8. Configure the amount of time that switch waits to receive a response from the Access Control Service:

```
[edit services united-access-control]
user@switch# set timeout seconds
```

9. Specify the time between continuity-check messages for the switch's connection with the Access Control Service:

```
[edit services united-access-control]
user@switch# set interval seconds
```

10. Specify an action for the switch to take if a timeout occurs for the connection between the switch and the Access Control Service:

```
[edit services united-access-control]
user@switch# set timeout-action action
```

11. Specify the name of the access profile to use for 802.1X, MAC RADIUS, or captive portal authentication:

NOTE: Use the same access profile that you configured previously (step 2).

```
[edit protocols dot1x]
user@switch# set authenticator authentication-profile-name profile-name
```

12. Configure the 802.1X interface that the switch will use for communicating with the Access Control Service:

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name
```

Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure)

If you have connected the EX Series switch to the Junos Pulse Access Control Service and you want to use the captive portal user authentication feature, configure the Access Control Service network access control (NAC) device as an external captive portal server. The captive portal feature is required only for user authentication. Unmanaged devices, such as printers or phones, can be authenticated through 802.1X and MAC address authentication.

When users try to access a protected network resource that is connected to the switch, the user must first sign in to the Access Control Service for authentication and endpoint security checking. The captive portal redirects the user to a login page located on the Access Control Service.

When the sign-in page for the Access Control Service is displayed, the user signs in and the Access Control Service examines the endpoint for compliance with security policies. If the endpoint passes the security check, access is granted to the protected resource.

Before you begin, be sure you have:

- Configured access between the switch and the Access Control Service. See "Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)" on page 401.
- Designed your captive portal login page on the Access Control Service.

To configure the switch to use the Access Control Service for captive portal:

1. Configure captive portal to authenticate clients connected to the switch for access to use the authentication profile that directs the client to the Access Control Service:

NOTE: The access profile name specified here must match the access profile name that you specified for the Access Control Service in "Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)" on page 401.

```
[edit]
user@switch# set services captive-portal authentication-profile-name access-profile-name
```

2. Enable an interface for use with captive portal authentication:

```
[edit]
user@switch# set services captive-portal interface interface-name supplicant multiple
```

3. (Optional) Specify which clients are to bypass captive portal authentication:

```
[edit]
user@switch# set ethernet-switching-options authentication-whitelist mac-address
```

NOTE: You can use set ethernet-switching-options authentication-whitelist *mac-address* interface *interface-name* to limit the scope to the interface.

NOTE: If the client is already attached to the switch, you must clear its MAC address from captive portal authentication by using the clear captive-portal mac-address *mac-address* command after adding its MAC address to the authentication whitelist. Otherwise the new entry for the MAC address will not be added to the Ethernet switching table and the authentication bypass will not be allowed.

Related Documentation

- Central Web Authentication on page 393
- Captive Portal Authentication on page 373

VoIP on EX Series Switches

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. When you use VoIP, you can connect IP telephones to the switch and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. For more information, read this topic.

- Understanding 802.1X and VoIP on EX Series Switches on page 406
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 416
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 421
- Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication on page 426
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support on page 433

Understanding 802.1X and VoIP on EX Series Switches

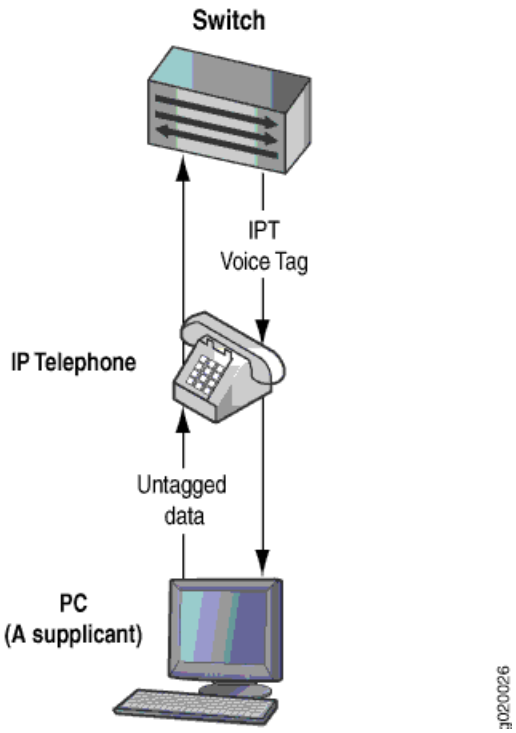
When you use VoIP, you can connect IP telephones to the switch and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. The 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.

VoIP is a protocol used for the transmission of voice through packet-switched networks. VoIP transmits voice calls by using a network connection instead of an analog phone line.

When VoIP is used with 802.1X, the RADIUS server authenticates the phone, and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) provides the class-of-service (CoS) parameters to the phone.

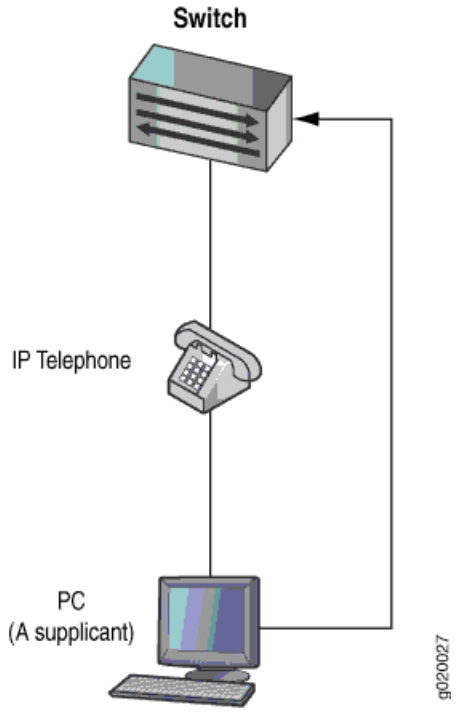
You can configure 802.1X authentication to work with VoIP in multiple supplicant or single supplicant mode. In *multiple supplicant* mode, the 802.1X process allows multiple supplicants to connect to the interface. Each supplicant is authenticated individually. For an example of a VoIP multiple supplicant topology, see Figure 21 on page 406.

Figure 21: VoIP Multiple Supplicant Topology



If an 802.1X-compatible IP telephone does not have an 802.1X host but has another 802.1X-compatible device connected to its data port, you can connect the phone to an interface in single supplicant mode. In *single supplicant* mode, the 802.1X process authenticates only the first supplicant. All other supplicants who connect later to the interface are allowed full access without any further authentication. They effectively "piggyback" on the first supplicant's authentication. For an example of a VoIP single supplicant topology, see Figure 22 on page 407 .

Figure 22: VoIP Single Supplicant Topology



If an IP telephone does not support 802.1X, you can configure VoIP to bypass 802.1X and LLDP-MED and have the packets forwarded to a VoIP VLAN.

Multi Domain 802.1X Authentication

Multi-domain 802.1X authentication is an extension of multiple supplicant mode that allows one default VoIP device and multiple data devices to authenticate on a single port. Multi-domain 802.1X authentication provides enhanced security over multiple supplicant mode by restricting the number of authenticated data and VoIP sessions on the port. In multiple supplicant mode, any number of VoIP or data sessions can be authenticated; the number of sessions can be restricted using MAC limiting, but there is no way to apply the limit specifically to either data or VoIP sessions.

With multi-domain 802.1X authentication, the single port is divided into two domains; one is the data domain and the other is the voice domain. Multi-domain 802.1X authentication maintains separate session counts based on the domain. You can configure the maximum number of authenticated data sessions allowed on the port. The number of VoIP sessions is not configurable; only one authenticated VoIP session is allowed on the port.

If a new client attempts to authenticate on the interface after the maximum session count has been reached, the default action is to drop the packet and generate an error log message. You can also configure the action to shut down the interface. The port can be manually recovered from the down state by issuing the **clear dot1x recovery-timeout** command, or by can recover automatically after a configured recovery timeout period.

Multi-domain authentication does not enforce the order of device authentication. However, for the best results, the VoIP device should be authenticated before a data device on a multi domain 802.1X-enabled port. Multi-domain authentication is supported only in multiple supplicant mode.

See Also
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol forwards VoIP parameters from the switch to the phone. You also configure 802.1X authentication to allow the telephone access to the LAN. Authentication is done through a backend RADIUS server.

This example describes how to configure VoIP on an EX Series switch to support an Avaya IP phone, as well as the LLDP-MED protocol and 802.1X authentication:

NOTE: If your switch runs Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, see "Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support" on page 433. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An Avaya 9620 IP telephone that supports LLDP-MED and 802.1X

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See *Installing and Connecting an EX3200 Switch*.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (J-Web Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

- Configured the RADIUS server for 802.1X authentication and set up the access profile. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.
- (Optional) Configured interface **ge-0/0/2** for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see *Configuring PoE on EX Series Switches (CLI Procedure)*.

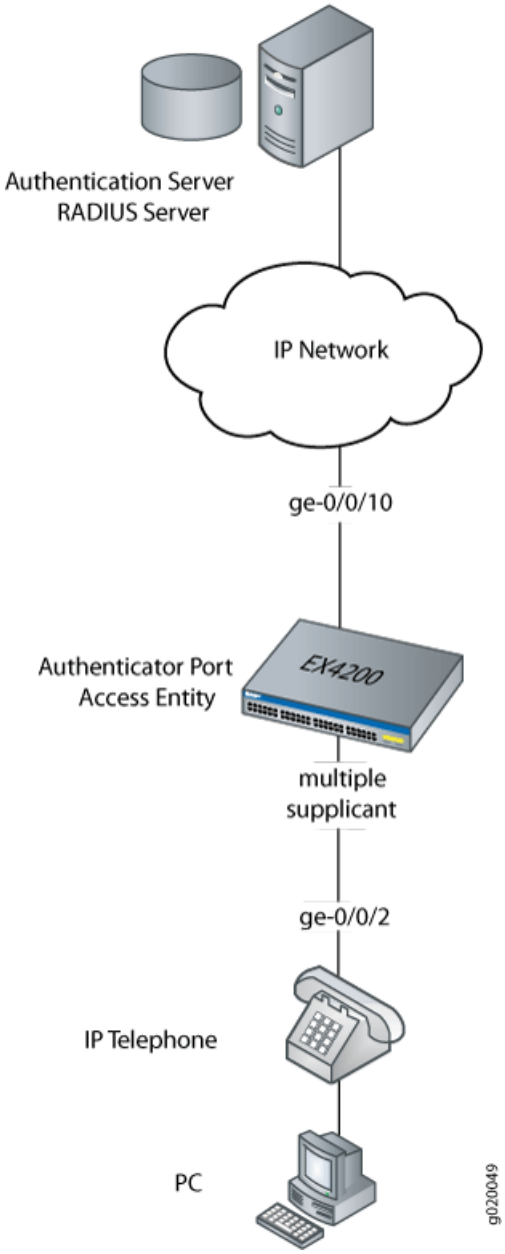
NOTE: If the IP address isn't configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the **voip** statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN's ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).

Overview and Topology

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

In this example, the access interface **ge-0/0/2** on the EX4200 switch is connected to an Avaya 9620 IP telephone. Avaya phones have a built-in bridge that allows you to connect a desktop PC to the phone, so the desktop and phone in a single office require only one interface on the switch. The EX Series switch is connected to a RADIUS server on interface **ge-0/0/10** (see Figure 23 on page 410).

Figure 23: VoIP Topology



In this example, you configure VoIP parameters and specify the forwarding class **assured-forward** for voice traffic to provide the highest quality of service.

Table 31 on page 410 describes the components used in this VoIP configuration example.

Table 31: Components of the VoIP Configuration Topology

Property	Settings
Switch hardware	EX4200 switch

Table 31: Components of the VoIP Configuration Topology (continued)

Property	Settings
VLAN names	**data-vlan** **voice-vlan**
Connection to Avaya phone—with integrated hub, to connect phone and desktop PC to a single interface (requires PoE)	**ge-0/0/2**
One RADIUS server	Provides backend database connected to the switch through interface **ge-0/0/10**.

As well as configuring a VoIP for interface **ge-0/0/2**, you configure:

- 802.1X authentication. Authentication is set to **multiple** supplicant to support more than one supplicant's access to the LAN through interface **ge-0/0/2**.
- LLDP-MED protocol information. The switch uses LLDP-MED to forward VoIP parameters to the phone. Using LLDP-MED ensures that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p class of service and 802.1Q tag information can be sent to the IP telephone.

NOTE: A PoE configuration is not necessary if an IP telephone is using a power adapter.

Configuration

To configure VoIP, LLDP-MED, and 802.1X authentication:

CLI Quick Configuration

To quickly configure VoIP, LLDP-MED, and 802.1X, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set ethernet-switching-options voip interface ge-0/0/2.0 vlan voice-vlan
set ethernet-switching-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2.0
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Step-by-Step Procedure

To configure VoIP with LLDP-MED and 802.1X:

1. Configure the VLANs for voice and data:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

2. Associate the VLAN **data-vlan** with the interface:

```
[edit vlans]
user@switch# set data-vlan interface ge-0/0/2.0
```

3. Configure the interface as an access interface, configure support for Ethernet switching, and add the **data-vlan** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode access
```

4. Configure VoIP on the interface and specify the **assured-forwarding** forwarding class to provide the most dependable class of service:

```
[edit ethernet-switching-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

5. Configure LLDP-MED protocol support:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/2.0
```

6. To authenticate an IP phone and a PC connected to the IP phone on the interface, configure 802.1X authentication support and specify **multiple** supplicant mode:

NOTE: If you do not want to authenticate any device, skip the 802.1X configuration on this interface.

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Results

Display the results of the configuration:

```
[edit]
user@switch# show configuration
interfaces {
   ge-0/0/2 {
      unit 0 {
         family ethernet-switching {
            port-mode access;
```

```
            vlan {
              members data-vlan;
            }
          }
        }
      }
    }
protocols {
    lldp-med {
      interface ge-0/0/2.0;
    }
    dot1x {
      authenticator {
        interface {
          ge-0/0/2.0 {
            supplicant multiple;
          }
        }
      }
    }
}
vlans {
    data-vlan {
      vlan-id 77;
      interface {
        ge-0/0/2.0;
      }
    }
    voice-vlan {
      vlan-id 99;
    }
}
ethernet-switching options {
    voip {
      interface ge-0/0/2.0 {
        vlan voice-vlan;
        forwarding-class assured-forwarding;
      }
    }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying LLDP-MED Configuration on page 413
- Verifying 802.1X Authentication for IP Phone and Desktop PC on page 414
- Verifying the VLAN Association with the Interface on page 415

Verifying LLDP-MED Configuration

Purpose Verify that LLDP-MED is enabled on the interface.

Action

```
user@switch> show lldp detail
LLDP                     : Enabled
Advertisement interval   : 30 Second(s)
Transmit delay           : 2 Second(s)
Hold timer               : 2 Second(s)
Config Trap Interval     : 300 Second(s)
Connection Hold timer    : 60 Second(s)

LLDP MED                 : Enabled
MED fast start count     : 3 Packet(s)


Interface      LLDP       LLDP-MED    Neighbor count
all            Enabled    -           0
ge-0/0/2.0     -          Enabled     0

Interface     VLAN-id     VLAN-name
ge-0/0/0.0    0           default
ge-0/0/1.0    0           employee-vlan
ge-0/0/2.0    0           data-vlan
ge-0/0/2.0    99          voice-vlan
ge-0/0/3.0    0           employee-vlan
ge-0/0/8.0    0           employee-vlan
ge-0/0/10.0   0           default
ge-0/0/11.0   20          employee-vlan
ge-0/0/23.0   0           default

LLDP basic TLVs supported:
Chassis identifier, Port identifier, Port description, System name, System
description, System capabilities, Management address.

LLDP 802 TLVs supported:
Power via MDI, Link aggregation, Maximum frame size, Port VLAN tag, Port
VLAN name.

LLDP MED TLVs supported:
LLDP MED capabilities, Network policy, Endpoint location, Extended power
Via MDI.
```

Meaning The **show lldp detail** output shows that both LLDP and LLDP-MED are configured on the **ge-0/0/2.0** interface. The end of the output shows the list of supported LLDP basic TLVs, 802.3 TLVs, and LLDP-MED TLVs that are supported.

Verifying 802.1X Authentication for IP Phone and Desktop PC

Purpose Display the 802.1X configuration to confirm that the VoIP interface has access to the LAN.

Action

```
user@switch> show dot1x interface ge/0/0/2.0 detail
ge-0/0/2.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning The field **Role** shows that the **ge-0/0/2.0** interface is in the authenticator state. The **Supplicant** field shows that the interface is configured in multiple supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

Verifying the VLAN Association with the Interface

Purpose Display the interface state and VLAN membership.

Action

```
user@switch> show ethernet-switching interfaces
 Ethernet-switching table: 0 entries, 0 learned

user@switch> show ethernet-switching interfaces
Interface   State    VLAN members           Blocking
ge-0/0/0.0  down     default                unblocked
ge-0/0/1.0  down     employee-vlan          unblocked
ge-0/0/5.0  down     employee-vlan          unblocked
ge-0/0/3.0  down     employee-vlan          unblocked
ge-0/0/8.0  down     employee-vlan          unblocked
ge-0/0/10.0 down     default                unblocked
ge-0/0/11.0 down     employee-vlan          unblocked
ge-0/0/23.0 down     default                unblocked
ge-0/0/2.0  up       voice-vlan             unblocked
                     data-vlan              unblocked
```

Meaning The field **VLAN members** shows that the **ge-0/0/2.0** interface supports both the **data-vlan** VLAN and **voice-vlan** VLAN. The **State** field shows that the interface is up.

See Also

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- *Defining CoS Forwarding Classes (CLI Procedure)*
- *Defining CoS Forwarding Classes (J-Web Procedure)*
- Configuring LLDP-MED (CLI Procedure) on page 521

Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol is sometimes used with IP phones to forward VoIP parameters from the switch to the phone. However, not all IP phones support LLDP-MED.

This example describes how to configure VoIP on an EX Series switch without using LLDP-MED:

Requirements

This example uses the following hardware and software components:

- One EX Series switch with support for ELS acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An IP phone that does not support LLDP-MED.
- Junos OS Release 13.2X50 or later for EX Series switches.

Before you configure VoIP, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* .
- Configured the IP phone as a member of the voice VLAN.
- (Optional) Configured interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. See *Configuring PoE on EX Series Switches (CLI Procedure)*.

Overview

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You can also power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

EX Series switches can accommodate an IP telephone and end host connected to a single switch port. In such a scenario, voice and data traffic must be separated into different broadcast domains, or VLANs. One method for accomplishing this is by configuring a voice VLAN, which enables access ports to accept untagged data traffic as well as tagged voice traffic from IP phones, and associate each type of traffic with separate and distinct VLANs. Voice traffic (tagged) can then be treated differently, generally with a higher priority than data traffic (untagged).

The voice VLAN delivers the greatest benefit when used with IP phones that support LLDP-MED, but it is flexible enough that IP phones that do not support LLDP-MED can also use it effectively. However, in the absence of LLDP-MED, the voice VLAN ID must be set manually on the IP phone because LLDP-MED is not available to accomplish this dynamically. For information about setting up a voice VLAN for IP phones that support LLDP-MED, see "Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support" on page 433.

Another method to separate voice (tagged) and data (untagged) traffic into different VLANs is to use a trunk port with the native VLAN ID option. The trunk port is added as a member of the voice VLAN, and processes only tagged voice traffic from that VLAN. The trunk port must also be configured with the native VLAN ID for the data VLAN so that it can process untagged data traffic from the data VLAN. This configuration also requires that the voice VLAN ID be set manually on the IP phone.

This example illustrates both methods. In this example, the interface ge-0/0/2 on the switch is connected to a non-LLDP-MED IP phone.

NOTE: The implementation of a voice VLAN on an IP telephone is vendor-specific. Consult the documentation that came with your IP telephone for instructions on configuring a voice VLAN. For example, on an Avaya phone, you can ensure that the phone gets the correct VoIP VLAN ID even in the absence of LLDP-MED by enabling DHCP option 176.

Configuring VoIP Without LLDP-MED by Using a Voice VLAN on an Access Port

CLI Quick Configuration

To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan switch-options interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set switch-options voip interface ge-0/0/2.0 vlan voice-vlan
set switch-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

Step-by-Step Procedure

1. Configure two VLANs: one for data traffic and one for voice traffic:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

NOTE: The voice VLAN ID must be set manually on the IP phone.

2. Associate the VLAN **data-vlan** with the interface ge-0/0/2:

```
[edit vlans]
user@switch# set data-vlan switch-options interface ge-0/0/2.0
```

3. Configure the interface ge-0/0/2 as an access port belonging to the data VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode access
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan member data-vlan
```

4. Configure VoIP on the interface ge-0/0/2 and add this interface to the voice VLAN:

```
[edit switch-options]
```

```
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
```

5. Specify the assured-forwarding forwarding class to provide the most dependable class of service:

```
[edit switch-options]
user@switch#  set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

Results Display the results of the configuration:

```
[edit]
user@switch> show configuration
interfaces {
   ge-0/0/2 {
      unit 0 {
         family ethernet-switching {
            port-mode access;
            vlan {
               members data-vlan;
            }
         }
      }
   }
}
vlans {
   data-vlan {
      vlan-id 77;
      interface {
         ge-0/0/2.0;
      }
   }
   voice-vlan {
      vlan-id 99;
   }
}
ethernet-switching options {
   voip {
      interface ge-0/0/2.0 {
         vlan voice-vlan;
         forwarding-class assured-forwarding;
      }
   }
}
```

Configuring VoIP Without LLDP-MED by Using a Trunk Port with Native VLAN Option

CLI Quick Configuration To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
```

```
set vlans voice-vlan vlan-id 99
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members voice-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan
```

Step-by-Step Procedure

1. Configure two VLANs: one for data traffic and one for voice traffic:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

NOTE: The voice VLAN ID must be set manually on the IP phone.

2. Configure interface ge-0/0/2 as a trunk port that includes only the voice VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode trunk
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan member voice-vlan
```

3. Configure the native VLAN ID for the data VLAN on the trunk port:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan
```

Results Display the results of the configuration:

```
[edit]
user@switch> show configuration
interfaces {
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members voice-vlan;
                }
                native-vlan-id data-vlan;
            }
        }
    }
}
vlans {
    data-vlan {
        vlan-id 77;
    }
    voice-vlan {
        vlan-id 99;
    }
}
```

Verification

To confirm that the configuration is working properly, perform the following task:

- Verifying the VLAN Association With the Interface on page 421

Verifying the VLAN Association With the Interface

Purpose Display the interface state and VLAN membership.

Action

```
user@switch> show ethernet-switching interfaces
Ethernet-switching table: 0 entries, 0 learned

user@switch> show ethernet-switching interfaces
Interface   State    VLAN members           Blocking
ge-0/0/0.0  down     default                unblocked
ge-0/0/1.0  down     employee-vlan          unblocked
ge-0/0/5.0  down     employee-vlan          unblocked
ge-0/0/3.0  down     employee-vlan          unblocked
ge-0/0/8.0  down     employee-vlan          unblocked
ge-0/0/10.0 down     default                unblocked
ge-0/0/11.0 down     employee-vlan          unblocked
ge-0/0/23.0 down     default                unblocked
ge-0/0/2.0  up       voice-vlan             unblocked
                     data-vlan              unblocked
```

Meaning The field **VLAN members** shows that the ge-0/0/2.0 interface supports both the data VLAN, data-vlan, and the voice VLAN, voice-vlan. The **State** field shows that the interface is up.

See Also

- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol is sometimes used with IP phones to forward VoIP parameters from the switch to the phone. However, not all IP phones support LLDP-MED.

This example describes how to configure VoIP on an EX Series switch without using LLDP-MED:

- Requirements on page 422
- Overview on page 422
- Configuring VoIP Without LLDP-MED by Using a Voice VLAN on an Access Port on page 423

Requirements

This example uses the following hardware and software components:

- One EX4200 switch acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An IP phone that does not support LLDP-MED.
- Junos OS Release 9.1 or later for EX Series switches.

Before you configure VoIP, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.
- Configured the IP phone as a member of the voice VLAN.
- (Optional) Configured interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. See *Configuring PoE on EX Series Switches (CLI Procedure)*.

Overview

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You can also power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

EX Series switches can accommodate an IP telephone and end host connected to a single switch port. In such a scenario, voice and data traffic must be separated into different broadcast domains, or VLANs. One method for accomplishing this is by configuring a voice VLAN, which enables access ports to accept untagged data traffic as well as tagged voice traffic from IP phones, and associate each type of traffic with separate and distinct VLANs. Voice traffic (tagged) can then be treated differently, generally with a higher priority than data traffic (untagged).

The voice VLAN delivers the greatest benefit when used with IP phones that support LLDP-MED, but it is flexible enough that IP phones that do not support LLDP-MED can also use it effectively. However, in the absence of LLDP-MED, the voice VLAN ID must be set manually on the IP phone because LLDP-MED is not available to accomplish this dynamically. For information about setting up a voice VLAN for IP phones that support LLDP-MED, see "Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch" on page 408.

Another method to separate voice (tagged) and data (untagged) traffic into different VLANs is to use a trunk port with the native VLAN ID option. The trunk port is added as a member of the voice VLAN, and processes only tagged voice traffic from that VLAN.

The trunk port must also be configured with the native VLAN ID for the data VLAN so that it can process untagged data traffic from the data VLAN. This configuration also requires that the voice VLAN ID be set manually on the IP phone.

This example illustrates both methods. In this example, the interface ge-0/0/2 on the EX4200 switch is connected to a non-LLDP-MED IP phone.

NOTE: The implementation of a voice VLAN on an IP telephone is vendor-specific. Consult the documentation that came with your IP telephone for instructions on configuring a voice VLAN. For example, on an Avaya phone, you can ensure that the phone gets the correct VoIP VLAN ID even in the absence of LLDP-MED by enabling DHCP option 176.

Configuring VoIP Without LLDP-MED by Using a Voice VLAN on an Access Port

CLI Quick Configuration

To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set ethernet-switching-options voip interface ge-0/0/2.0 vlan voice-vlan
```

Step-by-Step Procedure

1. Configure two VLANs: one for data traffic and one for voice traffic:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

NOTE: The voice VLAN ID must be set manually on the IP phone.

2. Configure the VLAN **data-vlan** on the interface ge-0/0/2:

```
[edit vlans]
user@switch# set data-vlan interface ge-0/0/2.0
```

3. Configure the interface ge-0/0/2 as an access port belonging to the data VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode access
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan member data-vlan
```

4. Configure VoIP on the interface ge-0/0/2 and add this interface to the voice VLAN:

```
[edit ethernet-switching-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
```

Results Display the results of the configuration:

```
[edit]
user@switch> show configuration
interfaces {
   ge-0/0/2 {
      unit 0 {
         family ethernet-switching {
            port-mode access;
            vlan {
               members data-vlan;
            }
         }
      }
   }
}
vlans {
   data-vlan {
      vlan-id 77;
      interface {
         ge-0/0/2.0;
      }
   }
   voice-vlan {
      vlan-id 99;
   }
}
ethernet-switching options {
   voip {
      interface ge-0/0/2.0 {
         vlan voice-vlan;
      }
   }
}
```

Configuring VoIP Without LLDP-MED by Using a Trunk Port with Native VLAN Option

CLI Quick Configuration To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members voice-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan
```

Step-by-Step Procedure

1. Configure two VLANs: one for data traffic and one for voice traffic:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

NOTE: The voice VLAN ID must be set manually on the IP phone.

2. Configure interface ge-0/0/2 as a trunk port that includes only the voice VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode trunk
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan member voice-vlan
```

3. Configure the native VLAN ID for the data VLAN on the trunk port:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan
```

Results Display the results of the configuration:

```
[edit]
user@switch> show configuration
interfaces {
   ge-0/0/2 {
      unit 0 {
         family ethernet-switching {
            port-mode trunk;
            vlan {
               members voice-vlan;
            }
            native-vlan-id data-vlan;
         }
      }
   }
}
vlans {
   data-vlan {
      vlan-id 77;
   }
   voice-vlan {
      vlan-id 99;
   }
}
```

Verification

To confirm that the configuration is working properly, perform the following task:

- Verifying the VLAN Association With the Interface on page 426

Verifying the VLAN Association With the Interface

Purpose Display the interface state and VLAN membership.

Action

```
user@switch>  show ethernet-switching interfaces
 Ethernet-switching table: 0 entries, 0 learned

user@switch> show ethernet-switching interfaces
Interface   State    VLAN members           Blocking
ge-0/0/0.0  down     default                unblocked
ge-0/0/1.0  down     employee-vlan          unblocked
ge-0/0/5.0  down     employee-vlan          unblocked
ge-0/0/3.0  down     employee-vlan          unblocked
ge-0/0/8.0  down     employee-vlan          unblocked
ge-0/0/10.0 down     default                unblocked
ge-0/0/11.0 down     employee-vlan          unblocked
ge-0/0/23.0 down     default                unblocked
ge-0/0/2.0  up       voice-vlan             unblocked
                     data-vlan              unblocked
```

Meaning The field **VLAN members** shows that the ge-0/0/2.0 interface supports both the data VLAN, data-vlan, and the voice VLAN, voice-vlan. The **State** field shows that the interface is up.

See Also

- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones.

To configure VoIP on an EX Series switch to support an IP phone that does not support 802.1X authentication, you must either add the MAC address of the phone to the static MAC bypass list or enable MAC RADIUS authentication on the switch.

This example describes how to configure VoIP on an EX Series switch without 802.1X authentication using static MAC bypass of authentication:

- Requirements on page 427
- Overview on page 427
- Configuration on page 428
- Verification on page 430

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches
- An IP telephone

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See the installation information for your switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.
- Configured the RADIUS server for 802.1X authentication and set up the access profile. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.
- (Optional) Configured interface **ge-0/0/2** for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see *Configuring PoE on EX Series Switches (CLI Procedure)*.

NOTE: If the IP address isn't configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the voip statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN's ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).

Overview

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

In this example, the access interface **ge-0/0/2** on the EX4200 switch is connected to a non-802.1X IP phone.

To configure VoIP on an EX Series switch to support an IP phone that does not support 802.1X authentication, add the MAC address of the phone as a static entry in the authenticator database and set the supplicant mode to multiple.

Configuration

To configure VoIP without 802.1X authentication:

CLI Quick Configuration

To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set ethernet-switching-options voip interface ge-0/0/2.0 vlan voice-vlan
set ethernet-switching-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2.0
set protocols dot1x authenticator authentication-profile-name auth-profile
set protocols dot1x authenticator static 00:04:f2:11:aa:a7
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Step-by-Step Procedure

To configure VoIP without 802.1X:

1. Configure the VLANs for voice and data:

   ```
   [edit vlans]
   user@switch# set data-vlan vlan-id 77
   user@switch# set voice-vlan vlan-id 99
   ```

2. Associate the VLAN **data-vlan** with the interface:

   ```
   [edit vlans]
   user@switch# set data-vlan interface ge-0/0/2.0
   ```

3. Configure the interface as an access interface, configure support for Ethernet switching, and add the **data-vlan** VLAN:

   ```
   [edit interfaces]
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode access
   ```

4. Configure VoIP on the interface and specify the **assured-forwarding** forwarding class to provide the most dependable class of service:

   ```
   [edit ethernet-switching-options]
   user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
   user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
   ```

5. Configure LLDP-MED protocol support:

   ```
   [edit protocols]
   user@switch# set lldp-med interface ge-0/0/2.0
   ```

6. Set the authentication profile (see "Configuring 802.1X Interface Settings (CLI Procedure)" on page 292 and "Configuring 802.1X RADIUS Accounting (CLI Procedure)" on page 335):

```
[edit protocols]
set dot1x authenticator authentication-profile-name auth-profile
```

7. Add the MAC address of the phone to the static MAC bypass list:

```
[edit protocols]
set dot1x authenticator static 00:04:f2:11:aa:a7
```

8. Set the supplicant mode to multiple:

```
[edit protocols]
set dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Results Display the results of the configuration:

```
[edit]
user@switch# show configuration
interfaces {
  ge-0/0/2 {
    unit 0 {
      family ethernet-switching {
        port-mode access;
        vlan {
          members data-vlan;
        }
      }
    }
  }
}
protocols {
  lldp-med {
    interface ge-0/0/2.0;
  }
  dot1x {
    authenticator {
      authentication-profile-name auth-profile;
        static {
          00:04:f2:11:aa:a7;
        }
      }
      interface {
        ge-0/0/2.0 {
          supplicant multiple;
        }
    }
  }
}
vlans {
  data-vlan {
```

```
      vlan-id 77;
      interface {
        ge-0/0/2.0;
      }
    }
    voice-vlan {
      vlan-id 99;
    }
  }
  ethernet-switching options {
    voip {
      interface ge-0/0/2.0 {
        vlan voice-vlan;
        forwarding-class assured-forwarding;
      }
    }
  }
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying LLDP-MED Configuration on page 430
- Verifying Authentication for the Desktop PC on page 431
- Verifying the VLAN Association with the Interface on page 432

Verifying LLDP-MED Configuration

Purpose Verify that LLDP-MED is enabled on the interface.

Action

```
user@switch> show lldp detail
LLDP                     : Enabled
Advertisement interval   : 30 Second(s)
Transmit delay           : 2 Second(s)
Hold timer               : 2 Second(s)
Config Trap Interval     : 300 Second(s)
Connection Hold timer    : 60 Second(s)

LLDP MED                 : Enabled
MED fast start count     : 3 Packet(s)


Interface      LLDP       LLDP-MED    Neighbor count
all            Enabled    -           0
ge-0/0/2.0     -          Enabled     0

Interface     VLAN-id     VLAN-name
ge-0/0/0.0    0           default
ge-0/0/1.0    0           employee-vlan
ge-0/0/2.0    0           data-vlan
ge-0/0/2.0    99          voice-vlan
ge-0/0/3.0    0           employee-vlan
ge-0/0/8.0    0           employee-vlan
ge-0/0/10.0   0           default
ge-0/0/11.0   20          employee-vlan
ge-0/0/23.0   0           default

LLDP basic TLVs supported:
Chassis identifier, Port identifier, Port description, System name, System
description, System capabilities, Management address.

LLDP 802 TLVs supported:
Power via MDI, Link aggregation, Maximum frame size, Port VLAN tag, Port
VLAN name.

LLDP MED TLVs supported:
LLDP MED capabilities, Network policy, Endpoint location, Extended power
Via MDI.
```

Meaning The **show lldp detail** output shows that both LLDP and LLDP-MED are configured on the **ge-0/0/2.0** interface. The end of the output shows the list of supported LLDP basic TLVs, 802.3 TLVs, and LLDP-MED TLVs that are supported.

Verifying Authentication for the Desktop PC

Purpose Display the 802.1X configuration for the desktop PC connected to the VoIP interface through the IP phone.

Action `user@switch>` show dot1x **interface ge/0/0/2.0 detail**

```
ge-0/0/2.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning The field **Role** shows that the **ge-0/0/2.0** interface is in the authenticator state. The **Supplicant** field shows that the interface is configured in multiple supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

Verifying the VLAN Association with the Interface

Purpose Display the interface state and VLAN membership.

Action

```
user@switch> show ethernet-switching interfaces
 Ethernet-switching table: 0 entries, 0 learned

user@switch> show ethernet-switching interfaces
Interface   State    VLAN members           Blocking
ge-0/0/0.0  down     default                unblocked
ge-0/0/1.0  down     employee-vlan          unblocked
ge-0/0/5.0  down     employee-vlan          unblocked
ge-0/0/3.0  down     employee-vlan          unblocked
ge-0/0/8.0  down     employee-vlan          unblocked
ge-0/0/10.0 down     default                unblocked
ge-0/0/11.0 down     employee-vlan          unblocked
ge-0/0/23.0 down     default                unblocked
ge-0/0/2.0  up       voice-vlan             unblocked
                     data-vlan              unblocked
```

Meaning The field **VLAN members** shows that the **ge-0/0/2.0** interface supports both the **data-vlan** VLAN and **voice-vlan** VLAN. The **State** field shows that the interface is up.

See Also

- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch" on page 408. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

You can configure VoIP on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol forwards VoIP parameters from the switch to the phone. You also configure 802.1X authentication to allow the telephone access to the LAN. Authentication is done through a backend RADIUS server.

This example describes how to configure VoIP on an EX Series switch to support an Avaya IP phone, as well as how to configure the LLDP-MED protocol and 802.1X authentication:

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 13.2X50 or later for EX Series switches
- One EX Series switch with support for ELS acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An Avaya IP telephone that supports LLDP-MED and 802.1X

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See the installation information for your switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*.
- Configured the RADIUS server for 802.1X authentication and set up the access profile. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 302.
- (Optional) Configured the interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant uses a power adapter. For information about configuring PoE, see *Configuring PoE on EX Series Switches (CLI Procedure)*.

NOTE: If the IP address is not configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the **voip** statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN's ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).

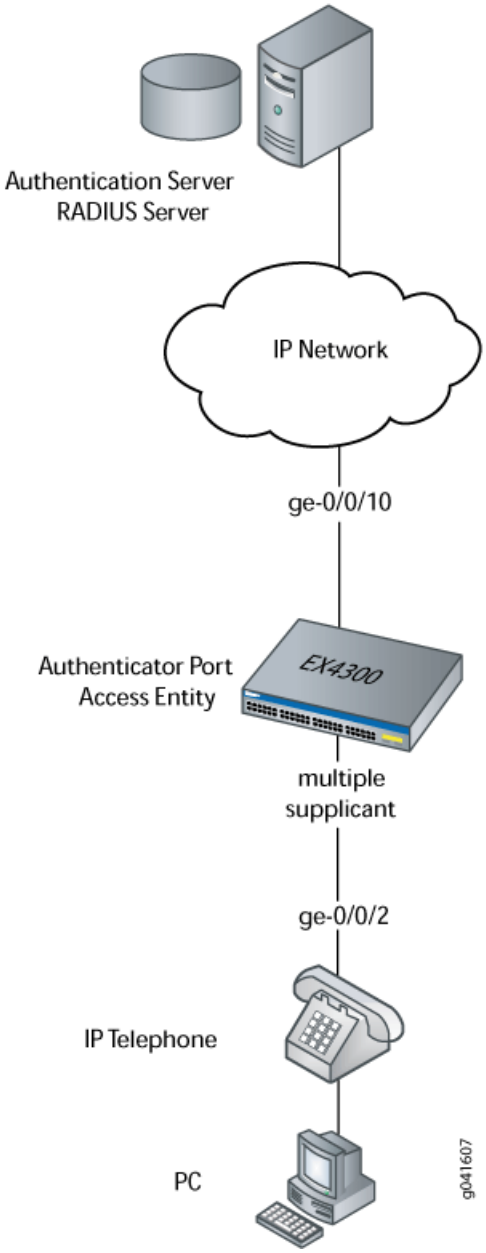
Overview and Topology

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

In this example, the access interface ge-0/0/2 on the EX Series switch is connected to an Avaya IP telephone. Avaya phones have a built-in bridge that enables you to connect a desktop PC to the phone, so the desktop and phone in a single office require only one interface on the switch. The EX Series switch is connected to a RADIUS server on the ge-0/0/10 interface (see Figure 24 on page 435).

NOTE: This figure also applies to QFX5100 switches.

Figure 24: VoIP Topology



In this example, you configure VoIP parameters and specify the forwarding class **assured-forward** for voice traffic to provide the highest quality of service.

Table 32 on page 436 describes the components used in this VoIP configuration example.

Table 32: Components of the VoIP Configuration Topology

Property	Settings
Switch hardware	EX Series switch with support for ELS.
VLAN names and IDs	data-vlan, 77 voice-vlan, 99
Connection to Avaya phone—with integrated hub, to connect phone and desktop PC to a single interface (requires PoE)	ge-0/0/2
One RADIUS server	Provides backend database connected to the switch through interface ge-0/0/10.

Besides configuring a VoIP for interface ge-0/0/2, you configure:

- 802.1X authentication. Authentication is set to **multiple** supplicant mode to support more than one supplicant's access to the LAN through interface ge-0/0/2.
- LLDP-MED protocol information. The switch uses LLDP-MED to forward VoIP parameters to the phone. Using LLDP-MED ensures that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p class of service and 802.1Q tag information can be sent to the IP telephone.

NOTE: A PoE configuration is not necessary if an IP telephone uses a power adapter.

Configuration

CLI Quick Configuration

To quickly configure VoIP, LLDP-MED, and 802.1X, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan switch-options interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set switch-options voip interface ge-0/0/2.0 vlan voice-vlan
set switch-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Step-by-Step Procedure

To configure VoIP with LLDP-MED and 802.1X:

1. Configure the VLANs for voice and data:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

2. Associate the VLAN **data-vlan** with the interface:

```
[edit vlans]
user@switch# set data-vlan switch-options interface ge-0/0/2.0
```

3. Configure the interface as an access interface, configure support for Ethernet switching, and add the interface as a member of the **data-vlan** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching interface-mode access
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
```

4. Configure VoIP on the interface and specify the **assured-forwarding** forwarding class to provide the most dependable class of service:

```
[edit switch–options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

5. Configure LLDP-MED protocol support:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/2
```

6. To authenticate an IP phone and a PC connected to the IP phone on the interface, configure 802.1X authentication support and specify **multiple** supplicant mode:

NOTE: If you do not want to authenticate any device, skip the 802.1X configuration on this interface.

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Results

Display the results of the configuration:

```
[edit]
user@switch# show configuration
interfaces {
   ge-0/0/2 {
      unit 0 {
         family ethernet-switching {
            interface-mode access;
```

```
            vlan {
              members data-vlan;
            }
          }
        }
      }
    }
protocols {
    lldp-med {
      interface ge-0/0/2;
    }
    dot1x {
      authenticator {
        interface {
          ge-0/0/2.0 {
            supplicant multiple;
          }
        }
      }
    }
}
vlans {
    data-vlan {
      vlan-id 77;
      switch-options {
        interface ge-0/0/2.0;
      }
    }
    voice-vlan {
      vlan-id 99;
    }
}
switch-options {
    voip {
      interface ge-0/0/2.0 {
        vlan voice-vlan;
        forwarding-class assured-forwarding;
      }
    }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying LLDP-MED Configuration on page 438
- Verifying 802.1X Authentication for IP Phone and Desktop PC on page 439
- Verifying the VLAN Association with the Interface on page 440

Verifying LLDP-MED Configuration

Purpose Verify that LLDP-MED is enabled on the interface.

Action

```
user@switch> show lldp detail
LLDP                     : Enabled
Advertisement interval   : 30 seconds
Transmit delay           : 2 seconds
Hold timer               : 120 seconds
Notification interval    : 0 Second(s)
Config Trap Interval     : 0 seconds
Connection Hold timer    : 300 seconds

LLDP MED                 : Enabled
MED fast start count     : 3 Packets

Port ID TLV subtype      : locally-assigned

Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
  Neighbor count
all            -                   Enabled     Enabled      Enabled
  0
ge-0/0/2       -                   -           Enabled      -
  0

Interface      Parent Interface    Vlan-id     Vlan-name
ge-0/0/0       -                   1           vlan-1
ge-0/0/1       -                   1           vlan-1
ge-0/0/2       -                   77          vlan-77
ge-0/0/2       -                   99          vlan-99
ge-0/0/3       -                   1           vlan-1
ge-0/0/4       -                   1           vlan-1
ge-0/0/5       -                   1           vlan-1
ge-0/0/6       -                   1           vlan-1
ge-0/0/7       -                   1           vlan-1
ge-0/0/8       -                   1           vlan-1
ge-0/0/9       -                   1           vlan-1
ge-0/0/10      -                   1           vlan-1

Basic Management TLVs supported:
End Of LLDPDU, Chassis ID, Port ID, Time To Live, Port Description, System Name,

 System Description, System Capabilities, Management Address

Organizationally Specific TLVs supported:
MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum Frame Size,

 Port VLAN tag, Port VLAN name.
```

Meaning The **show lldp detail** output shows that both **LLDP** and **LLDP-MED** are configured on the **ge-0/0/2** interface. The end of the output shows the list of supported LLDP basic management TLVs and organizationally specific TLVs that are supported.

Verifying 802.1X Authentication for IP Phone and Desktop PC

Purpose Display the 802.1X configuration to confirm that the VoIP interface has access to the LAN.

Action

```
user@switch> show dot1x interface ge/0/0/2.0 detail
ge-0/0/2.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning The field **Role** shows that the **ge-0/0/2.0** interface is in the authenticator state. The **Supplicant mode** field shows that the interface is configured in **multiple** supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

Verifying the VLAN Association with the Interface

Purpose Display the interface's VLAN membership.

Action

```
user@switch> show ethernet-switching interface ge-0/0/2.0
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members           limit    state        interface flags
ge-0/0/2.0                     65535                                 untagged
             voice-vlan 99
                               65535    Discarding
             data-vlan  77
                               65535    Discarding
```

Meaning The field **VLAN members** shows that the **ge-0/0/2.0** interface supports both the **data-vlan** VLAN and **voice-vlan** VLAN.

See Also

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- *Defining CoS Forwarding Classes (CLI Procedure)*
- *Defining CoS Forwarding Classes (J-Web Procedure)*
- Configuring LLDP-MED (CLI Procedure) on page 521

Related Documentation

- RADIUS Server Configuration for Authentication on page 282
- 802.1X Authentication on page 289

CHAPTER 7

Configuring IEEE 802.1x Port-Based Network Access Control

IEEE 802.1x Port-Based Network Access Control Overview

MX Series routers support the IEEE 802.1x Port-Based Network Access Control (dot1x) protocol on Ethernet interfaces for validation of client and user credentials to prevent unauthorized access to a specified router port. Before authentication is complete, only 802.1x control packets are allowed and forwarded to the router control plane for processing. All other packets are dropped.

Authentication methods used must be 802.1x compliant. Authentication using RADIUS and Microsoft Active Directory servers is supported. The following user/client authentication methods are allowed:

- EAP-MD5 (RFC 3748)
- EAP-TTLS requires a server certificate (RFC 2716)
- EAP-TLS requires a client and server certificate
- PEAP requires only a server certificate

You can use both client and server certificates in all types of authentication except EAP-MD5.

NOTE: On the MX Series router, 802.1x can be enabled on bridged ports only and not on routed ports.

Dynamic changes to a user session are supported to allow the router administrator to terminate an already authenticated session by using the “RADIUS disconnect” message defined in RFC 3576.

Related Documentation

- Understanding the Administrative State of the Authenticator Port on page 444
- Understanding the Administrative Mode of the Authenticator Port on page 444
- Configuring the Authenticator on page 445
- Viewing the dot1x Configuration on page 445
- *Ethernet Interfaces Feature Guide for Routing Devices*

Understanding the Administrative State of the Authenticator Port

The administrative state of an authenticator port can take any of the following three states:

- Force authorized—Allows network access to all users of the port without requiring them to be authenticated. This is equivalent to not having any authentication enabled on the port.
- Force unauthorized—Denies network access to all users of the port. This is equivalent to disabling the port.
- Automatic—This is the default mode where the authentication server response determines if the port is opened for traffic or not. Only the successfully authenticated clients are allowed access, all others are denied.

In Junos OS, the default mode is “automatic.” The “force authorized” and “force unauthorized” admin modes are not supported. You can achieve the functionality of “force authorized” mode by disabling **dot1x** on the required port. You can achieve the functionality of “force unauthorized” mode by disabling the port itself.

Related Documentation

- IEEE 802.1x Port-Based Network Access Control Overview on page 443
- Understanding the Administrative Mode of the Authenticator Port on page 444
- Configuring the Authenticator on page 445
- Viewing the dot1x Configuration on page 445
- *Ethernet Interfaces Feature Guide for Routing Devices*

Understanding the Administrative Mode of the Authenticator Port

Junos OS supports the supplicant mode “single” and not the “single secure” nor “multiple” modes. The “Single” mode option authenticates only the first client that connects to a port. All other clients that connect later (802.1x compliant or noncompliant) are allowed free access on that port without any further authentication. If the first authenticated client logs out, all other users are locked out until a client authenticates again.

Related Documentation

- IEEE 802.1x Port-Based Network Access Control Overview on page 443
- Understanding the Administrative State of the Authenticator Port on page 444
- Configuring the Authenticator on page 445
- Viewing the dot1x Configuration on page 445
- *Ethernet Interfaces Feature Guide for Routing Devices*

Configuring the Authenticator

To configure the IEEE 802.1x Port-Based Network Access Control protocol on Ethernet interfaces you must configure the **authenticator** statement at the **[edit protocols dot1x]** hierarchy level. Use the **authentication-profile-name** *access-profile-name* statement to specify the authenticating RADIUS server, and use the **interface** statement to specify and configure the Gigabit Ethernet or Fast Ethernet interface on the router specifically for IEEE 802.1x protocol use; both at the **[edit protocols dot1x authenticator]** hierarchy level.

```
[edit protocols dot1x]
authenticator {
   authentication-profile-name access-profile-name;
   interface (xe-fpc/pic/port | ge-fpc/pic/port | fe-fpc/pic/port) {
      maximum-requests seconds;
      quiet-period seconds;
      reauthentication (disable | interval seconds);
      retries integer;
      server-timeout seconds;
      supplicant (single);
      supplicant-timeout seconds;
      transmit-period seconds;
   }
}
```

Related Documentation

- IEEE 802.1x Port-Based Network Access Control Overview on page 443
- Understanding the Administrative State of the Authenticator Port on page 444
- Understanding the Administrative Mode of the Authenticator Port on page 444
- Viewing the dot1x Configuration on page 445
- *Ethernet Interfaces Feature Guide for Routing Devices*

Viewing the dot1x Configuration

Purpose To review and verify the dot1x configuration.

Action To view all **dot1x** configurations, use the **show dot1x interface** operational mode command. To view a **dot1x** configuration for a specific interface, use the **show dot1x interface (xe-*fpc/pic/port* | ge-*fpc/pic/port* | fe-*fpc/pic/port*) detail** operational mode command.

See the *Network Interfaces Command Reference* for more information about this command.

Related Documentation

- IEEE 802.1x Port-Based Network Access Control Overview on page 443
- Understanding the Administrative State of the Authenticator Port on page 444
- Understanding the Administrative Mode of the Authenticator Port on page 444
- Configuring the Authenticator on page 445
- *Ethernet Interfaces Feature Guide for Routing Devices*

CHAPTER 8

Configuring IEEE 802.1x Port-Based Network Access Control in Enhanced LAN Mode

802.1X for MX Series Routers in Enhanced LAN Mode Overview

Starting with Junos os Release 14.2, IEEE 802.1X provides network edge security, protecting Ethernet LANs from unauthorized user access. Support is implemented for controlling access to your network through an MX Series router by using several different authentication methods, such as 802.1X, MAC RADIUS, or a captive portal.

This functionality is supported on the following MPCs on MX240, MX480, and MX960 routers in enhanced LAN mode:

- MPC4E with two 100-Gigabit Ethernet ports and eight 10-Gigabit Ethernet ports
- MPC4E with thirty-two 10-Gigabit Ethernet ports
- MPC3E that contains a 2-port 40-Gigabit Ethernet MIC with QSFP+
- MPC1E with forty 1-Gigabit Ethernet ports or twenty 1-Gigabit Ethernet ports

You must reboot the router when you configure or delete the enhanced LAN mode on the router. Configuring the **network-services lan** option implies that the system is running in the enhanced IP mode. When you configure a device to function in MX-LAN mode, only the supported configuration statements and operational show commands that are available for enabling or viewing in this mode are displayed in the CLI interface. If your system contains parameters that are not supported in MX-LAN mode in a configuration file, you cannot commit those unsupported attributes. You must remove the settings that are not supported and then commit the configuration. After the successful CLI commit, a system reboot is required for the attributes to be come effective. Similarly, if you remove the **network-services lan** statement, the system does not run in MX-LAN mode. Therefore, all of the settings that are supported outside of the MX-LAN mode are displayed and are available for definition in the CLI interface. If your configuration file contains settings that are supported only in MX-LAN mode, you must remove those attributes before you commit the configuration. After the successful CLI commit, a system reboot will be required for the CLI settings to take effect. The Layer 2 Next-Generation CLI configuration settings are supported in MX-LAN mode. As a result, the typical MX Series-format of CLI configurations might differ in MX-LAN mode.

This functionality is supported on an MX Series Virtual Chassis combination that functions in enhanced LAN mode (by entering the **network-services lan** statement at the **[edit chassis]** hierarchy level). Port-based network access control is supported on MX240, MX480, and MX960 routers with MPCs in both the MX-LAN mode and the non-MX-LAN mode (with other supported network services modes on MPCs on these routers). To configure the IEEE 802.1x port-based network access control (PNAC) protocol on Ethernet interfaces, you must configure the **authenticator** statement at the **[edit protocols authentication-access- control]** hierarchy level. You can also configure captive portal authentication on a router so that users connected to the switch are authenticated before being allowed to access the network. You can also configure Junos Pulse Access Control Service as the access policy to authenticate and authorize users connected to the switch for admission to the network and for access to protected network resources by using the **uac-policy** statement.

How 802.1X Authentication Works

802.1X authentication works by using an *Authenticator Port Access Entity* (the switch) to block all traffic to and from a supplicant (end device) at the port until the supplicant's credentials are presented and matched on the *Authentication server* (a RADIUS server). When authenticated, the switch stops blocking traffic and opens the port to the supplicant.

The end device is authenticated in either *single* mode, *single-secure* mode, or *multiple* mode:

- **single**—Authenticates only the first end device. All other end devices that connect later to the port are allowed full access without any further authentication. They effectively "piggyback" on the end devices' authentication.
- **single-secure**—Allows only one end device to connect to the port. No other end device is allowed to connect until the first logs out.
- **multiple**—Allows multiple end devices to connect to the port. Each end device will be authenticated individually.

Network access can be further defined using VLANs and firewall filters, which both act as filters to separate and match groups of end devices to the areas of the LAN they require. For example, you can configure VLANs to handle different categories of authentication failures depending upon:

- Whether or not the end device is 802.1X-enabled.
- Whether or not MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected.
- Whether the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message. See "Configuring RADIUS Server Fail Fallback (CLI Procedure)" on page 287.

802.1X Features Overview

NOTE: **The 802.1X features available on the MX Series routers depend upon which switch you are using.**

802.1X features on Juniper Networks MX Series routers are:

- Guest VLAN—Provides limited access to a LAN, typically just to the Internet, for nonresponsive end devices that are not 802.1X-enabled when MAC RADIUS authentication has not been configured on the switch interfaces to which the hosts are connected . Also, a guest VLAN can be used to provide limited access to a LAN for guest users. Typically, the guest VLAN provides access just to the Internet and to other guests' end devices.
- Server-reject VLAN—Provides limited access to a LAN, typically just to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials.
- Server-fail VLAN—Provides limited access to a LAN, typically just to the Internet, for 802.1X end devices during a RADIUS server timeout.

- Dynamic VLAN—Enables an end device, after authentication, to be a member of a VLAN dynamically.
- Private VLAN—Enables configuration of 802.1X authentication on interfaces that are members of private VLANs (PVLANs).
- Dynamic changes to a user session—Allows the switch administrator to terminate an already authenticated session. This feature is based on support of the RADIUS Disconnect Message defined in RFC 3576.
- RADIUS accounting—Sends accounting information to the RADIUS accounting server. Accounting information is sent to the server whenever a subscriber logs in or logs out and whenever a subscriber activates or deactivates a subscription.

Supported Features Related to 802.1X Authentication

802.1X does not replace other security technologies. 802.1X works together with port security features, such as DHCP snooping, dynamic ARP inspection (DAI), and MAC limiting, to guard against spoofing.

Supported features related to authentication include:

- Static MAC bypass—Provides a bypass mechanism to authenticate devices that are not 802.1X-enabled (such as printers). Static MAC bypass connects these devices to 802.1X-enabled ports, bypassing 802.1X authentication.
- MAC RADIUS authentication—Provides a means to enable or disable MAC authentication independently of whether 802.1X authentication is enabled.

Release History Table

Release	Description
14.2	Starting with Junos os Release 14.2, IEEE 802.1X provides network edge security, protecting Ethernet LANs from unauthorized user access. Support is implemented for controlling access to your network through an MX Series router by using several different authentication methods, such as 802.1X, MAC RADIUS, or a captive portal.

Understanding 802.1X and LLDP and LLDP-MED on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, Juniper Networks MX Series routers use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information allows the router to quickly identify a variety of devices, resulting in a LAN that interoperates smoothly and efficiently.

LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include information such as chassis and port identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in the Juniper Networks Junos operating system (Junos OS).

LLDP-MED goes one step further than LLDP, exchanging IP-telephony messages between the router and the IP telephone.

LLDP and LLDP-MED also provide PoE power management capabilities. LLDP power negotiation allows the router to manage PoE power by negotiating with LLDP-enabled powered devices to dynamically allocate PoE power as needed. LLDP power priority allows an LLDP-enabled powered device to set the PoE power priority on the router interface to which it connects.

The router also uses these protocols to ensure that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p CoS and 802.1Q tag information can be sent to the IP telephone.

EX Series routeres support the following basic TLVs:

- **Chassis Identifier**—The MAC address associated with the local system.

  NOTE: The Chassis ID TLV has a subtype for Network Address Family. LLDP frames are validated only if this subtype has a value of 1 (IPv4) or 2 (IPv6). For any other value, the transmitting device is detected by LLDP as a neighbor and displayed in the output of the "show lldp neighbors" command, but is not assigned to the VLAN.

- **Port Identifier**—The port identification for the specified port in the local system.
- **Port Description**—Textual description of the interface or the logical unit. The description for the logical unit is used, if available; otherwise, the Port Description TLV will contain the description configured on the physical interface. For example, LAG member interfaces do not contain a logical unit, so only the description configured on the physical interface can be used.
- **System Name**—The user-configured name of the local system. The system name can be a maximum of 256 characters.
- **System Description**—The system description containing information about the software and current image running on the system. This information is not configurable, but taken from the software.
- **System Capabilities**—The primary function performed by the system. The capabilities that system supports; for example, bridge or router. This information is not configurable, but based on the model of the product.
- **Management Address**—The IPv4 or IPv6 management address of the local system.

EX Series routeres support the following 802.3 TLVs:

- **Power via MDI**—A TLV that advertises MDI power support, PSE power pair, and power class information.
- **MAC/PHY Configuration Status**—A TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information is not configurable, but based on the physical interface structure.

NOTE: The MAC/PHY Configuration Status TLV has a subtype for the PMD Auto-Negotiation Advertised Capability field. This field will contain a value of other or unknown if the LLDP packet was transmitted from a 10-gigabit SFP+ port.

- **Link Aggregation**—A TLV that advertises if the port is aggregated and its aggregated port ID.
- **Maximum Frame Size**—A TLV that advertises the Maximum Transmission Unit (MTU) of the interface sending LLDP frames.
- **Port Vlan**—A TLV that advertises the VLAN name configured on the interface.

EX Series routeres support the following LLDP-MED TLVs:

- **LLDP MED Capabilities**—A TLV that advertises the primary function of the port. The capabilities values range 0 through 15:
  - **0**— Capabilities
  - **1**— Network Policy
  - **2**— Location Identification
  - **3**— Extended Power via MDI-PSE
  - **4**— Inventory
  - **5–15**— Reserved
- LLDP-MED Device Class Values:
  - **0**— Class not defined.
  - **1**— Class 1 Device.
  - **2**— Class 2 Device.
  - **3**— Class 3 Device.
  - **4**— Network Connectivity Device
  - **5–255**— Reserved.
- **Network Policy**—A TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types, such as voice or streaming video, 802.1Q VLAN tagging, and 802.1p priority bits and Diffserv code points.
- **Endpoint Location**— A TLV that advertises the physical location of the endpoint.
- **Extended Power via MDI**— A TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, Juniper Networks MX Series routers use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information allows the router to quickly identify a variety of devices, resulting in a LAN that interoperates smoothly and efficiently.

Understanding 802.1X and RADIUS Accounting on MX Series Routers in Enhanced LAN Mode

Juniper Networks MX Series routers support IETF RFC 2866, *RADIUS Accounting*. Starting with Junos OS Release 14.2, you can configure RADIUS accounting on an MX Series router which enables statistical data about users logging onto or off a LAN to be collected and sent to a RADIUS accounting server. The statistical data gathered can be used for general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

To configure RADIUS accounting, specify one or more RADIUS accounting servers to receive the statistical data from the switch, and select the type of accounting data to be collected.

The RADIUS accounting server you specify can be the same server used for RADIUS authentication, or it can be a separate RADIUS server. You can specify a list of RADIUS accounting servers. In the event that the primary server (the first one configured) is unavailable, each RADIUS server in the list is tried in the order in which they are configured in the Juniper Networks Junos operating system (Junos OS).

The RADIUS accounting process between a switch and a RADIUS server works like this:

1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. For example, on FreeRADIUS, the default port is 1813.

2. The switch forwards an *accounting-request* packet containing an event record to the accounting server. For example, a supplicant is authenticated through 802.1X authentication and connected to the LAN. The event record associated with this supplicant contains an *Acct-Status-Type* attribute whose value indicates the beginning of user service for this supplicant. When the supplicant's session ends, the accounting request will contain an *Acct-Status-Type* attribute value indicating the end of user service. The RADIUS accounting server records this as a stop-accounting record containing session information and the length of the session.

3. The RADIUS accounting server logs these events as start-accounting or stop-accounting records. The records are in a file. On FreeRADIUS, the file name is the server's address; for example, 122.69.1.250.

4. The accounting server sends an *accounting-response* packet back to the switch confirming it has received the accounting request.

5. If the switch does not receive a response from the server, it continues to send accounting requests until an accounting response is returned from the accounting server.

The statistics collected through this process can be displayed from the RADIUS server; to see those statistics, the user accesses the log file configured to receive them.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, you can configure RADIUS accounting on an MX Series router which enables statistical data about users logging onto or off a LAN to be collected and sent to a RADIUS accounting server. The statistical data gathered can be used for general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

Understanding 802.1X and VoIP on MX Series Routers in Enhanced LAN Mode

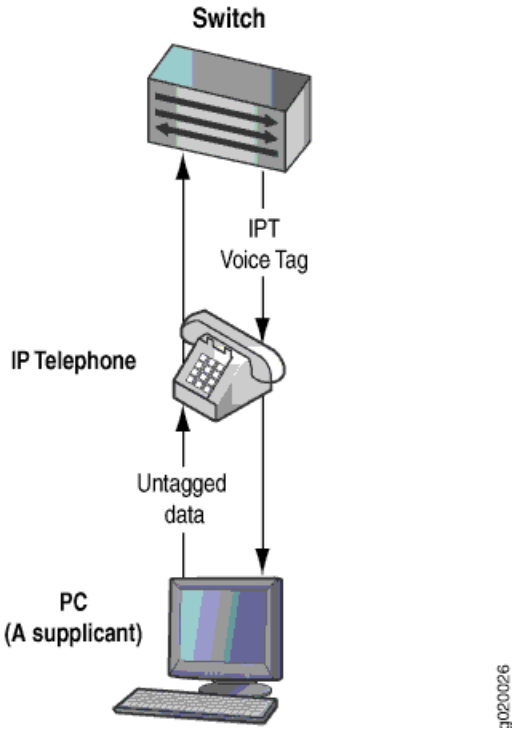
When you use Voice over IP (VoIP), you can connect IP telephones to the router and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. Starting with Junos OS Release 14.2, 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.

VoIP is a protocol used for the transmission of voice through packet-switched networks. VoIP transmits voice calls using a network connection instead of an analog phone line.

When VoIP is used with 802.1X, the RADIUS server authenticates the phone, and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) provides the class-of-service (CoS) parameters to the phone.

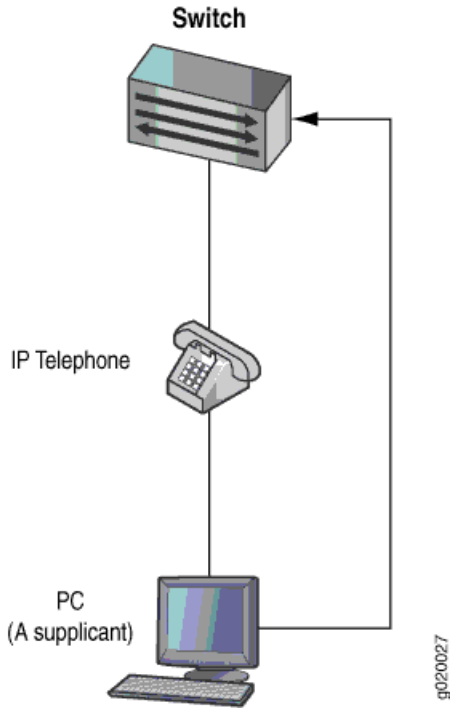
You can configure 802.1X authentication to work with VoIP in multiple supplicant or single supplicant mode. In *multiple-supplicant* mode, the 802.1X process allows multiple supplicants to connect to the interface. Each supplicant will be authenticated individually. For an example of a VoIP multiple supplicant topology, see Figure 21 on page 406.

Figure 25: VoIP Multiple Supplicant Topology



If an 802.1X-compatible IP telephone does not have an 802.1X host but has another 802.1X-compatible device connected to its data port, you can connect the phone to an interface in single-supplicant mode. In *single-supplicant* mode, the 802.1X process authenticates only the first supplicant. All other supplicants who connect later to the interface are allowed full access without any further authentication. They effectively "piggyback" on the first supplicant's authentication. For an example of a VoIP single supplicant topology, see Figure 22 on page 407 .

Figure 26: VoIP Single Supplicant Topology



If an IP telephone does not support 802.1X, you can configure VoIP to bypass 802.1X and LLDP-MED and have the packets forwarded to a VoIP VLAN,

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.

Understanding Guest VLANs for 802.1X on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, guest VLANs can be configured on switches that are using 802.1X authentication to provide limited access—typically only to the Internet—for:

- Corporate guests
- End devices that are not 802.1X-enabled
- Nonresponsive end devices when MAC RADIUS authentication has not been configured on the switch interfaces to which the hosts are connected

A guest VLAN is not used for supplicants sending incorrect credentials. Those supplicants are directed to the server-reject VLAN instead.

For end devices that are not 802.1X-enabled, a guest VLAN can allow limited access to a server from which the non-802.1X-enabled end device can download the supplicant software and attempt authentication again.

A guest VLAN is not used when MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected. Some end devices, such as a printer, cannot be enabled for 802.1X. The hosts for such devices should be connected to switch interfaces that are configured for MAC RADIUS authentication.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, guest VLANs can be configured on switches that are using 802.1X authentication to provide limited access—typically only to the Internet

Understanding Dynamic VLANs for 802.1X on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, dynamic VLANs, in conjunction with the 802.1X authentication process, provide secure access to the LAN for end devices belonging to different VLANs on a single port.

When this feature is configured on the RADIUS server, an end device or user authenticating on the RADIUS server is assigned to the VLAN configured for it. The end device or user becomes a member of a VLAN dynamically after successful 802.1X authentication. For information on configuring dynamic VLANs on your RADIUS server, see the documentation for your RADIUS server.

Successful authentication requires that the VLAN ID or VLAN name exist on the router and match the VLAN ID or VLAN name sent by the RADIUS server during authentication. If neither exists, the end device is unauthenticated. If a guest VLAN is established, the unauthenticated end device is automatically moved to the guest VLAN.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, dynamic VLANs, in conjunction with the 802.1X authentication process, provide secure access to the LAN for end devices belonging to different VLANs on a single port.

Understanding Server Fail Fallback and Authentication on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, server fail fallback allows you to specify how end devices connected to the router are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

Juniper Networks MX Series routers in enhanced LAN mode use authentication to implement access control in an enterprise network. If 802.1X, MAC RADIUS, or captive portal authentication are configured on the interface, end devices are evaluated at the initial connection by an authentication (RADIUS) server. If the end device is configured on the authentication server, the device is granted access to the LAN and the MX Series router opens the interface to permit access.

A RADIUS server timeout occurs if no RADIUS authentication servers are reachable when an end device logs in and attempts to access the LAN. Server fail fallback allows you to specify one of four actions to be taken toward end devices awaiting authentication when the server is timed out:

- *Permit* authentication, allowing traffic to flow from the end device through the interface as if the end device were successfully authenticated by the RADIUS server.
- *Deny* authentication, preventing traffic from flowing from the end device through the interface. This is the default.
- *Move* the end device to a specified VLAN. (The VLAN must already exist on the router.)
- *Sustain* authenticated end devices that already have LAN access and *deny* unauthenticated end devices. If the RADIUS servers time out during reauthentication, previously authenticated end devices are reauthenticated and new users are denied LAN access.

Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by an end device's first attempt at authentication through the RADIUS server.

Server fail fallback allows you to specify that an end device be moved to a specified VLAN if the router receives a RADIUS access-reject message. The configured VLAN name overrides any attributes sent by the server.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, server fail fallback allows you to specify how end devices connected to the router are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

Configuring 802.1X RADIUS Accounting on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, RADIUS accounting permits statistical data about users logging onto or off a LAN to be collected and sent to a RADIUS accounting server.The statistical data gathered can be used for general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

To configure basic RADIUS accounting using the CLI:

1. Specify the accounting servers to which the switch will forward accounting statistics:

```
[edit access ]
user@router# set profile profile1 radius accounting-serveraccounting-server [122.69.1.250
122.69.1.252]
```

2. Define the RADIUS accounting servers:

```
[edit access]
user@router# set radius-server 122.69.1.250 secret juniper
user@router# set radius-server 122.69.1.252 secret juniper1
```

3. Enable accounting for an access profile:

```
[edit access]
user@router# set profile profile1 accounting
```

4. Configure the RADIUS servers to use while sending accounting messages and updates:

```
[edit access]
user@router# set profile profile1 accounting order radius
```

5. Configure the statistics to be collected on the router and forwarded to the accounting server:

```
[edit access ]
user@router# set profile profile1 accounting accounting-stop-on-access-deny
user@router# set profile profile1 accounting accounting-stop-on-failure
```

6. Display accounting statistics collected on the router:

```
user@router> show network-access aaa statistics accounting
Accounting module statistics
  Requests received: 1
  Accounting Response failures: 0
```

```
Accounting Response Success: 1
Requests timedout: 0
```

7. Open an accounting log on the RADIUS accounting server using the server's address, and view accounting statistics:

```
[root@freeradius]# cd /usr/local/var/log/radius/radacct/122.69.1.250
[root@freeradius 122.69.1.250]# ls

detail-20071214

[root@freeradius 122.69.1.250]# vi details-20071214

        User-Name = "000347e1bab9"
        NAS-Port = 67
        Acct-Status-Type = Stop
        Acct-Session-Id = "802.1x811912"
        Acct-Input-Octets = 17454
        Acct-Output-Octets = 4245
        Acct-Session-Time = 1221041249
        Acct-Input-Packets = 72
        Acct-Output-Packets = 53
        Acct-Terminate-Cause = Lost-Carrier
        Acct-Input-Gigawords = 0
        Acct-Output-Gigawords = 0
        Called-Station-Id = "00-19-e2-50-52-60"
        Calling-Station-Id = "00-03-47-e1-ba-b9"
        Event-Timestamp = "Sep 10 2008 16:52:39 PDT"
        NAS-Identifier = "esp48t-1b-01"
        NAS-Port-Type = Virtual

        User-Name = "000347e1bab9"
        NAS-Port = 67
        Acct-Status-Type = Start
        Acct-Session-Id = "802.1x811219"
        Called-Station-Id = "00-19-e2-50-52-60"
        Calling-Station-Id = "00-03-47-e1-ba-b9"
        Event-Timestamp = "Sep 10 2008 18:58:52 PDT"
        NAS-Identifier = "esp48t-1b-01"
        NAS-Port-Type = Virtual
```

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, RADIUS accounting permits statistical data about users logging onto or off a LAN to be collected and sent to a RADIUS accounting server.

Related Documentation

Configuring 802.1X Interface Settings on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, IEEE 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the *authentication server* (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

NOTE:

- You can also specify an 802.1X exclusion list to specify supplicants can that can bypass authentication and be automatically connected to the LAN.
- You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.
- You cannot configure 802.1X user authentication on redundant trunk groups (RTGs).

Before you begin, specify the RADIUS server or servers to be used as the authentication server.

To configure 802.1X on an interface:

1. Configure the supplicant mode as **single** (authenticates the first supplicant), **single-secure** (authenticates only one supplicant), or **multiple** (authenticates multiple supplicants):

   ```
   [edit protocols authentication-access-control]
   user@switch# set interface ge-0/0/5 supplicant multiple
   ```

2. Enable reauthentication and specify the reauthentication interval:

   ```
   [edit protocols authentication-access-control]
   user@switch# set interface ge-0/0/5/0 dot1x reauthentication interval 5
   ```

3. Configure the interface timeout value for the response from the supplicant:

   ```
   [edit protocols authentication-access-control]
   user@switch# set interface ge-0/0/5 dot1x supplicant-timeout 5
   ```

4. Configure the timeout for the interface before it resends an authentication request to the RADIUS server:

   ```
   [edit protocols authentication-access-control]
   user@switch# set interface ge-0/0/5 server-timeout 5
   ```

5. Configure how long, in seconds, the interface waits before retransmitting the initial EAPOL PDUs to the supplicant:

```
[edit protocols authentication-access-control]
user@switch# set interface ge-0/0/5 dot1x transmit-period 60
```

6. Configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out:

```
[edit protocols authentication-access-control]
user@switch# set interface ge-0/0/5 dot1x maximum-requests 5
```

7. Configure the number of times the switch attempts to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt.

```
[edit protocols authentication-access-control]
user@switch# set interface ge-0/0/5 retries 1
```

NOTE: This setting specifies the number of tries before the switch puts the interface in a “HELD” state.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, IEEE 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the *authentication server* (a RADIUS server).

Related Documentation

Configuring LLDP-MED on MX Series Routers in Enhanced LAN Mode

Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) is an extension of LLDP. Starting with Junos OS Release 14.2, the router uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations.

LLDP-MED is turned on by default on MX Series routers.

This topic describes:

- Enabling LLDP-MED on Interfaces on page 464
- Configuring Location Information Advertised by the Router on page 464
- Configuring for Fast Start on page 464

Enabling LLDP-MED on Interfaces

LLDP-MED is enabled on all interfaces by default. If it is disabled, you can enable LLDP-MED by configuring it on all interfaces or on specific interfaces.

To configure LLDP-MED on all interfaces or on a specific interface:

```
[edit protocols lldp-med]
user@router# set interface (LLDP-MED) ge-0/0/2.0
```

Configuring Location Information Advertised by the Router

You can configure the location information that is advertised from the router to the LLDP-MED device. You can specify a civic-based location (geographic location) or a location based on an ELIN (Emergency Location Identification Number):

- To specify a location by geography:

  ```
  [edit protocols lldp-med]
  user@router# set interface ge-0/0/2.0 location civic-based country-code US
  user@router# set interface ge-0/0/2.0 location civic-based ca-type 1 ca-value “El Dorado County”
  user@router# set interface ge-0/0/2.0 location civic-based ca-type 2 ca-value CA
  user@router# set interface ge-0/0/2.0 location civic-based ca-type 3 ca-value Somerset
  user@router# set interface ge-0/0/2.0 location civic-based ca-type 6 ca-value “Mount Aukum Road”
  user@router# set interface ge-0/0/2.0 location civic-based ca-type 19 ca-value 6450
  user@router# set interface ge-0/0/2.0 location civic-based ca-type 21 ca-value “Holiday Market”
  ```

- To specify a location using an **elin** string:

  ```
  [edit protocols lldp-med]
  user@router# set interface ge-0/0/2.0 location elin 4085551212
  ```

Configuring for Fast Start

You can specify the number of LLDP-MED advertisements sent from the router in the first second after it has detected an LLDP-MED device. The default is 3; to set it to another value:

```
[edit protocols lldp-med]
user@router# set fast-start 6
```

NOTE: If an interface is configured as a VoIP interface, then the router does not wait for an attached phone to identify itself as an LLDP-MED device before it performs an LLDP-MED fast start after a graceful Routing Engine switchover (GRES) or a reboot. Instead, it immediately performs an LLDP-MED fast start after a GRES or reboot. This behavior prevents certain models of IP phones from resetting after a GRES.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, the router uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations.

Related Documentation

Configuring LLDP on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, devices use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links.The information enables the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.

This topic describes:

Enabling LLDP on Interfaces

LLDP is enabled on all interfaces by default. If it is disabled, you can enable LLDP by configuring it on all interfaces or on specific interfaces.

- To configure LLDP on all interfaces:

```
[edit protocols lldp]
user@router# set interface all
```

- To configure LLDP on a specific interface:

```
[edit protocols lldp]
user@router# set interface interface-name
```

NOTE: On MX Series routers, LLDP cannot be configured on the management Ethernet interface. Issuing the command set protocols lldp interfaceem0 generates the following error message:

```
error: name: 'em0': Invalid interface
error: statement creation failed: interface
```

Adjusting LLDP Advertisement Settings

You can adjust the following settings for LLDP advertisements for troubleshooting or verification purposes. The default values are applied when LLDP is enabled. For normal operations, we recommend that you do not change the default values.

- To specify the frequency at which LLDP advertisements are sent (in seconds):

  ```
  [edit protocols lldp]
  user@router# set advertisement-interval seconds
  ```

  For example, using the default value:

  ```
  [edit protocols lldp]
  user@router# set advertisement-interval 45
  ```

- To specify the number of seconds that LLDP information is held before it is discarded (the multiplier value is used in combination with the **advertisement-interval** value):

  ```
  [edit protocols lldp]
  user@router# set hold-multiplier seconds
  ```

  For example, using the default value:

  ```
  [edit protocols lldp]
  user@router# set hold-multiplier 5
  ```

- To specify the number of seconds the device delays before sending advertisements to neighbors after a change is made in a TLV (type, length, or value) element in LLDP or in the state of the local system, such as a change in hostname or management address, set the transmit delay. The transmit delay is enabled by default on switches to reduce the delay in notifying neighbors of a change in the local system. The default value is 2 seconds (if the **advertisement-interval** value is set to 8 seconds or more) or 1 second (if the **advertisement-interval** value is set to less than 8 seconds).

  ```
  [edit protocols lldp]
  user@router# set transmit-delay seconds
  ```

  For example:

  ```
  [edit protocols lldp]
  user@router# set transmit-delay 2
  ```

NOTE: The advertisement-interval value must be greater than or equal to four times the transmit-delay value; otherwise, an error is returned when you attempt to commit the configuration.

Adjusting SNMP Notification Settings of LLDP Changes

You can adjust the following settings for SNMP notifications of LLDP changes. If the values are not specified or if the interval values are set to **0**, the notifications are disabled.

- To specify the frequency at which LLDP database changes are sent (in seconds):

  ```
  [edit protocols lldp]
  user@router# set lldp-configuration-notification-interval seconds
  ```

  For example:

  ```
  [edit protocols lldp]
  user@router# set lldp-configuration-notification-interval 600
  ```

- To configure the time interval for SNMP trap notifications to wait for topology changes (in seconds):

  ```
  [edit protocols lldp]
  user@router# set ptopo-configuration-trap-interval seconds
  ```

  For example:

  ```
  [edit protocols lldp]
  user@router# set ptopo-configuration-trap-interval 600
  ```

- To specify the holding time (used in combination with the **ptopo-configuration-trap-interval** value) to maintain dynamic topology entries (in seconds):

  ```
  [edit protocols lldp]
  user@router# set ptopo-configuration-maximum-hold-time seconds
  ```

  For example:

  ```
  [edit protocols lldp]
  user@router# set ptopo-configuration-maximum-hold-time 2147483647
  ```

Specifying a Management Address for the LLDP Management TLV

You can configure an IPv4 or IPv6 management address to be used in the LLDP Management Address type, length, and value (TLV) messages. Only out-of-band management addresses must be used as the value for the **management-address** statement.

To configure the management address:

```
[edit protocols lldp]
user@router# set management-address ip-address
```

NOTE: Ensure that the interface with the configured management address has LLDP enabled using the **set protocols lldp interface** command. If you configure a customized management address for LLDP on an interface that has LLDP disabled, the **show lldp local-information** command output will not display the correct interface information.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, devices use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links.

Configuring Server Fail Fallback on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, server fail fallback allows you to specify how end devices connected to the router are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

802.1X and MAC RADIUS authentication work by using an *authenticator port access entity* (the router) to block all traffic to and from an end device at the interface until the end device's credentials are presented and matched on the *authentication server* (a RADIUS server). When the end device has been authenticated, the router stops blocking and opens the interface to the end device.

When you set up 802.1X or MAC RADIUS authentication on the router, you specify a primary authentication server and one or more backup authentication servers. If the primary authentication server cannot be reached by the router and the secondary authentication servers are also unreachable, a RADIUS server timeout occurs. Because the authentication server grants or denies access to the end devices awaiting authentication, the router does not receive access instructions for end devices attempting access to the LAN and normal authentication cannot be completed. Server fail fallback allows you to configure authentication alternatives that permit the router to take appropriate actions toward end devices awaiting authentication or reauthentication.

NOTE: The authentication fallback method called *server-reject VLAN* provides limited access to a LAN, typically just to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials. If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is not allowed.

To configure basic server fail fallback options using the CLI:

- Configure an interface to allow traffic to flow from a supplicant to the LAN if a RADIUS server timeout occurs (as if the end device had been successfully authenticated by a RADIUS server):

```
[edit protocols authentication-access-control]
user@router# set interface ge-0/0/1 dot1x server-fail permit
```

- Configure an interface to prevent traffic flow from an end device to the LAN (as if the end device had failed authentication and had been rejected by the RADIUS server):

```
[edit protocols authentication-access-control]
user@router# set interface ge-0/0/1 dot1x server-fail deny
```

- Configure an interface to move an end device to a specified VLAN if a RADIUS server timeout occurs (in this case, the VLAN name is **vlan1**):

```
[edit protocols authentication-access-control]
user@router# set interface ge-0/0/1 dot1x server-fail vlan-name vlan1
```

- Configure an interface to recognize already connected end devices as reauthenticated if there is a RADIUS timeout during reauthentication (new users will be denied access):

```
[edit protocols authentication-access-control]
user@router# set interface ge-0/0/1 dot1x server-fail use-cache
```

- Configure an interface that receives a RADIUS access-reject message from the authentication server to move end devices attempting LAN access on the interface to a specified VLAN already configured on the router (in this case, the VLAN name is **vlan-sf**):

```
[edit protocols authentication-access-control]
user@router# set interface ge-0/0/1 dot1x server-reject-vlan vlan-sf
```

NOTE: If an IP phone is authenticated in the server-reject VLAN, voice traffic is not allowed.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, server fail fallback allows you to specify how end devices connected to the router are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

Understanding Captive Portal Authentication on the MX Series Routers

Starting with Junos OS Release 14.2, captive portal authentication (hereafter referred to as captive portal) allows you to authenticate users on MX Series routers by redirecting Web browser requests to a login page that requires users to input a username and password before they are allowed access to the network.Captive portal controls network access by requiring users to provide information that is authenticated against a RADIUS server database using EAP-MD5, You can also use captive portal to display an acceptable-use policy to users before they access your network.

Juniper Networks Junos Software for MX Series routers provides a template that allows you to easily design and modify the look of the captive portal login page. You enable specific interfaces for captive portal. The first time a client connected to a captive portal interface attempts to access a webpage, the switch presents the captive portal login page. Upon successful authentication, the user is allowed access to the network and to continue to the original page requested.

NOTE: If Hypertext Transfer Protocol Secure (HTTPS) is enabled, Hypertext Transfer Protocol (HTTP) requests are redirected to an HTTPS connection for the captive portal authentication process. After authentication, the client is returned to the HTTP connection.

If there are clients that are not HTTP-enabled connected to the captive portal interface, you can allow them to bypass captive portal authentication by adding their MAC address to an authentication whitelist. (If the MAC address has already been learned on the interface, you must clear it using the **clear captive-portal interface *interface-name***) before adding it to the whitelist.)

When the user is authenticated by the RADIUS server, any per-user policies (attributes) associated with that user are also sent to the switch.

Limitations of Captive Portal

Captive portal on MX Series routers has the following limitations:

- The captive portal interface must be configured for **family ethernet-switching** and set to port mode access. The VLAN must be configured with a routed VLAN interface (RVI).
- The DHCP gateway IP address for the switch must be configured as the IP address of the routed VLAN interface.
- Captive portal does not support dynamic assignment of VLANs downloaded from the RADIUS server.
- If the user is idle for more than about 5 minutes and there is no traffic passed, the user is required to log back in to the captive portal.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, captive portal authentication (hereafter referred to as captive portal) allows you to authenticate users on MX Series routers by redirecting Web browser requests to a login page that requires users to input a username and password before they are allowed access to the network.

Understanding Authentication Session Timeout on MX Series Routers

Starting with Junos OS Release 14.2, you can specify authentication session timeout values for captive portal authentication sessions and 802.1X and MAC RADIUS authentication sessions.

For captive portal authentication, the length of the session depends on the value configured for the **session-expiry** statement. The remainder of this topic pertains only to 802.1X and MAC RADIUS authentication sessions.

For 802.1X and MAC RADIUS authentication sessions, the timeout of the session depends on the value of **reauthentication interval** for **dot1x authentication**. The authentication session might also end when the MAC table aging time expires because, unless you configure it not to, the session is removed from the authentication session table when the MAC address is removed from the Ethernet switching table.

Information about each 802.1X and MAC RADIUS authentication session—including the associated interfaces and VLANs for each MAC address that is authenticated by 802.1X authentication or MAC RADIUS authentication—is stored in the authentication session table. The authentication session table is tied to the Ethernet switching table (also called the MAC table). Each time the switch detects traffic from a MAC address, it updates the timestamp for that network node in the Ethernet switching table. A timer on the switch periodically checks the timestamp and if its value exceeds the user-configured **mac-table-aging-time** value, the switch removes the MAC address from the Ethernet switching table. When a MAC address ages out of the Ethernet switching table, the entry for that MAC address is also removed from the authentication database, with the result that the session ends.

You can control variables affecting timeout of authentication sessions in the following ways:

- Set the authentication session timeout on all interfaces or on selected interfaces using the **reauthentication** statement.
- Disassociate the authentication session table from the Ethernet switching table using the **no-mac-table-binding** statement. This setting prevents the termination of the authentication session when the associated MAC address ages out of the Ethernet switching table.

Release History Table

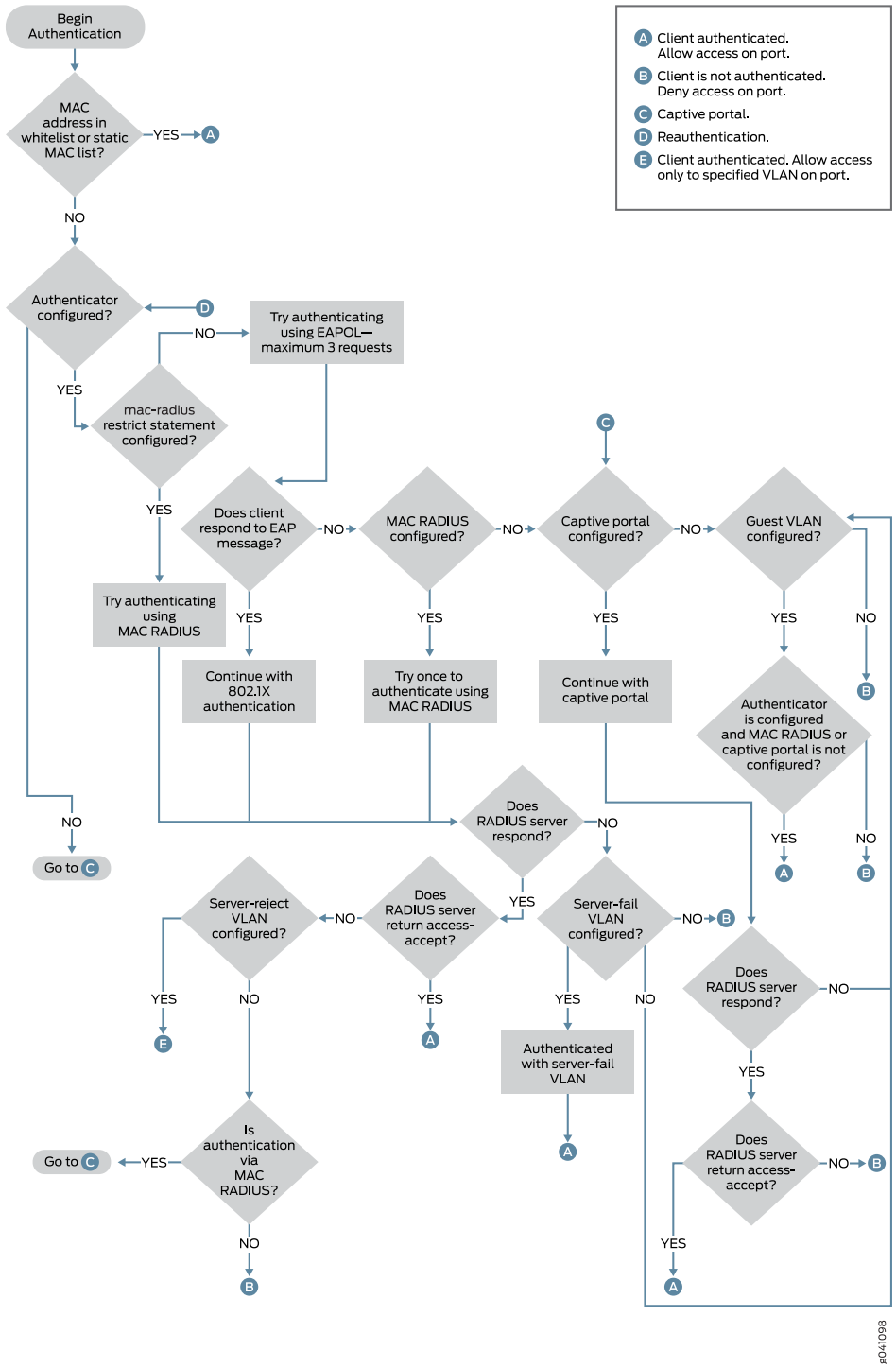
Release	Description
14.2	Starting with Junos OS Release 14.2, you can specify authentication session timeout values for captive portal authentication sessions and 802.1X and MAC RADIUS authentication sessions.

Authentication Process Flow for MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, you can control access to your network through an MX Series router by using several different authentication methods—including 802.1X, MAC RADIUS, or captive portal.

Figure 6 on page 275 illustrates the authentication process:

Figure 27: Authentication Process Flow for an MX Series Router



Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, you can control access to your network through an MX Series router by using several different authentication methods—including 802.1X, MAC RADIUS, or captive portal.

Specifying RADIUS Server Connections on an MX Series Router in Enhanced LAN Mode

IEEE 802.1X and MAC RADIUS authentication both provide network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from devices at the interface until the supplicant's credentials or MAC address are presented and matched on the *authentication server* (a RADIUS server). When the supplicant is authenticated, the router stops blocking access and opens the interface to the supplicant.

Starting with Junos OS Release 14.2, to use 802.1X or MAC RADIUS authentication, you must specify the connections on the router for each RADIUS server to which you will connect.

To configure a RADIUS server on the router:

1. Define the IP address of the RADIUS server, the RADIUS server authentication port number, and the secret password. You can define more than one RADIUS server. The secret password on the router must match the secret password on the server:

   ```
   [edit access]
   user@router# set radius-server 10.0.0.100 port 1812 secret abc
   ```

   NOTE: Specifying the authentication port is optional, and port 1812 is the default. However, we recommend that you configure it in order to avoid confusion as some RADIUS servers might refer to an older default.

2. (Optional) Specify the IP address by which the router is identified by the RADIUS server. If you do not specify this, the RADIUS server uses the address of the interface sending the RADIUS request. We recommend that you specify this IP address because if the request gets diverted on an alternate route to the RADIUS server, the interface relaying the request might not be an interface on the router.

   ```
   [edit access]
   user@router# set radius-server source-address 10.93.14.100
   ```

3. Configure the authentication order, making **radius** the first method of authentication:

   ```
   [edit access]
   user@router# set profile profile1 authentication-order radius
   ```

4. Create a profile and specify the list of RADIUS servers to be associated with the profile. For example, you might choose to group your RADIUS servers geographically by city.

This feature enables easy modification whenever you want to change to a different sent of authentication servers.

```
[edit access profile]
user@router# set atlanta radius authentication-server 10.0.0.100 10.2.14.200
```

5. Specify the group of servers to be used for 802.1X or MAC RADIUS authentication by identifying the profile name:

```
[edit access profile]
user@router# set protocols authentication-access-control authentication-profile-name
denver
```

6. Configure the IP address of the MX Series router in the list of clients on the RADIUS server. For specifics on configuring the RADIUS server, consult the documentation for your server.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, to use 802.1X or MAC RADIUS authentication, you must specify the connections on the router for each RADIUS server to which you will connect.

Configuring Captive Portal Authentication on MX Series Routers in Enhanced LAN Mode

NOTE: This example uses Junos OS for MX240, MX480, and MX960 routers with support for the Enhanced LAN mode configuration style. If your router does not run MX-LAN mode, you cannot configure port-based authentication settings in the same manner as described in this section. If you remove the network-services lan statement at the [edit chassis] hierarchy level, the system does not run in MX-LAN mode. Therefore, all of the settings that are supported outside of the MX-LAN mode are displayed and are available for definition in the CLI interface. In such a scenario, you must use the statements at the **[edit protocols dot1x]** hierarchy level to configure 802.1x and MAC RADIUS authentication, and the options at the **[edit services captive-portal]** hierarchy level to configure captive portal authentication. In MX-LAN mode, you can configure all the port-based network access control methodologies using the statements at the **[edit protocols authentication-access-control]** hierarchy level.

Starting with Junos OS Release 14.2, configure captive portal authentication (hereafter referred to as captive portal) on an MX Series router so that users connected to the router are authenticated before being allowed to access the network. When the user requests a webpage, a login page is displayed that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the router.
- Generated an SSL certificate and installed it on the router.
- Configured basic access between the MX Series router and the RADIUS server.
- Designed your captive portal login page.

This topic includes the following tasks:

- Configuring Secure Access for Captive Portal on page 477
- Enabling an Interface for Captive Portal on page 477
- Configuring Bypass of Captive Portal Authentication on page 477

Configuring Secure Access for Captive Portal

To configure secure access for captive portal:

1. Associate the security certificate with the Web server and enable HTTPS on the router:

```
[edit]
user@router# set system services web-management https local-certificate my-signed-cert
```

NOTE: You can enable HTTP instead of HTTPS, but we recommend HTTPS for security purposes.

2. Configure captive portal to use HTTPS:

```
[edit]
user@router# set protocols custom-options-captive-portal secure-authentication https
```

Enabling an Interface for Captive Portal

To enable an interface for use with captive portal authentication:

```
[edit]
user@router# set authentication-access-control interface ge-0/0/10
```

Configuring Bypass of Captive Portal Authentication

You can allow specific clients to bypass captive portal authentication:

```
[edit]
user@router# set authentication-access-control static 00:10:12:e0:28:22
```

NOTE: Optionally, you can use set authentication-access-control static 00:10:12:e0:28:22 interface ge-0/0/10.0 to limit the scope to the interface.

NOTE: If the client is already attached to the router, you must clear its MAC address from the captive portal authentication by using the **clear captive-portal mac-address** *session-mac-addr* command after adding its MAC address to the whitelist. Otherwise the new entry for the MAC address will not be added to the Ethernet switching table and the authentication bypass will not be allowed.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, configure captive portal authentication (hereafter referred to as captive portal) on an MX Series router so that users connected to the router are authenticated before being allowed to access the network.

Designing a Captive Portal Authentication Login Page on an MX Series Router

Starting with Junos OS Release 14.2, you can set up captive portal authentication on your switch to redirect all Web browser requests to a login page that requires the user to input a username and password before they are allowed access.Upon successful authentication, the user is allowed access to the network and redirected to the original page requested.

Junos OS provides a customizable template for the captive portal window that allows you to easily design and modify the look of the captive portal login page. You can modify the design elements of the template to change the look of your captive portal login page and to add instructions or information to the page. You can also modify any of the design elements of a captive portal login page.

The first screen displayed before the captive login page requires the user to read the “Terms and Conditions of Use”. By clicking the Agree button, the user can access the captive portal login page.

Figure 19 on page 381 shows an example of a captive portal login page:

Figure 28: Example of a Captive Portal Login Page

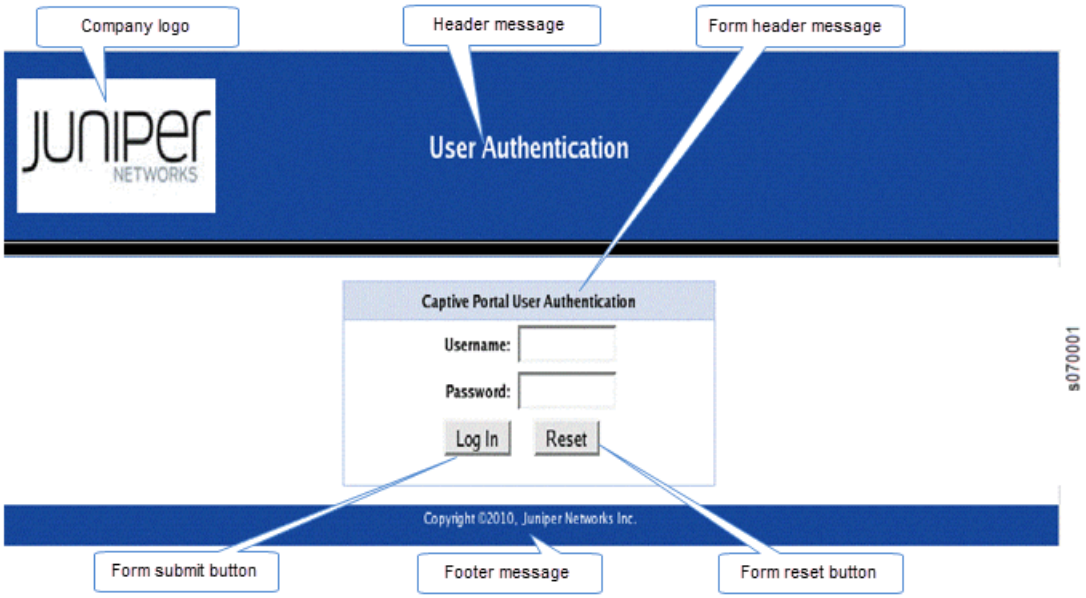


Table 30 on page 381 summarizes the configurable elements of a captive portal login page.

Table 33: Configurable Elements of a Captive Portal Login Page

Element	CLI Statement	Description
Footer background color	**footer-bgcolor** ***hex-color***	The HTML hexadecimal code for the background color of the captive portal login page footer.
Footer message	**footer-message** ***text-string***	Text displayed in the footer of the captive portal login page. You can include copyright information, links, and additional information such as help instructions, legal notices, or a privacy policy The default text shown in the footer is **Copyright @2010, Juniper Networks Inc.**
Footer text color	**footer- text-color** ***color***	Color of the text in the footer. The default color is white.
Form header background color	**form-header-bgcolor** ***hex-color***	The HTML hexadecimal code for the background color of the header bar across the top of the form area of the captive portal login page.
Form header message	**form-header-message** ***text-string***	Text displayed in the header of the captive portal login page. The default text is **Captive Portal User Authentication**
Form header text color	**form-header- text- color** *color*	Color of the text in the form header. The default color is black.
Form reset button label	**form-reset-label** ***label-name***	Using the **Reset** button, the user can clear the username and password fields on the form.

Table 33: Configurable Elements of a Captive Portal Login Page (continued)

Element	CLI Statement	Description
Form submit button label	**form-submit-label** ***label-name***	Using the **Login** button, the user can submit the login information.
Header background color	**header-bgcolor** ***hex-color***	The HTML hexadecimal code for the background color of the captive portal login page header.
Header logo	**header-logo** ***filename***	Filename of the file containing the image of the logo that you want to appear in the header of the captive portal login page. The image file can be in GIF, JPEG, or PNG format You can upload a logo image file to the switch. Copy the logo to the /var/tmp directory on the switch (during commit, the files are saved to persistent locations). If you do not specify a logo image, the Juniper Networks logo is displayed.
Header message	**header-message** ***text-string***	Text displayed in the page header. The default text is **User Authentication**.
Header text color	**header-text- color***color*	Color of the text in the header. The default color is white.
Post-authentication URL	**post-authentication-url** ***url***	URL to which the users are directed on successful authentication. By default, users are directed to the page they had originally requested.

To design the captive portal login page:

1. (Optional) Upload your logo image file to the switch:

   ```
   user@router> file copy ftp://username:prompt@ftp.hostname.net/var/tmp/my-logo.jpeg
   ```

2. Configure the custom options to specify the background colors and text displayed in the captive portal page:

   ```
   [edit protocols]
   user@router# set captive-portal-custom-options header-bgcolor #006600
   set captive-portal-custom-options header-message “Welcome to Our Network”
   set captive-portal-custom-options banner-message “Please enter your username and
   password”.The banner displays the message ”XXXXXXX” by default. The user can modify this
   message.
   set custom-options footer-message “Copyright ©2010, Our Network”
   ```

Now you can commit the configuration.

NOTE: For the custom options that you do not specify, the default value is used.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, you can set up captive portal authentication on your switch to redirect all Web browser requests to a login page that requires the user to input a username and password before they are allowed access.

Configuring Static MAC Bypass of Authentication on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, you can configure a static MAC bypass list (sometimes called the exclusion list) on the switch to specify MAC addresses of devices allowed access to the LAN without 802.1X or MAC RADIUS authentication requests to the RADIUS server.

To configure the static MAC bypass list:

- Specify a MAC address to bypass authentication:

```
[edit protocols authentication-access-control]
user@router# set static 00:04:0f:fd:ac:fe
```

- Configure a supplicant to bypass authentication if connected through a particular interface:

```
[edit protocols authentication-access-control]
user@router# set static 00:04:0f:fd:ac:fe interface ge-0/0/5
```

- You can configure a supplicant to be moved to a specific VLAN after it is authenticated:

```
[edit protocols authentication-access-control]
user@router# set static 00:04:0f:fd:ac:fe interface ge-0/0/5 vlan-assignment default-vlan
```

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, you can configure a static MAC bypass list (sometimes called the exclusion list) on the switch to specify MAC addresses of devices allowed access to the LAN without 802.1X or MAC RADIUS authentication requests to the RADIUS server.

Controlling Authentication Session Timeouts on an MX Series Router in Enhanced LAN Mode

Starting with Junos OS Release 14.2, for 802.1X and MAC RADIUS authentication sessions, you can specify authentication session timeout values using the **reauthentication** statement.

The session might also end when the MAC table aging time expires, because the session is removed from the authentication session table when the MAC address is removed from the Ethernet switching table. In order to prevent the session from being removed from the authentication session table, you must disassociate the authentication table from the Ethernet switching table using the **no-mac-table-binding** statement.

Before you begin:

- Specify the RADIUS server or servers to be used as the authentication server.
- Configure 802.1X authentication on the router.

To configure the authentication session time on all interfaces:

```
[edit]
user@router# set protocols authentication-access-control interface all dot1x reauthentication seconds;
```

To configure the authentication session time on a single interface:

```
[edit]
user@router# set protocols authentication-access-control interface interface-name dot1x reauthentication seconds;
```

To disable removal of authentication sessions from the authentication session table when a MAC address ages out of the Ethernet switching table, remove the binding of the authentication table to the Ethernet switching table.

To remove the binding on all interfaces:

```
[edit]
user@router# set protocols authentication-access-control no-mac-table-binding interface all;
```

To remove the binding on a single interface:

```
[edit]
user@router# set protocols authentication-access-control no-mac-table-binding interface interface-name;
```

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, for 802.1X and MAC RADIUS authentication sessions, you can specify authentication session timeout values using the **reauthentication** statement.

Related Documentation

Configuring MAC RADIUS Authentication on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, you can permit devices that are not 802.1X-enabled LAN access by configuring MAC RADIUS authentication on the MX Series router interfaces to which the hosts are connected.

NOTE: You can also allow non-802.1X-enabled devices to access the LAN by configuring their MAC address for static MAC bypass of authentication.

You can configure MAC RADIUS authentication on an interface that also allows 802.1X authentication, or you can configure either authentication method alone.

If both MAC RADIUS and 802.1X authentication are enabled on the interface, the router first sends the host three EAPOL requests to the host. If there is no response from the host, the router sends the host's MAC address to the RADIUS server to check whether it is a permitted MAC address. If the MAC address is configured as permitted on the RADIUS server, the RADIUS server sends a message to the router that the MAC address is a permitted address, and the router opens LAN access to the nonresponsive host on the interface to which it is connected.

If MAC RADIUS authentication is configured on the interface but 802.1X authentication is not (by using the **mac-radius restrict** option), the router attempts to authenticate the MAC address with the RADIUS server without delaying by attempting 802.1X authentication first.

Before you configure MAC RADIUS authentication, be sure you have:

- Configured basic access between the MX Series router and the RADIUS server.
- Configured MX240, MX480, and MX960 routers to function in enhanced LAN mode by entering the **network-services lan** statement at the **[edit chassis]** hierarchy level.

To configure MAC RADIUS authentication using the CLI:

- On the router, configure the interfaces to which the nonresponsive hosts are attached for MAC RADIUS authentication, and add the **restrict** qualifier for interface **ge-0/0/20** to have it use only MAC RADIUS authentication:

```
[edit]
user@router# set protocols authentication-access-control interface ge-0/0/19 dot1x
mac-radius
user@router# set protocols authentication-access-control interface ge-0/0/20 dot1x
mac-radius restrict
```

- On a RADIUS authentication server, create user profiles for each nonresponsive host using the MAC address (without colons) of the nonresponsive host as the username and password (here, the MAC addresses are **00:04:0f:fd:ac:fe** and **00:04:ae:cd:23:5f**):

```
[root@freeradius]#
edit /etc/raddb
vi users
00040ffdacfe Auth-type:=Local, User-Password = "00040ffdacfe"
0004aecd235f Auth-type:=Local, User-Password = "0004aecd235f"
```

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, you can permit devices that are not 802.1X-enabled LAN access by configuring MAC RADIUS authentication on the MX Series router interfaces to which the hosts are connected.

Related Documentation

Example: Configuring MAC RADIUS Authentication on an MX Series Router

Starting with Junos OS Release 14.2 to permit hosts that are not 802.1X-enabled to access the LAN, you can configure MAC RADIUS authentication on the router interfaces to which the non-802.1X-enabled hosts are connected. When MAC RADIUS authentication is configured, the router will attempt to authenticate the host with the RADIUS server using the host's MAC address.

This example describes how to configure MAC RADIUS authentication for two non-802.1X-enabled hosts:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 14.2 or later for MX240, MX480, or MX960 routers running in enhanced LAN mode.
- An MX Series router acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- A RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the router, be sure you have:

- Configured enhanced LAN mode on the router.
- Performed basic bridging and VLAN configuration on the router.
- Configured users on the RADIUS authentication server.

Overview and Topology

IEEE 802.1X Port-Based Network Access Control (PNAC) authenticates and permits devices access to a LAN if the devices can communicate with the router using the 802.1X protocol (are 802.1X-enabled). To permit non-802.1X-enabled end devices to access the LAN, you can configure MAC RADIUS authentication on the interfaces to which the end devices are connected. When the MAC address of the end device appears on the interface, the router consults the RADIUS server to check whether it is a permitted MAC address. If the MAC address of the end device is configured as permitted on the RADIUS server, the router opens LAN access to the end device.

You can configure both MAC RADIUS authentication and 802.1X authentication methods on an interface configured for multiple supplicants. Additionally, if an interface is only connected to a non-802.1X-enabled host, you can enable MAC RADIUS and not enable 802.1X authentication using the **mac-radius restrict** option, and thus avoid the delay that occurs while the router determines that the device is does not respond to EAP messages.

Two printers are connected to an MX Series router over interfaces, ge-0/0/19 and ge-0/0/20.

Table 24 on page 328 shows the components in the example for MAC RADIUS authentication.

Table 34: Components of the MAC RADIUS Authentication Configuration Topology

Property	Settings
Router hardware	Ports (ge-0/0/0 through ge-0/0/23)
VLAN name	sales

Table 34: Components of the MAC RADIUS Authentication Configuration Topology (continued)

Property	Settings
Connections to printers	ge-0/0/19, MAC address 00040ffdacfe ge-0/0/20, MAC address 0004aecd235f
RADIUS server	Connected to the router on interface **ge-0/0/10**

The printer with the MAC address 00040ffdacfe is connected to access interface ge-0/0/19. A second printer with the MAC address 0004aecd235f is connected to access interface ge-0/0/20. In this example, both interfaces are configured for MAC RADIUS authentication on the router, and the MAC addresses (without colons) of both printers are configured on the RADIUS server. Interface ge-0/0/20 is configured to eliminate the normal delay while the router attempts 802.1X authentication; MAC RADIUS authentication is enabled and 802.1X authentication is disabled using the **mac radius restrict** option.

Configuration

CLI Quick Configuration

To quickly configure MAC RADIUS authentication, copy the following commands and paste them into the router terminal window:

```
[edit]
set protocols authentication-access-control interface ge-0/0/19 dot1x mac-radius
set protocols authentication-access-control authenticator interface ge-0/0/20 dot1x mac-radius
restrict
```

NOTE: You must also configure the two MAC addresses as usernames and passwords on the RADIUS server, as is done in step 2 of the Step-by-Step Procedure.

Step-by-Step Procedure

Configure MAC RADIUS authentication on the router and on the RADIUS server:

1. On the router, configure the interfaces to which the printers are attached for MAC RADIUS authentication, and configure the **restrict** option on interface **ge-0/0/20**, so that only MAC RADIUS authentication is used:

   ```
   [edit]
   user@router# set protocols authentication-access-control interface ge-0/0/19 dot1x
   mac-radius
   user@router# set protocols authentication-access-control authenticator interface
   ge-0/0/20 dot1x mac-radius restrict
   ```

2. On the RADIUS server, configure the MAC addresses **00040ffdacfe** and **0004aecd235f** as usernames and passwords:

   ```
   [root@freeradius]#
   edit /etc/raddb
   ```

```
vi users
00040ffdacfe Auth-type:=EAP, User-Password = "00040ffdacfe"
0004aecd235f Auth-type:=EAP, User-Password = "0004aecd235f"
```

Results Display the results of the configuration on the router:

```
user@router> show configuration
protocols {
  authentication-access-control {
    authentication-profile-name profile52;
    interface {
      ge-0/0/19.0 {
        dot1x {
          mac-radius;
        }
      }
      ge-0/0/20.0 {
        dot1x {
          mac-radius {
            restrict;
          }
        }
      }
    }
  }
}
```

Verification

Verify that the supplicants are authenticated:

- Verifying That the Supplicants Are Authenticated on page 488

Verifying That the Supplicants Are Authenticated

Purpose After supplicants are configured for MAC RADIUS authentication on the router and on the RADIUS server, verify that they are authenticated and display the method of authentication:

Action Display information about 802.1X-configured interfaces **ge-0/0/19** and **ge-0/0/20**:

```
user@router> show dot1x interface ge-0/0/19.0 detail
ge-0/0/19.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

```
user@router> show dot1x interface ge-0/0/20.0 detail
ge-0/0/20.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Enabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user102, 00:04:ae:cd:23:5f
      Operational state: Authenticated
      Authentcation method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning The sample output from the **show dot1x interface detail** command displays the MAC address of the connected end device in the **Supplicant** field. On interface ge-0/0/19, the MAC address is **00:04:0f:fd:ac:fe**, which is the MAC address of the first printer configured for MAC RADIUS authentication. The **Authentication method** field displays the

authentication method as **MAC Radius**. On interface **ge-0/0/20**, the MAC address is **00:04:ae:cd:23:5f**, which is the MAC address of the second printer configured for MAC RADIUS authentication. The **Authentication method** field displays the authentication method as **MAC Radius**.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2 to permit hosts that are not 802.1X-enabled to access the LAN, you can configure MAC RADIUS authentication on the router interfaces to which the non-802.1X-enabled hosts are connected.

Example: Setting Up Captive Portal Authentication on an MX Series Router

Starting with Junos OS Release 14.2, you can set up captive portal authentication (hereafter referred to as captive portal) on a router to redirect Web browser requests to a login page that requires the user to input a username and password.Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

This example describes how to set up captive portal on an MX Series router:

Requirements

This example uses the following hardware and software components:

- An MX Series router that supports captive portal
- Junos OS Release 14.2 or later for MX Series routers

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the router.
- Generated an SSL certificate and installed it on the router.
- Configured basic access between the MX Series router and the RADIUS server.
- Designed your captive portal login page. .

Overview and Topology

This example shows the configuration required on the router to enable captive portal on an interface. To permit a printer connected to the captive portal interface to access the LAN without going through captive portal, add its MAC address to the authentication

whitelist. The MAC addresses in this list are permitted access on the interface without captive portal.

The topology for this example consists of one MX Series router connected to a RADIUS authentication server. One interface on the router is configured for captive portal. In this example, the interface is configured in multiple supplicant mode.

Configuration

To configure captive portal on your router:

CLI Quick Configuration

To quickly configure captive portal on the router after completing the tasks in the Requirements section, copy the following commands and paste them into the router terminal window:

```
[edit]
set system services web-management http
set system services web-management https local-certificate my-signed-cert
set protocols captive-portal-custom-options secure-authentication https
set protocols authentication-access-control interface ge-0/0/10.0 supplicant multiple
set protocols authentication-access-control static 00:10:12:e0:28:22
set protocols captive-portal-custom-options post-authentication-url
http://www.my-home-page.com
```

Step-by-Step Procedure

To configure captive portal on the router:

1. Enable HTTP access on the router:

   ```
   [edit]
   user@router# set system services web-management http
   ```

2. To create a secure channel for Web access to the router, configure captive portal for HTTPS:

   NOTE: You can enable HTTP without enabling HTTPS, but we recommend HTTPS for security purposes.

   a. Associate the security certificate with the Web server and enable HTTPS access on the router:

      ```
      [edit]
      user@router# set system services web-management https local-certificate
      my-signed-cert
      ```

   b. Configure captive portal to use HTTPS:

      ```
      [edit]
      user@router# set protocols captive-portal-custom-options secure-authentication
      https
      ```

3. Enable an interface for captive portal:

```
[edit]
user@router# set protocols authentication-access-control interface ge-0/0/10.0 supplicant
multiple
```

4. (Optional) Allow specific clients to bypass captive portal:

NOTE: If the client is already attached to the router, you must clear its MAC address from the captive portal authentication by using the clear captive-portal mac-address *mac-address* command after adding its MAC address to the whitelist. Otherwise the new entry for the MAC address will not be added to the Ethernet routering table and authentication bypass will not be allowed.

```
[edit]
user@router# set protocols authentication-access-control static 00:10:12:e0:28:22
```

NOTE: Optionally, you can use set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22 interface ge-0/0/10.0 to limit the scope to the interface.

5. (Optional) To redirect clients to a specified page rather than the page they originally requested, configure the post-authentication URL:

```
[edit services captive-portal]
user@router# set protocols captive-portal-custom-options post-authentication-url
http://www.my-home-page.com
```

Results Display the results of the configuration:

```
[edit]
user@router> show
system {
   services {
      web-management {
         http;
         https {
            local-certificate my-signed-cert;
         }
      }
   }
}
security {
   certificates {
      local {
         my-signed-cert {
```

```
            "-----BEGIN RSA PRIVATE KEY-----\nMIICXwIBAAKBgQDk8sUggnXdDUmr7T
              vLv63yJq/LRpDASfIDZlX3z9ZDe1Kfk5C9\nr/tkyvzv
              ...
              Pt5YmvWDoGo0mSjoE/liH0BqYdh9YGqv3T2IEUfflSTQQHEOShS0ogWDHF\
              nnyOb1O/vQtjk20X9NVQg JHBwidssY9eRp\n-----END CERTIFICATE-----\n";
              ## SECRET-DATA
        }
      }
    }
  }
  protocols {
    authentication-access-control {
    static 00:10:12:e0:28:22/48;
      interface {
        ge-0/0/10.0 {
          supplicant multiple;
        }
      }
    custom-captive-portal-options {
      secure-authentication https;
      post-authentication-url http://www.my-home-page.com;
    }
  }
```

Verification

To confirm that captive portal is configured and working properly, perform these tasks:

- Verifying That Captive Portal Is Enabled on the Interface on page 493
- Verify That Captive Portal Is Working Correctly on page 494

Verifying That Captive Portal Is Enabled on the Interface

Purpose Verify that captive portal is configured on interface ge-0/0/10.

Action Use the operational mode command **show captive-portal interface *interface-name* detail**:

```
user@router> show captive-portal interface ge-0/0/10.0 detail
```

```
ge-0/0/10.0
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Configured CP session timeout: 3600 seconds
  Server timeout: 15 seconds
```

Meaning The output confirms that captive portal is configured on interface ge-0/0/10 with the default settings for number of retries, quiet period, CP session timeout, and server timeout.

Verify That Captive Portal Is Working Correctly

Purpose Verify that captive portal is working on the router.

Action Connect a client to interface ge-0/0/10. From the client, open a Web browser and request a webpage. The captive portal login page that you designed should be displayed. After you enter your login information and are authenticated against the RADIUS server, the Web browser should display either the page you requested or the post-authentication URL that you configured.

Troubleshooting

To troubleshoot captive portal, perform these tasks:

- Troubleshooting Captive Portal on page 494

Troubleshooting Captive Portal

Problem The router does not return the captive portal login page when a user connected to a captive portal interface on the router requests a Web page.

Solution You can examine the ARP, DHCP, HTTPS, and DNS counters—if one or more of these counters are not incrementing, this provides an indication of where the problem lies. For example, if the client cannot get an IP address, check the router interface to determine whether the DHCP counter is incrementing—if the counter increments, the DHCP packet was received by the router.

```
user@router> show captive-portal firewall ge-0/0/10.0
ge-0/0/10.0
  Filter name: dot1x_ge-0/0/10
Counters:
Name                            Bytes              Packets
dot1x_ge-0/0/10_CP_arp           7616                  119
dot1x_ge-0/0/10_CP_dhcp             0                    0
dot1x_ge-0/0/10_CP_http             0                    0
dot1x_ge-0/0/10_CP_https            0                    0
dot1x_ge-0/0/10_CP_t_dns            0                    0
dot1x_ge-0/0/10_CP_u_dns            0                    0
```

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, you can set up captive portal authentication (hereafter referred to as captive portal) on a router to redirect Web browser requests to a login page that requires the user to input a username and password.

Example: Connecting a RADIUS Server for 802.1X to an MX Series Router

802.1X is the IEEE standard for Port-Based Network Access Control (PNAC). You use 802.1X to control network access. Only users and devices providing credentials that have been verified against a user database are allowed access to the network. Starting with Junos OS Release 14.2, you can use a RADIUS server as the user database for 802.1X authentication, as well as for MAC RADIUS authentication.

This example describes how to connect a RADIUS server to an MX Series router, and configure it for 802.1X:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 14.2 or later for MX240, MX480, or MX960 routers running in enhanced LAN mode and Junos OS Release 14.2R3 for all other routers.
- One router acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the router, be sure you have:

- Configured enhanced LAN mode on the router.
- Performed basic bridging and VLAN configuration on the router.
- Configured users on the RADIUS authentication server.

Overview and Topology

The MX Series router acts as an authenticator Port Access Entity (PAE). It blocks all traffic and acts as a control gate until the supplicant (client) is authenticated by the server. All other users and devices are denied access.

Consider an MX Series router that functions as an authenticator port. It is connected using the interface, ge-0/0/10, over the IP network to a RADIUS server. The router is also linked to a conference room using the interface, ge-0/0/1, to a printer using the interface, ge-0/0/20, to a hub using the interface, ge-0/0/8, and to two supplicants or clients over interfaces, ge-0/0/2 and ge-0/0/9 respectively.

Table 35: Components of the Topology

Property	Settings
Router hardware	MX Series router
VLAN name	**default**
One RADIUS server	Backend database with an address of **10.0.0.100** connected to the switch at port **ge-0/0/10**

In this example, connect the RADIUS server to access port **ge-0/0/10** on the MX Series router. The switch acts as the authenticator and forwards credentials from the supplicant to the user database on the RADIUS server. You must configure connectivity between the MX Series router and the RADIUS server by specifying the address of the server and configuring the secret password. This information is configured in an access profile on the switch.

Configuration

CLI Quick Configuration

To quickly connect the RADIUS server to the switch, copy the following commands and paste them into the switch terminal window:

```
[edit]
set access radius-server 10.0.0.100 secret juniper
set access radius-server 10.0.0.200 secret juniper
set access profile profile1 authentication-order radius
set access profile profile1 radius authentication-server [10.0.0.100 10.0.0.200]
```

Step-by-Step Procedure

To connect the RADIUS server to the switch:

1. Define the address of the servers, and configure the secret password. The secret password on the switch must match the secret password on the server:

   ```
   [edit]
   user@switch# set access radius-server 10.0.0.100 secret juniper
   user@switch# set access radius-server 10.0.0.200 secret juniper
   ```

2. Configure the authentication order, making **radius** the first method of authentication:

   ```
   [edit]
   user@switch# set access profile profile1 authentication-order radius
   ```

3. Configure a list of server IP addresses to be tried in order to authenticate the supplicant:

   ```
   [edit]
   ```

```
user@switch# set access profile profile1 radius authentication-server [10.0.0.100
10.0.0.200]
```

Results Display the results of the configuration:

```
user@switch> show configuration access
radius-server {
   10.0.0.100
      port 1812;
      secret "$9$qPT3ApBSrv69rvWLVb.P5"; ## SECRET-DATA
      }
   }
   profile profile1{
      authentication-order radius;
      radius {
         authentication-server 10.0.0.100 10.0.0.200;
      }
   }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verify That the Switch and RADIUS Server are Properly Connected on page 497

Verify That the Switch and RADIUS Server are Properly Connected

Purpose Verify that the RADIUS server is connected to the switch on the specified port.

Action Ping the RADIUS server to verify the connection between the switch and the server:

```
user@switch> ping 10.0.0.100
PING 10.0.0.100 (10.0.0.100): 56 data bytes
64 bytes from 10.93.15.218: icmp_seq=0 ttl=64 time=9.734 ms
64 bytes from 10.93.15.218: icmp_seq=1 ttl=64 time=0.228 ms
```

Meaning ICMP echo request packets are sent from the switch to the target server at 10.0.0.100 to test whether it is reachable across the IP network. ICMP echo responses are being returned from the server, verifying that the switch and the server are connected.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, you can use a RADIUS server as the user database for 802.1X authentication, as well as for MAC RADIUS authentication.

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an MX Series Router

Starting with Junos OS Release 14.2, 802.1X on MX Series routers provides LAN access to users who do not have credentials in the RADIUS database.These users, referred to as guests, are authenticated and typically provided with access to the Internet.

This example describes how to create a guest VLAN and configure 802.1X authentication for it.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 14.2 or later for MX240, MX480, or MX960 routers running in enhanced LAN mode.
- One router acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the router, be sure you have:

- Configured enhanced LAN mode on the router.
- Performed basic bridging and VLAN configuration on the router.
- Configured users on the RADIUS authentication server.

Overview and Topology

The MX Series router acts as an authenticator Port Access Entity (PAE). It blocks all traffic and acts as a control gate until the supplicant (client) is authenticated by the server. All other users and devices are denied access.

Consider an MX Series router that functions as an authenticator port. It is connected using the interface, ge-0/0/10, over the IP network to a RADIUS server. The router is also linked to a conference room using the interface, ge-0/0/1, to a printer using the interface, ge-0/0/20, to a hub using the interface, ge-0/0/8, and to two supplicants or clients over interfaces, ge-0/0/2 and ge-0/0/9 respectively.

Table 36: Components of the Topology

Property	Settings
Router hardware	MX Series router
VLAN name	**default**
One RADIUS server	Backend database with an address of **10.0.0.100** connected to the switch at port **ge-0/0/10**

In this example, access interface **ge-0/0/1** provides LAN connectivity in the conference room. Configure this access interface to provide LAN connectivity to visitors in the conference room who are not authenticated by the corporate VLAN.

Configuration of a Guest VLAN That Includes 802.1X Authentication

CLI Quick Configuration

To quickly configure a guest VLAN, with 802.1X authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans bridge-domain-name vlan-id 300
set protocols dot1x authenticator interface all guest-bridge-domain bridge-domain-name
```

Step-by-Step Procedure

To configure a guest VLAN that includes 802.1X authentication on MX Series routers:

1. Configure the VLAN ID for the guest VLAN:

   ```
   [edit]
   user@switch# set bridge-domains bridge-domain-name vlan-id 300
   ```

2. Configure the guest VLAN under dot1x protocols:

   ```
   [edit]
   user@switch# set protocols dot1x authenticator interface all guest-bridge-domain
   bridge-domain-name
   ```

Results

Check the results of the configuration:

```
user@switch> show configuration
protocols {
  dot1x {
    authenticator {
    interface {
      all {
```

```
            guest-bridge-domain {
              bridge-domain-name;
            }
          }
        }
      }
    }
  }
}
bridge-domains {
  bridge-domain-name {
    vlan-id 300;
  }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That the Guest VLAN is Configured on page 500

Verifying That the Guest VLAN is Configured

Purpose Verify that the guest VLAN is created and that an interface has failed authentication and been moved to the guest VLAN.

Action Use the operational mode commands:

```
user@switch> show bridge-domain

Instance                    Bridging Domain          Type
            Primary Table                                          Active
vs1                         dynamic                   bridge
            bridge.0                                               2
vs1                         guest                     bridge
            bridge.0                                               0
vs1                         guest-vlan                bridge
            bridge.0                                               0
vs1                         vlan_dyn                  bridge
            bridge.0                                               0
```

```
user@switch> show dot1x interface ge-0/0/1.0 detail
ge-0/0/1.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: guest-vlan
  Number of connected supplicants: 1
    Supplicant: user1, 00:00:00:00:13:23
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning The output from the **show bridge domain** command shows bridge-domain-name as the name of the VLAN and the VLAN ID as **300**.

The output from the **show dot1x interface ge-0/0/1.0 detail** command displays the bridge domain name , indicating that a supplicant at this interface failed 802.1X authentication and was passed through to the bridge-domain-name.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, 802.1X on MX Series routers provides LAN access to users who do not have credentials in the RADIUS database.

Example: Configuring Static MAC Bypass of Authentication on an MX Series Router

Starting with Junos OS Release 14.2, to allow devices to access your LAN through 802.1X-configured interfaces without authentication, you can configure a static MAC bypass list on the MX Series router.The static MAC bypass list, also known as the *exclusion list*, specifies MAC addresses that are allowed on the router without a request to an authentication server.

You can use static MAC bypass of authentication to allow connection for devices that are not 802.1X-enabled, such as printers. If a host's MAC address is compared and matched against the static MAC address list, the nonresponsive host is authenticated and an interface opened for it.

This example describes how to configure static MAC bypass of authentication for two printers:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 14.2 or later for MX240, MX480, or MX960 routers running in enhanced LAN mode.
- One router acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.

Before you connect the server to the router, be sure you have:

- Configured enhanced LAN mode on the router.
- Performed basic bridging and VLAN configuration on the router.
- Configured users on the RADIUS authentication server.

Overview and Topology

To permit printers access to the LAN, add them to the static MAC bypass list. The MAC addresses on this list are permitted access without authentication from the RADIUS server.

Consider an MX Series router that functions as an authenticator port. It is connected using the interface, ge-0/0/10, over the IP network to a RADIUS server. The router is also linked to a conference room using the interface, ge-0/0/1, to a printer using the interface, ge-0/0/20, to a hub using the interface, ge-0/0/8, and to two supplicants or clients over interfaces, ge-0/0/2 and ge-0/0/9 respectively.

The interfaces shown in Table 29 on page 370 will be configured for static MAC authentication.

Table 37: Components of the Static MAC Authentication Configuration Topology

Property	Settings
Router hardware	MX Series router
VLAN name	**default**
Connections to integrated printer/fax/copier machines (no PoE required)	**ge-0/0/19**, MAC address 00:04:0f:fd:ac:fe **ge-0/0/20**, MAC address 00:04:ae:cd:23:5f

The printer with the MAC address 00:04:0f:fd:ac:fe is connected to access interface **ge-0/0/19**. A second printer with the MAC address 00:04:ae:cd:23:5f is connected to access interface **ge-0/0/20**. Both printers will be added to the static list and bypass 802.1X authentication.

Configuration

CLI Quick Configuration

To quickly configure static MAC authentication, copy the following commands and paste them into the router terminal window:

```
[edit]
set protocols authentication-access-control static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
set protocols authentication-access-control interface all supplicant multiple
set protocols authentication-access-control authenticaton-profile-name profile1
```

Step-by-Step Procedure

Configure static MAC authentication:

1. Configure MAC addresses **00:04:0f:fd:ac:fe** and **00:04:ae:cd:23:5f** as static MAC addresses:

   ```
   [edit protocols]
   user@router# set authentication-access-control static [00:04:0f:fd:ac:fe
   00:04:ae:cd:23:5f]
   ```

2. Configure the 802.1X authentication method:

   ```
   [edit protocols]
   user@router# set authentication-access-control interface all supplicant multiple
   ```

3. Configure the authentication profile name (access profile name) to use for authentication:

   ```
   [edit protocols]
   ```

```
user@router# set authentication-access-control authentication-profile-name profile1
```

NOTE: Access profile configuration is required only for 802.1X clients, not for static MAC clients.

Results Display the results of the configuration:

```
user@router> show
interfaces {
   ge-0/0/19 {
      unit 0 {
         family bridge {
            vlan-id 10;
         }
      }
   }
   ge-0/0/20 {
      unit 0 {
         family bridge {
            vlan-id 10;
         }
      }
   }
}
protocols {
   authentication-access-control {
      authentication-profile-name profile1;
      static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f];
      interface {
         all {
            supplicant multiple;
         }
      }
   }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying Static MAC Bypass of Authentication on page 504

Verifying Static MAC Bypass of Authentication

Purpose Verify that the MAC address for both printers is configured and associated with the correct interfaces.

Action Use the operational mode command:

```
user@switch> show dot1x static-mac-address

MAC address           VLAN-Assignment          Interface
00:04:0f:fd:ac:fe     default                  ge-0/0/19.0
00:04:ae:cd:23:5f     default                  ge-0/0/20.0
```

Meaning The output field **MAC address** shows the MAC addresses of the two printers.

The output field **Interface** shows that the MAC address **00:04:0f:fd:ac:fe** can connect to the LAN through interface **ge-0/0/19.0** and that the MAC address **00:04:ae:cd:23:5f** can connect to the LAN through interface **ge-0/0/20.0**.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, to allow devices to access your LAN through 802.1X-configured interfaces without authentication, you can configure a static MAC bypass list on the MX Series router.

Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on MX Series Routers

Starting with Junos OS Release 14.2, on MX Series routers, firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server.The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.

This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

Requirements

This example uses the following hardware and software components:

- Junos OS Release 14.2 or later for MX Series routers
- One MX Series router

- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

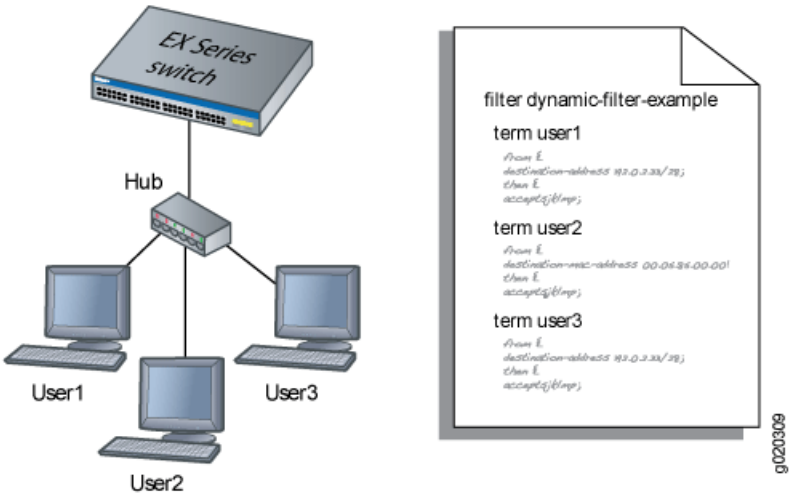
- Set up a connection between the router and the RADIUS server.
- Configured 802.1X authentication on the router, with the authentication mode for interface **ge-0/0/2** set to **multiple**.
- Configured users on the RADIUS authentication server.

Overview and Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines interface firewall filter with the user policies sent to the router from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in Figure 14 on page 358, when User1 is authenticated by the MX Series router, the system creates the firewall filter **dynamic-filter-example**. When User2 is authenticated, another term is added to the firewall filter, and so on.

Figure 29: Conceptual Model: Dynamic Filter Updated for Each New User

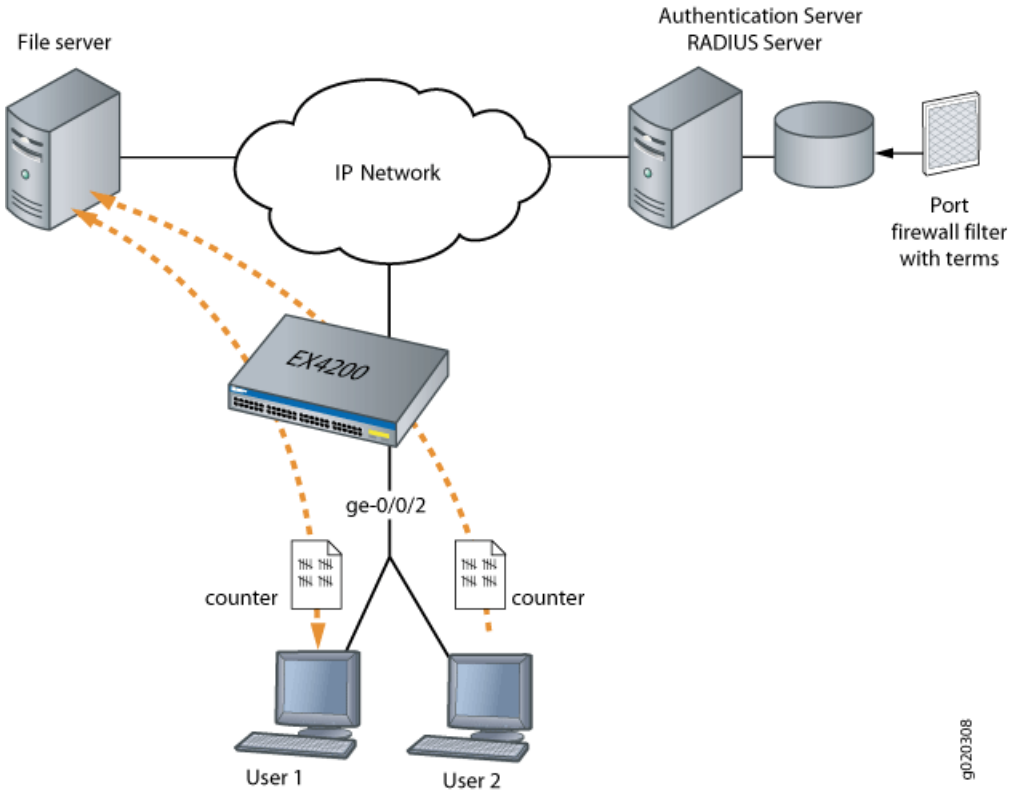


This is a conceptual model of the internal process—you cannot access or view the dynamic filter.

NOTE: If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface **ge-0/0/2** to the file server, which is located on subnet **192.0.2.16/28**, and set policer definitions to rate limit the traffic. Figure 15 on page 359 shows the network topology for this example.

Figure 30: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server



Configuration

To configure firewall filters for multiple supplicants on 802.1X-enabled interfaces:

- Configuring Firewall Filters on Interfaces with Multiple Supplicants on page 507

Configuring Firewall Filters on Interfaces with Multiple Supplicants

CLI Quick Configuration

To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the router terminal window:

```
[edit]
set protocols authentication-access-control interface ge-0/0/2 supplicant multiple
```

```
set firewall family bridge filter filter1 term term1 from destination-address 192.0.2.16/28
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall family bridge filter filter1 term term1 then count counter1
set firewall family bridge filter filter1 term term2 then policer p1
```

Step-by-Step Procedure

To configure firewall filters on an interface enabled for multiple supplicants:

1. Configure interface **ge-0/0/2** for multiple supplicant mode authentication:

   ```
   [edit protocols]
   user@router# set authentication-access-control interface ge-0/0/2 supplicant multiple
   ```

2. Set policer definition:

   ```
   user@router# show policer p1 |display set
   set firewall policer p1 if-exceeding bandwidth-limit 1m
   set firewall policer p1 if-exceeding burst-size-limit 1k
   set firewall policer p1 then discard
   ```

3. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

   ```
   [edit firewall family bridge]
   user@router# set filter filter1 term term1 from destination-address 192.0.2.16/28
   user@router# set filter filter1 term term1 then count counter1
   user@router# set filter filter1 term term2 then policer p1
   ```

Results

Check the results of the configuration:

```
user@router> show configuration

firewall {
   family bridge {
      filter filter1 {
         term term1 {
            from {
               destination-address {
                  192.0.2.16/28;
               }
            }
            then count counter1;
            term term2 {
            from {
               destination-address {
                  192.0.2.16/28;
               }
            }
            then policer p1;
         }
```

```
    }
  }
  policer p1 {
    if-exceeding {
      bandwidth-limit 1m;
        burst-size-limit 1k;
      }
      then discard;
    }
}
protocols {
  authentication-access-control {
    interface ge-0/0/2 {
      supplicant multiple;
    }
  }
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying Firewall Filters on Interfaces with Multiple Supplicants on page 509

Verifying Firewall Filters on Interfaces with Multiple Supplicants

Purpose Verify that firewall filters are functioning on the interface with multiple supplicants.

Action

1. Check the results with one user authenticated on the interface. In this case, the user is authenticated on **ge-0/0/2**:

   ```
   user@router> show dot1x firewall
   Filter: dot1x_ge-0/0/2
   Counters
   counter1_dot1x_ge-0/0/2_user1 100
   ```

2. When a second user, User2, is authenticated on the same interface, **ge-0/0/2**, you can verify that the filter includes the results for both of the users authenticated on the interface:

   ```
   user@router> show dot1x firewall
   Filter: dot1x-filter-ge-0/0/0
   Counters
   counter1_dot1x_ge-0/0/2_user1 100
   counter1_dot1x_ge-0/0/2_user2 400
   ```

Meaning The results displayed by the **show dot1x firewall** command output reflect the dynamic filter created with the authentication of each new user. User1 accessed the file server located at the specified destination address 100 times, while User2 accessed the same file server 400 times.

Release History Table

Release	Description
14.2	Starting with Junos OS Release 14.2, on MX Series routers, firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server.

CHAPTER 9

Device Discovery

Device Discovery Using LLDP and LLDP-MED on Switches

The Link Layer Discovery Protocol (LLDP) is an industry-standard, vendor-neutral method to allow networked devices to advertise capabilities, identity, and other information onto a LAN. It also provides additional TLVs for capabilities discovery, network policy, Power over Ethernet (PoE), and inventory management. For more information, read this topic.

Understanding LLDP

The device uses Link Layer Discovery Protocol (LLDP) to learn and distribute device information on network links. The information enables the switch to identify a variety of devices quickly. This quick identification results in a LAN that interoperates smoothly and efficiently.

LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include specifics, such as chassis and port identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in Junos OS.

The device supports the following basic TLVs:

- **Chassis Identifier**—The MAC address associated with the local system.
- **Port Identifier**—The port identification for the specified port in the local system.
- **Port Description**—The user-configured port description. The port description can be a maximum of 256 characters.

- **System Name**—The user-configured name of the local system. The system name can be a maximum of 256 characters.
- **System Description**—The system description containing information about the software and current image running on the system. This information cannot be configured, but is taken from the software.
- **System Capabilities**—The primary function performed by the system. The capabilities that system supports are defined; for example, bridge or router. This information cannot be configured, but is based on the model of the product.
- **Management Address**—The IP management address of the local system.

The device supports the following 802.3 TLVs:

- **Power via MDI**—A TLV that advertises media dependent interface (MDI) power support, power source equipment (PSE) power pair, and power class information.
- **MAC/PHY Configuration Status**—A TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information cannot be configured, but is based on the physical interface structure.
- **Link Aggregation**—A TLV that advertises whether the port is aggregated and its aggregated port ID.
- **Maximum Frame Size**—A TLV that advertises the Maximum Transmission Unit (MTU) of the interface sending LLDP frames.
- **Port Vlan**—A TLV that advertises the VLAN name configured on the interface.

Configuring LLDP (CLI Procedure)

Devices use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information enables the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.

This topic describes:

Enabling LLDP on Interfaces

LLDP is enabled on all interfaces by default. If it is disabled, you can enable LLDP by configuring it on all interfaces or on specific interfaces.

- To configure LLDP on all interfaces:

```
[edit protocols lldp]
user@switch# set interface all
```

- To configure LLDP on a specific interface:

```
[edit protocols lldp]
user@switch# set interface interface-name
```

Adjusting LLDP Advertisement Settings

You can adjust the following settings for LLDP advertisements for troubleshooting or verification purposes. The default values are applied when LLDP is enabled. For normal operations, we recommend that you do not change the default values.

- To specify the frequency at which LLDP advertisements are sent (in seconds):

```
[edit protocols lldp]
user@switch# set advertisement-interval seconds
```

For example, using the default value:

```
[edit protocols lldp]
user@switch# set advertisement-interval 45
```

- To specify the number of seconds that LLDP information is held before it is discarded (the multiplier value is used in combination with the **advertisement-interval** value):

```
[edit protocols lldp]
user@switch# set hold-multiplier seconds
```

For example, using the default value:

```
[edit protocols lldp]
user@switch# set hold-multiplier 5
```

- To specify the number of seconds the device waits before sending advertisements to neighbors after a change is made in a TLV (type, length, or value) element in LLDP or in the state of the local system, such as a change in hostname or management address, set the transmit delay. The transmit delay is enabled by default on switches to reduce the delay in notifying neighbors of a change in the local system. The default value is 2 seconds (if the **advertisement-interval** value is set to 8 seconds or more) or 1 second (if the **advertisement-interval** value is set to less than 8 seconds).

```
[edit protocols lldp]
user@switch# set transmit-delay seconds
```

For example:

```
[edit protocols lldp]
user@switch# set transmit-delay 2
```

NOTE: The **advertisement-interval** value must be greater than or equal to four times the **transmit-delay** value; otherwise, an error is returned when you attempt to commit the configuration.

Adjusting SNMP Notification Settings of LLDP Changes

You can adjust the following settings for SNMP notifications of LLDP changes. If the values are not specified or if the interval values are set to **0**, the notifications are disabled.

- To specify the frequency at which LLDP database changes are sent (in seconds):

  ```
  [edit protocols lldp]
  user@switch# set lldp-configuration-notification-interval seconds
  ```

  For example:

  ```
  [edit protocols lldp]
  user@switch# set lldp-configuration-notification-interval 600
  ```

- To configure the time interval for SNMP trap notifications to wait for topology changes (in seconds):

  ```
  [edit protocols lldp]
  user@switch# set ptopo-configuration-trap-interval seconds
  ```

  For example:

  ```
  [edit protocols lldp]
  user@switch# set ptopo-configuration-trap-interval 600
  ```

- To specify the holding time (used in combination with the **ptopo-configuration-trap-interval** value) to maintain dynamic topology entries (in seconds):

  ```
  [edit protocols lldp]
  user@switch# set ptopo-configuration-maximum-hold-time seconds
  ```

  For example:

  ```
  [edit protocols lldp]
  user@switch# set ptopo-configuration-maximum-hold-time 2147483647
  ```

Specifying a Management Address for the LLDP Management TLV

You can configure an IPv4 or IPv6 management address to be used in the LLDP Management Address type, length, and value (TLV) messages. Only an out-of-band management address must be used as the value for the **management-address** statement.

To configure the management address:

```
[edit protocols lldp]
```

```
user@switch# set management-address ip-address
```

NOTE: Ensure that the interface with the configured management address has LLDP enabled using the **set protocols lldp interface** command. If you configure a customized management address for LLDP on an interface that has LLDP disabled, the **show lldp local-information** command output does not display the correct interface information.

Configuring LLDP Power Negotiation

LLDP power negotiation enables the switch's Power over Ethernet (PoE) controller to dynamically allocate PoE power to PoE interfaces, based on the needs of the powered device, by negotiating with LLDP-enabled powered devices.

NOTE: LLDP power negotiation is not supported on EX3200 or EX4200 switches (except for the EX4200-PX models).

LLDP power negotiation is supported on switches running PoE controller software version 4.04 or later. For information about upgrading the PoE controller software, see *Upgrading the PoE Controller Software*.

LLDP power negotiation is automatically enabled when the PoE management mode is set to **class**:

- ```
  [edit poe]
  user@switch# set management class
  ```

To disable LLDP power negotiation:

- On switch interfaces:

  ```
  [edit protocols lldp interface all power-negotiation]
  user@switch# disable
  ```

- On a specific switch interface:

  ```
  [edit protocols lldp interface interface-name power-negotiation]
  user@switch# disable
  ```

Disabling LLDP TLVs

LLDP sends TLV messages by default. You can configure LLDP to disable non-mandatory TLVs. Mandatory TLVs are: chassis-id, port-id, and time-to-live. In this procedure, any reference to disabling all TLVs means disabling all non-mandatory TLVs.

There are two options for disabling TLVs:

- tlv-select—Select which TLVs are allowed to be advertised by LLDP. This approach is useful if you want to allow only a few TLVs and nothing else.
  ```

- tlv-filter—Filter the TLVs that should not be advertised by LLDP. This approach is useful if you want to filter only few TLVs, and allow everything else.

NOTE: The tlv-select and tlv-filter are mutually exclusive and cannot be used on the same configuration stanza at the same time.

You can disable TLVs on a specific interfaces or on all interfaces. The configuration under the interface configuration stanza takes precedence over global the global configuration.

To select which TLVs are allowed to be advertised by LLDP:

- On all interfaces:

```
[edit protocols lldp]
user@switch# set tlv-select tlv-name
```

- On a specific interface:

```
[edit protocols lldp]
user@switch# set interface interface-name tlv-select tlv-name
```

To filter TLVs that should not be advertised by LLDP:

- On all interfaces:

```
[edit protocols lldp]
user@switch# set tlv-filter tlv-name
```

- On a specific interface:

```
[edit protocols lldp]
user@switch# set interface interface-name tlv-filter tlv-name
```

The following example disables all TLVs except port-description:

```
[edit protocols lldp]
user@switch# set tlv-select port-description
```

The following example disables the system-description TLV on ge-2/1/1 interface:

```
[edit protocols lldp]
user@switch# set interface ge-2/1/1 tlv-filter system-description
```

The following example disables all TLVs except port-description and system-description on all interfaces except on the ge-0/0/1 interface, where it disables only the system-name TLV:

```
[edit protocols lldp]
user@switch# set tlv-select [port-description system-description]
user@switch# set interface ge-0/0/1 tlv-filter system-name
```

You can also disable TLVs for the LLDP Media Endpoint Discovery (LLDP-MED) protocol. See "Configuring LLDP-MED (CLI Procedure)" on page 521 for more information.

Configuring LLDP (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

Use the LLDP Configuration page to configure LLDP global and port settings for an EX Series switch on the J-Web interface.

To configure LLDP:

1. Select **Configure** > **Switching** > **LLDP**.

   The LLDP Configuration page displays LLDP Global Settings and Port Settings.

   The second half of the screen displays operational details for the selected port.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. For an EX8200 Virtual Chassis configuration, select the member and the slot (FPC) from the list.

3. To modify LLDP Global Settings, click **Global Settings**.

   Enter information as described in Table 38 on page 517.

4. To modify Port Settings, click **Edit** in the Port Settings section.

   Enter information as described in Table 39 on page 518.

Table 38: Global Settings

Field	Function	Your Action
Advertising interval	Specifies the frequency of outbound LLDP advertisements. You can increase or decrease this interval.	Type the number of seconds.
Hold multiplier	Specifies the multiplier factor to be used by an LLDP-enabled switch to calculate the time-to-live (TTL) value for the LLDP advertisements it generates and transmits to LLDP neighbors.	Type the required number in the field.

Table 38: Global Settings (continued)

Field	Function	Your Action
Fast start count	Specifies the number of LLDP advertisements sent in the first second after the device connects. The default is 3. Increasing this number results in the port initially advertising LLDP–MED at a faster rate for a limited time.	Type the Fast start count.

Table 39: Edit Port Settings

Field	Function	Your Action
LLDP Status	Specifies whether LLDP has been enabled on the port.	Select one: **Enabled**, **Disabled**, or **None**.
LLDP-MED Status	Specifies whether LLDP–MED has been enabled on the port.	Select **Enable** from the list.

Understanding LLDP and LLDP-MED on EX Series Switches

EX Series Ethernet Switches use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information enables the switch to quickly identify a variety of devices, resulting in a LAN that interoperates smoothly and efficiently.

Benefits of LLDP and LLDP-MED

- Enables the switch to quickly identify a variety of devices.
- Provides PoE power management capabilities.
- Ensures that voice traffic gets tagged and prioritized with the correct values at the source itself.

LLDP and LLDP-MED Overview

LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include information such as chassis and port identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in the Junos operating system (Junos OS).

LLDP-MED goes one step further than LLDP, exchanging IP-telephony messages between the switch and the IP telephone.

NOTE: If your IP telephone is configured for VoIP (VoIP), the switch automatically detects the configuration and assigns the telephone to the voice VLAN. The implementation of a voice VLAN on an IP telephone is vendor-specific. Consult the documentation that came with your IP telephone for instructions on configuring a voice VLAN. For example, on an Avaya phone, you can ensure that the phone gets the correct VoIP VLAN ID even in the absence of LLDP-MED by enabling DHCP option 176.

LLDP and LLDP-MED also provide PoE power management capabilities. LLDP power negotiation allows the switch to manage PoE power by negotiating with LLDP-enabled powered devices to dynamically allocate PoE power as needed. LLDP power priority allows an LLDP-enabled powered device to set the PoE power priority on the switch interface to which it connects.

The switch also uses these protocols to ensure that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p CoS and 802.1Q tag information can be sent to the IP telephone.

Supported LLDP TLVs

EX Series switches and QFX5100 switches support the following basic management TLVs:

- Chassis ID—The MAC address associated with the local system.

  NOTE: The Chassis ID TLV has a subtype for the network address family. LLDP frames are validated only if this subtype has a value of 1 (IPv4) or 2 (IPv6). For any other value, the transmitting device is detected by LLDP as a neighbor and displayed in the output of the **show lldp neighbors** command, but is not assigned to the VLAN.

- Port ID—The port identification for the specified port in the local system.
- Time to Live—The length of time that the received information should remain valid.
- Port Description—Textual description of the interface or the logical unit. The description for the logical unit is used, if available; otherwise, the Port Description TLV contains the description configured on the physical interface. For example, LAG member interfaces do not contain a logical unit; therefore, only the description configured on the physical interface can be used.
- System Name—The user-configured name of the local system. The system name can be a maximum of 256 characters. The system name field contains the host name and the domain name in the following format: *host-name.domain-name.*
- System Description—The system description that contains information about the software and current image running on the system. This information is not configurable, but taken from the software.

- System Capabilities—The primary function performed by the system. The capabilities that the system supports—for example, bridge or router. This information is not configurable, but based on the model of the product.
- Management Address—The IPv4 or IPv6 management address of the local system.

EX Series switches and QFX5100 switches support the following organizationally defined TLVs:

- Power via MDI—A TLV that advertises MDI (media dependent interface) power support, PSE (power sourcing equipment) power pair, and power class information.
- MAC/PHY Configuration Status—A TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU (medium attachment unit) type. The information is not configurable, but based on the physical interface structure.

NOTE: The MAC/PHY Configuration Status TLV has a subtype for the PMD Auto-Negotiation Advertised Capability field. This field contains a value of other or unknown if the LLDP packet is transmitted from a 10-gigabit SFP+ port.

- Link Aggregation—A TLV that advertises whether the port is aggregated and its aggregated port ID.
- Maximum Frame Size—A TLV that advertises the maximum transmission unit (MTU) of the interface sending LLDP frames.
- Port Vlan—A TLV that advertises the VLAN name configured on the interface.

Supported LLDP-MED TLVs

EX Series switches and QFX5100 switches support the following LLDP-MED TLVs:

- LLDP MED Capabilities—A TLV that advertises the primary function of the port. The values of capabilities range from 0 through 15:
  - 0—Capabilities
  - 1—Network Policy
  - 2—Location Identification
  - 3—Extended Power via MDI-PSE
  - 4—Inventory
  - 5-15—Reserved
- LLDP-MED Device Class Values—Categorizes media endpoint devices into classes:
  - 0—Class not defined
  - 1—Class 1 (generic endpoints). This class definition is applicable to all endpoints that require the base LLDP discovery services.

  - 2—Class 2 (media endpoints). This class includes endpoints that have IP media capabilities.
  - 3—Class 3 (communication endpoints). Devices acting as end user communication applicances
  - 4—Network Connectivity Device
  - 5-255—Reserved
- Network Policy—A TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types, such as voice or streaming video, 802.1Q VLAN tagging, and 802.1p priority bits and Diffserv code points.
- Endpoint Location— A TLV that advertises the physical location of the endpoint.
- Extended Power via MDI— A TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.

Disabling TLVs

In multi-vendor networks, it might not be desirable to send TLV messages because they can contain sensitive information about a network device. You can configure LLDP or LLDP-MED to disable any non-mandatory TLV message. Mandatory TLVs are: chassis-id, port-id, and time-to-live. All other TLVs can be disabled, either on specific interfaces or on a global basis. See "Configuring LLDP (CLI Procedure)" on page 512 and "Configuring LLDP-MED (CLI Procedure)" on page 521 for more information.

See Also
- *Understanding PoE on EX Series Switches*

Configuring LLDP-MED (CLI Procedure)

Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) is an extension of LLDP. The EX Series switch uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations.

LLDP-MED is enabled by default on EX Series switches.

This topic describes:

Enabling LLDP-MED on Interfaces

LLDP-MED is enabled on all interfaces by default. If it is disabled, you can enable LLDP-MED by configuring it on all interfaces or on specific interfaces.

NOTE: On switches running Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, configure LLDP-MED on the physical interface—for example, on ge-0/0/2. For more about ELS, see *Using the Enhanced Layer 2 Software CLI*.

To configure LLDP-MED on all interfaces or on a specific interface:

```
[edit protocols lldp-med]
user@switch# set interface interface-name
```

Configuring Location Information Advertised by the Switch

You can configure the location information that is advertised from the switch to the LLDP-MED device. You can specify a civic-based location (geographic location) or a location based on an ELIN (Emergency Location Identification Number):

- To specify a location by geography:

  ```
  [edit protocols lldp-med]
  user@switch# set interface ge-0/0/2.0 location civic-based country-code country-code
  user@switch# set interface ge-0/0/2.0 location civic-based ca-type ca-type ca-value ca-value
  ```

- To specify a location by using an **elin** string:

  ```
  [edit protocols lldp-med]
  user@switch# set interface ge-0/0/2.0 location elin 4085551212
  ```

Configuring a Fast Start for LLDP-MED

When the switch detects an LLDP-MED capable device, it begins to send LLDP advertisements from the port connected to the device. The fast start count indicates how many advertisements will be send in the first second after the switch detects the LLDP-MED device. The default is 3; to set it to another value:

```
[edit protocols lldp-med]
user@switch# set fast-start seconds
```

For example:

```
[edit protocols lldp-med]
user@switch# set fast-start 6
```

NOTE: If an interface is configured as a VoIP interface, then the switch does not wait for an attached phone to identify itself as an LLDP-MED device before it performs an LLDP-MED fast start after a graceful Routing Engine switchover (GRES) or a reboot. Instead, it immediately performs an LLDP-MED fast start after a GRES or reboot. This behavior prevents certain models of IP phones from resetting after a GRES.

Disabling LLDP-MED TLVs

LLDP-MED sends TLV messages by default. You can configure LLDP-MED to disable non-mandatory TLVs. Mandatory TLVs are: chassis-id, port-id, and time-to-live. In this procedure, any reference to disabling all TLVs means disabling all non-mandatory TLVs.

There are two options for disabling TLVs:

- tlv-select—Select which TLVs are allowed to be advertised by LLDP. This approach is useful if you want to allow only a few TLVs and nothing else.
- tlv-filter—Filter the TLVs that should not be advertised by LLDP. This approach is useful if you want to filter only few TLVs, and allow everything else.

NOTE: **The tlv-select and tlv-filter are mutually exclusive and cannot be used on the same configuration stanza at the same time.**

You can disable TLVs on a specific interfaces or on all interfaces. The configuration under the interface configuration stanza takes precedence over global the global configuration.

To select which TLVs are allowed to be advertised by LLDP-MED:

- On all interfaces:

```
[edit protocols lldp-med]
user@switch# set tlv-select tlv-name
```

- On a specific interface:

```
[edit protocols lldp-med]
user@switch# set interface interface-name tlv-select tlv-name
```

To filter TLVs that should not be advertised by LLDP-MED:

- On all interfaces:

```
[edit protocols lldp-med]
user@switch# set tlv-filter tlv-name
```

- On a specific interface:

```
[edit protocols lldp-med]
user@switch# set interface interface-name tlv-filter tlv-name
```

The following example disables all TLVs except location-id:

```
[edit protocols lldp-med]
user@switch# set tlv-select location-id
```

The following example disables the ext-power-via-mdi TLV on ge-2/1/1 interface:

```
[edit protocols lldp-med]
user@switch# set interface ge-2/1/1 tlv-filter ext-power-via-mdi
```

The following example disables all TLVs except location-id and ext-power-via-mdi on all interfaces except on the ge-0/0/1 interface, where it disables only the network-policy TLV:

```
[edit protocols lldp-med]
user@switch# set tlv-select [location-id ext-power-via-mdi]
user@switch# set interface ge-0/0/1 tlv-filter network-policy
```

You can also disable TLVs for the LLDP protocol. See "Configuring LLDP (CLI Procedure)" on page 512 for more information.

See Also

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support on page 433

Related Documentation

- VoIP on EX Series Switches on page 405

NetBIOS Snooping on EX Series Switches

NetBIOS snooping enables an EX Series switch to learn information about NetBIOS hosts that are connected to the switch. The NetBIOS snooping-enabled switch extracts the host details from the NetBIOS name registration packet and stores the details in the LLDP neighbor database. for more information, read this topic.

- Understanding NetBIOS Snooping on page 524
- Configuring NetBIOS Snooping (CLI Procedure) on page 525

Understanding NetBIOS Snooping

NetBIOS snooping allows Juniper Networks EX Series Ethernet Switches to discover NetBIOS hosts that are connected to the switch.

- What Is a NetBIOS Name? on page 524
- How NetBIOS Snooping Works on page 525

What Is a NetBIOS Name?

A NetBIOS name is a key element in communications between NetBIOS resources. A NetBIOS name identifies a NetBIOS resource on the network. A NetBIOS name is either a unique (exclusive) name or a group (nonexclusive) name. When a NetBIOS resource communicates with one other NetBIOS resource, a unique name is used in that communication. When a NetBIOS resource communicates with multiple resources, a group name is used.

The NetBIOS name of each NetBIOS resource is stored on the NetBIOS Name Server (NBNS). The NetBIOS name of a NetBIOS resource is mapped to its IP address.

A NetBIOS name is a 16-byte address. The first 15 bytes contain the name and the last byte contains the name type.

The NetBIOS name service is supported over UDP port 137.

How NetBIOS Snooping Works

You can enable NetBIOS snooping on the switch so that the switch can identify NetBIOS resources that are connected to it.

When a host connected to the switch initializes itself, it attempts to register its NetBIOS name by sending a NetBIOS name registration request message. The host can opt for either a unique or a group NetBIOS name. For a unique NetBIOS name, the host either broadcasts a NetBIOS name query message on the local network or unicasts it to the NBNS to check whether the requested name is already being used by another host. If so, the host that previously registered the name or the NBNS responds with a negative name registration response. If the host receives no negative response, it broadcasts the NetBIOS name registration packet to confirm the name. For a NetBIOS group name, the host sends a NetBIOS name registration packet, which generates no responses from other hosts because multiple hosts can use the same group name at the same time.

The NetBIOS snooping-enabled switch extracts the host details from the NetBIOS name registration packet and stores the details in the LLDP neighbor database.

See Also

- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

Configuring NetBIOS Snooping (CLI Procedure)

NetBIOS snooping enables an EX Series switch to learn information about NetBIOS hosts that are connected to the switch.

This topic describes:

Enabling NetBIOS Snooping

To enable NetBIOS snooping:

```
[edit protocols lldp]
user@switch# set netbios-snooping
```

Disabling NetBIOS Snooping

To disable NetBIOS snooping:

```
[edit protocols lldp]
user@switch# delete netbios-snooping
```

See Also

- show lldp neighbors on page 1840

Related Documentation

- netbios-snooping on page 1264

CHAPTER 10

Domain Name Security

DNSSEC Overview

Junos OS devices support the domain name service security extensions (DNSSEC) standard. DNSSEC is an extension of DNS that provides authentication and integrity verification of data by using public-key based signatures.

In DNSSEC, all the resource records in a DNS are signed with the private key of the zone owner. The DNS resolver uses the public key of the owner to validate the signature. The zone owner generates a private key to encrypt the hash of a set of resource records. The private key is stored in RRSIG record. The corresponding public key is stored in the DNSKEY record. The resolver uses the public key to decrypt the RRSIG and compares the result with the hash of the resource record to verify that it has not been altered.

Similarly, the hash of the public DNSKEY is stored in a DS record in a parent zone. The zone owner generates a private key to encrypt the hash of the public key. The private key is stored in the RRSIG record. The resolver retrieves the DS record and its corresponding RRSIG record and public key. Using the public key, the resolver decrypts the RRSIG record and compares the result with the hash of the public DNSKEY to verify that it has not been altered. This establishes a chain of trust between the resolver and the name servers.

Related Documentation

- *DNS Overview*
- Example: Configuring Keys for DNSSEC on page 531
- Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 529

Example: Configuring the TTL Value for DNS Server Caching

This example shows how to configure the TTL value for a DNS server cache to define the period for which DNS query results are cached.

Requirements

No special configuration beyond device initialization is required before performing this task.

Overview

The DNS name server stores DNS query responses in its cache for the TTL period specified in the TTL field of the resource record. When the TTL value expires, the name server sends a fresh DNS query and updates the cache. You can configure the TTL value from 0 to 604,800 seconds. You can also configure the TTL value for cached negative responses. Negative caching is the storing of the record that a value does not exist. In this example, you set the maximum TTL value for cached (and negative cached) responses to 86,400 seconds.

Configuration

Step-by-Step Procedure

To configure the TTL value for a DNS server cache:

1. Specify the maximum TTL value for cached responses, in seconds.

```
[edit]
user@host# set system services dns max-cache-ttl 86400
```

2. Specify the maximum TTL value for negative cached responses, in seconds.

```
[edit]
user@host# set system services dns max-ncache-ttl 86400
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show system services** command.

Related Documentation

- *DNS Overview*

Example: Configuring DNSSEC

DNS-enabled devices run a DNS resolver (proxy) that listens on loopback address 127.0.0.1 or ::1. The DNS resolver performs a hostname resolution for DNSSEC. Users need to set name server IP address to 127.0.0.1 or ::1 so the DNS resolver forwards all DNS queries to DNSSEC instead of to DNS. If the name server IP address is not set, DNS will handle all queries instead of to DNSSEC.

The following example shows how to set the server IP address to 127.0.0.1:

```
[edit]
user@host# set system name-server 127.0.0.1
```

The DNSSEC feature is enabled by default. You can disable DNSSEC in the server by using the following CLI command:

```
[edit]
set system services dns dnssec disable
```

Related Documentation

- DNSSEC Overview on page 527

Example: Configuring Secure Domains and Trusted Keys for DNSSEC

This example shows how to configure secure domains and trusted keys for DNSSEC.

Requirements

Set the name server IP address so the DNS resolver forwards all DNS queries to DNSSEC instead of DNS. See "Example: Configuring DNSSEC" on page 529 for more information.

Overview

You can configure secure domains and assign trusted keys to the domains. Both signed and unsigned responses can be validated when DNSSEC is enabled.

When you configure a domain as a secure domain and if DNSSEC is enabled, all unsigned responses to that domain are ignored and the server returns a SERVFAIL error code to the client for the unsigned responses. If the domain is not configured as a secure domain, unsigned responses will be accepted.

When the server receives a signed response, it checks if the DNSKEY in the response matches any of the trusted keys that are configured. If it finds a match, the server accepts the signed response.

You can also attach a DNS root zone as a trusted anchor to a secure domain to validate the signed responses. When the server receives a signed response, it queries the DNS root zone for a DS record. When it receives the DS record, it checks if the DNSKEY in the DS record matches the DNSKEY in the signed response. If it finds a match, the server accepts the signed response.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system services dns dnssec secure-domains domain1.net
set system services dns dnssec secure-domains domain2.net
set system services dns dnssec trusted-keys key domain1.net.ABC123ABCh
set system services dns dnssec dlv domain domain2.net trusted-anchor dlv.isc.org
```

Step-by-Step Procedure

To configure secure domains and trusted keys for DNSSEC:

1. Configure domain1.net and domain2.net as secure domains.

```
[edit]
user@host# set system services dns dnssec secure-domains domain1.net
user@host# set system services dns dnssec secure-domains domain2.net
```

2. Configure trusted keys to domain1.net.

```
[edit]
user@host# set system services dns dnssec trusted-keys key
   "domain1.net.ABC123ABCh"
```

3. Attach a root zone div.isc.org as a trusted anchor to a secure domain.

```
[edit]
user@host# set system services dns dnssec dlv domain domain2.net trusted-anchor
   dlv.isc.org
```

Results

From configuration mode, confirm your configuration by entering the **show system services** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
dns {
```

```
    dnssec {
      trusted-keys {
        key domain1.net.ABC123ABCh; ## SECRET-DATA
      }
      dlv {
        domain domain2.net trusted-anchor dlv.isc.org;
      }
      secure-domains {
        domain1.net;
        domain2.net;
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- DNSSEC Overview on page 527
- Example: Configuring Keys for DNSSEC on page 531

Example: Configuring Keys for DNSSEC

You can load a public key from a file or you can copy and paste the key file from a terminal. In both cases, you must save the keys to the configuration instead of to a file. The following example shows how to load a key from a file:

```
[edit system services dns dnssec trusted-keys]
#load-key filename
```

The following example explains how to load the key from a terminal:

```
[edit system services dns dnssec trusted-keys]
# set key "...pasted-text..."
```

If you are done loading the keys from the file or terminal, click **commit** in the CLI editor.

Related Documentation

- DNSSEC Overview on page 527
- Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 529

DNS Proxy Overview

A dynamic name system (DNS) proxy allows clients to use an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DNS proxy server. A DNS proxy improves domain lookup performance by caching previous lookups. A typical DNS proxy processes DNS queries by issuing a new DNS resolution query to each name server that it has detected until the hostname is resolved.

DNS Proxy Cache

When a DNS query is resolved by a DNS proxy, the result is stored in the device's DNS cache. This stored cache helps the device to resolve subsequent queries from the same domain and avoid network latency delay.

NOTE: If the proxy cache is not available, the device sends the query to the configured DNS server, which results in network latency delays.

DNS proxy maintains a cache entry for each resolved DNS query. These entries have a time-to-live (TTL) timer so the device purges each entry from the cache as it reaches its TTL and expires. You can clear a cache by using the **clear cache** command , or the cache will automatically expire along with TTL when it goes to zero.

DNS Proxy with Split DNS

The split DNS proxy feature allows you to configure your proxy server to split the DNS query based on both the interface and the domain name. You can also configure a set of name servers and associate then with a given domain name. When you query that domain name, the device sends the DNS queries to only those name servers that are configured for that domain name to ensure localization of DNS queries.

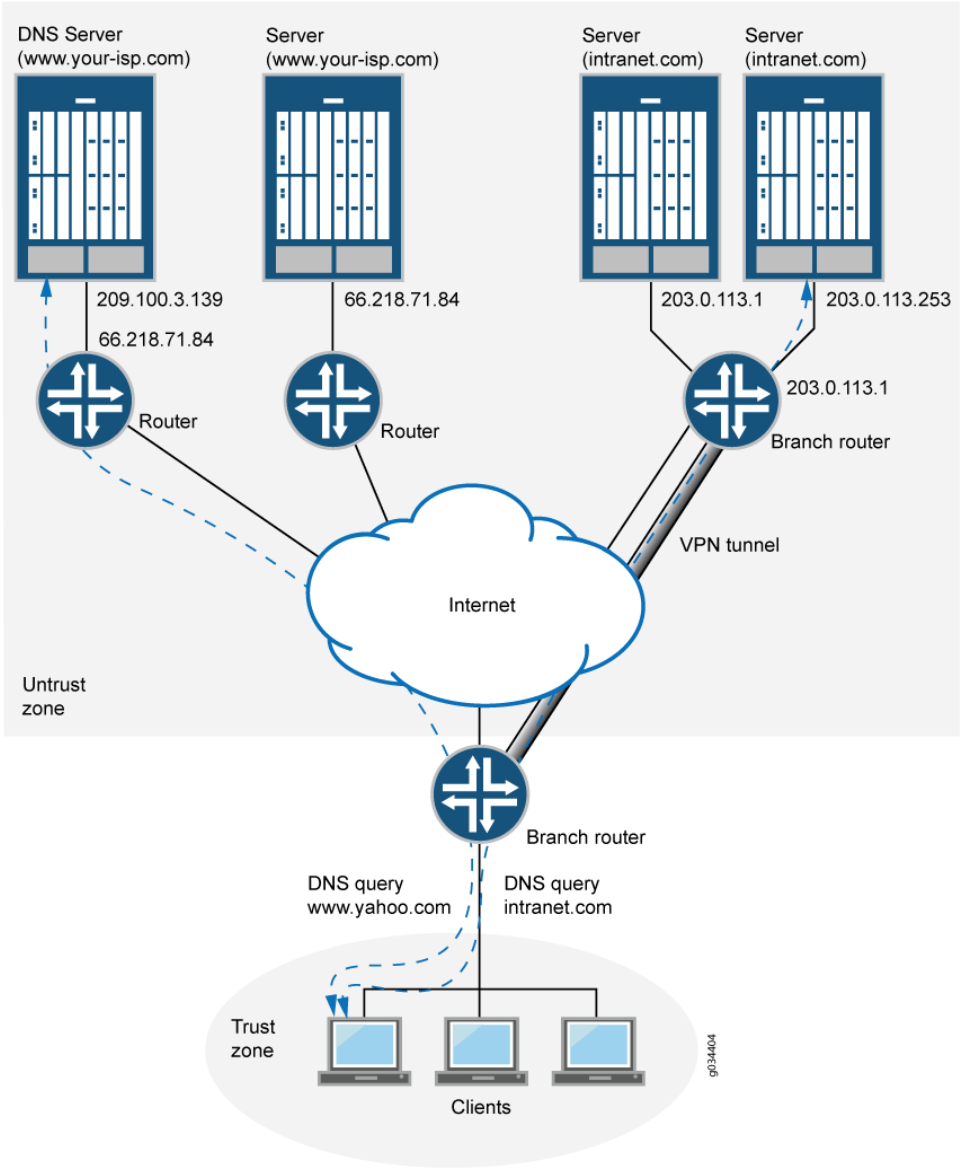
You can configure the transport method used to resolve a given domain name—for example, when the device connects to the corporate network through an IPsec VPN or any other secure tunnel. When you configure a secure VPN tunnel to transport the domain names belonging to the corporate network, the DNS resolution queries are not leaked to the ISP DNS server and are contained within the corporate network.

You can also configure a set of default domain (*) and name servers under the default domain to resolve the DNS queries for a domain for which a name server is not configured.

Each DNS proxy must be associated with an interface. If an interface has no DNS proxy configuration, all the DNS queries received on that interface are dropped.

Figure 31 on page 533 shows how the split DNS proxy works in a corporate network.

Figure 31: DNS Proxy with Split DNS



In the corporate network shown in Figure 31 on page 533, a PC client that points to the SRX Series device as its DNS server makes two queries—to www.your-isp.com and to www.intranet.com, The DNS proxy redirects the www.intranet.com, query to the www.intranet.com DNS server (203.0.113.253), while the www.your-isp.com query is redirected to the ISP DNS server (209.100.3.130). Although the query for www.your-isp.com is sent to the ISP DNS server as a regular DNS query using clear text protocols (TCP/UDP), the query for the www.intranet.com domain goes to the intranet's DNS servers over a secure VPN tunnel.

A split DNS proxy has the following advantages:

- Domain lookups are usually more efficient. For example, DNS queries meant for a corporate domain (such as acme.com) can go to the corporate DNS server exclusively, while all others go to the ISP DNS server. Splitting DNS lookups reduces the load on the corporate server and can also prevent corporate domain information from leaking onto the Internet.
- A DNS proxy allows you to transmit selected DNS queries through a tunnel interface, which prevents malicious users from learning about the internal configuration of a network. For example, DNS queries bound for the corporate server can pass through a tunnel interface to use security features such as authentication and encryption.

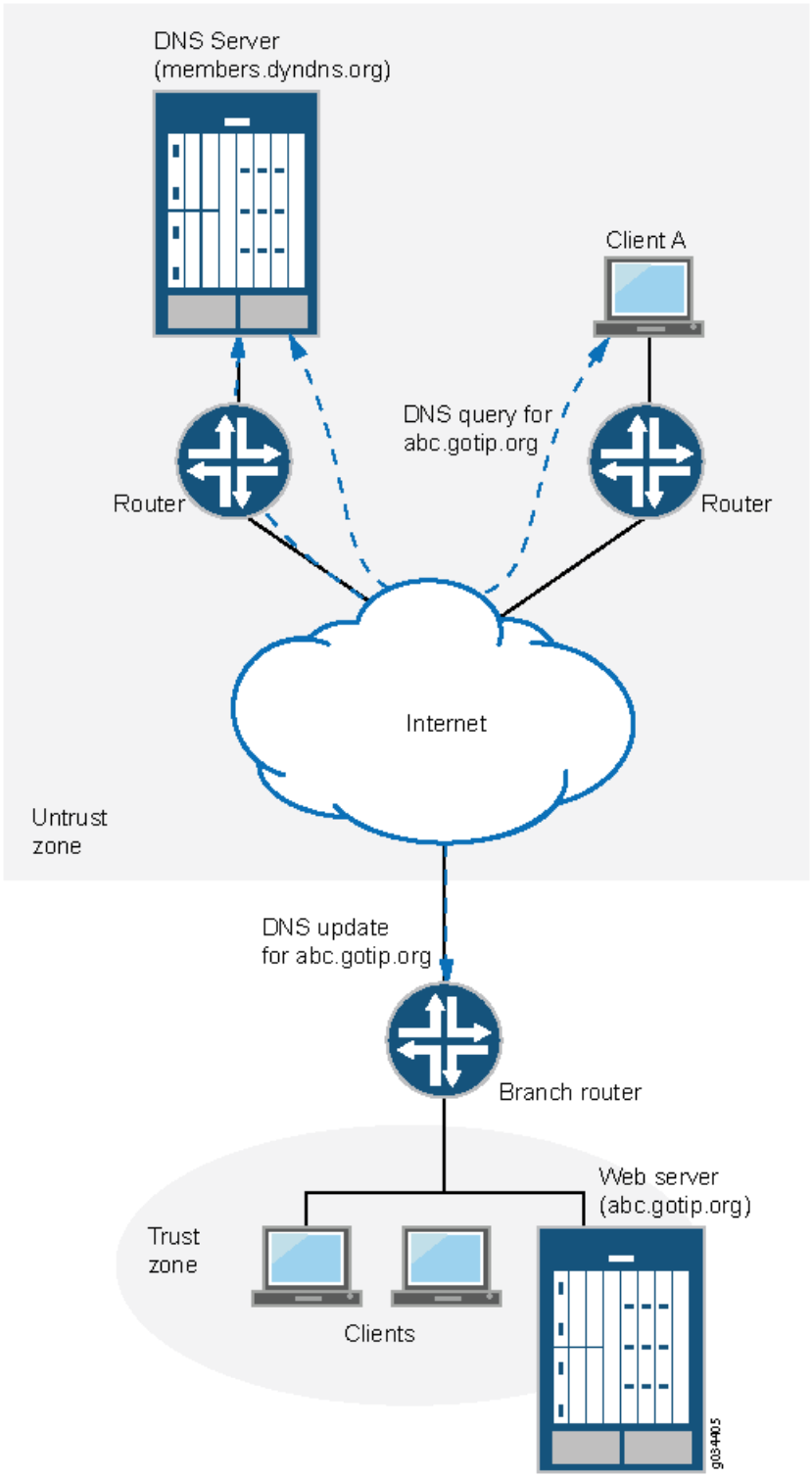
Dynamic Domain Name System Client

Dynamic DNS (DDNS) allows clients to dynamically update IP addresses for registered domain names. This feature is useful when an ISP uses Point-to-Point Protocol (PPP), Dynamic Host Configuration Protocol (DHCP), or external authentication (XAuth) to dynamically change the IP address for a customer premises equipment (CPE) router (such as a security device) that protects a Web server. Internet clients can reach the Web server by using a domain name even if the IP address of the security device has previously changed dynamically.

A DDNS server maintains a list of the dynamically changed addresses and their associated domain names. The device updates these DDNS servers with this information periodically or in response to IP address changes. The Junos OS DDNS client supports popular DDNS servers such as dyndns.org and ddo.jp

Figure 32 on page 535 illustrates how the DDNS client works.

Figure 32: Dynamic DNS



The IP address of the internal Web server is translated by Network Address Translation (NAT) to the IP address of the untrust zone interface on the device. The hostname

abc-host.com is registered with the DDNS server and is associated with the IP address of the device's untrust zone interface, which is monitored by the DDNS client on the device. When the IP address of abc-host.com is changed, the DDNS server is informed of the new address.

If a client in the network shown in Figure 32 on page 535 needs to access abc-host.com, the client queries the DNS servers on the Internet. When the query reaches the DDNS server, it resolves the request and provides the client with the latest IP address of abc-host.com.

Related Documentation

- Configuring the Device as a DNS Proxy on page 536

Configuring the Device as a DNS Proxy

The Junos operating system (Junos OS) incorporates domain name system (DNS) support, which allows you to use domain names as well as IP addresses for identifying locations. A DNS server keeps a table of the IP addresses associated with domain names. Using DNS enables an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device to reference locations by domain name (such as www.example.net) in addition to using the routable IP address.

DNS features include:

- DNS proxy cache—The device proxies hostname resolution requests on behalf of the clients behind the SRX Series device. DNS proxy improves domain lookup performance by using caching.
- Split DNS—The device redirects DNS queries over a secure connection to a specified DNS server in the private network. Split DNS prevents malicious users from learning the network configuration, and thus also prevents domain information leaks. Once configured, split DNS operates transparently.
- Dynamic DNS (DDNS) client—Servers protected by the device remain accessible despite dynamic IP address changes. For example, a protected Web server continues to be accessible with the same hostname, even after the dynamic IP address is changed because of address reassignment by the Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP) by Internet service provider (ISP).

To configure the device as a DNS proxy, you enable DNS on a logical interface and configure DNS proxy servers. Configuring a static cache enables branch office and corporate devices to use hostnames to communicate. Configuring dynamic DNS (DDNS) clients allows IP address changes.

Perform the following procedure to configure the device as a DNS proxy server by enabling DNS proxy on a logical interface—for example, ge-2/0/0.0—and configuring a set of name servers that are to be used for resolving the specified domain names. You can specify a default domain name by using an asterisk (*) and then configure a set of name servers for resolution. Use this approach when you need global name servers to resolve domain name entries that do not have a specific name server configured.

1. DNS proxy with non-split dns configuration

   - Enable DNS proxy on a logical interface.

     ```
     [edit]
     user@host# set system services dns dns-proxy interface ge-0/0/3.0
     ```

   - Set dns resolver to forward received dns query.

     ```
     [edit]
     user@host# set system services dns forwarders 192.0.2.0
     ```

   - If you are done configuring the device, commit the configuration.

     ```
     [edit]
     user@host# commit
     ```

     To verify if the configuration is working properly, execute the show command.

     ```
     user@host# show system services dns dns-proxy
     ```

2. DNS proxy with split dns configuration

   - Enable DNS proxy on a logical interface.

     ```
     [edit]
     user@host# set system services dns dns-proxy interface ge-2/0/0.0
     ```

   - Configure view for split DNS, specify the internal IP interface to handle the DNS query and view the logical subnet address.

     ```
     [edit]
     user@host# set system services dns dns-proxy view internal match-clients 1.1.1.0/24
     ```

   - Set a default internal domain name, and specify IP server for forwarding the DNS query according to their IP addresses.

     ```
     [edit]
     user@host# set system services dns dns-proxy view internal domain aa.internal.com
       forwarders 1.1.1.1
     ```



```
user@host# set system services dns dns-proxy view internal domain bb.internal.com
  forwarders 2.2.2.2
```

- Configure view for split DNS, specify the external IP interface to handle the DNS query and view the logical subnet address.

```
[edit]
user@host# set system services dns dns-proxy view external match-clients 11.1.1.0/24
```

- Set a default external domain name, and specify IP server for forwarding the DNS query according to their IP addresses.

```
[edit]
user@host# set system services dns dns-proxy view external domain aa.external.com
  forwarders 3.3.3.3
user@host# set system services dns dns-proxy view external domain bb.external.com
  forwarders 4.4.4.4
```

- If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

To verify if the configuration is working properly, execute the show command.

```
user@host# show system services dns dns-proxy
```

3. DNS proxy cache configuration

- Configure the dns proxy static cache entries to specify the host's IPv4 address.

```
[edit]
user@host# set system services dns dns-proxy cache aa.example.net inet 10.10.10.10
user@host# set system services dns dns-proxy cache bb.example.net inet
  20.20.20.20
```

- If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

To verify if the configuration is working properly, execute the show command.

```
user@host# show system services dns dns-proxy
```

4. Dynamic DNS proxy configuration

- Enable client.

```
[edit]
user@host# set system services dynamic-dns client abc.com agent juniper interface
  ge-2/0/0.0 username test password test123
```

- Configure the server.

```
[edit]
user@host# set system services dynamic-dns client abc.com agent juniper interface
   ge-2/0/0.0 username test password test123 server ddo
user@host# set system services dynamic-dns client abc.com agent juniper interface
   ge-2/0/0.0 username test password test123 server dyndns
```

- If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

To verify if the configuration is working properly

```
user@host# show system services dynamic-dns client
```

Related Documentation

- Configuring the Device as a DNS Proxy on page 536

CHAPTER 11

DHCP on Routers

DHCP for Routing Devices

A Dynamic Host Configuration Protocol (DHCP) server provides a framework to pass configuration information to client hosts on a TCP/IP network. A Junos OS device acting as a DHCP server can dynamically allocate IP addresses and other configuration parameters, minimizing the overhead that is required to add clients to the network. For more information, read this topic.

DHCP Access Service Overview

DHCP access service consists of two components: a protocol for delivering host-specific configuration information from a server to a client host and a method for allocating network addresses to a client host. The client sends a message to request configuration information. A DHCP server sends the configuration information back to the client.

With DHCP, clients can be assigned a network address for a fixed *lease*, enabling serial reassignment of network addresses to different clients. A DHCP server leases IP addresses for specific times to various clients. If a client does not use its assigned address for some period of time, the DHCP server can assign that IP address to another host. When assignments are made or changed, the DHCP server updates information in the DNS server. The DHCP server provides clients with their previous lease assignments whenever possible.

A DHCP server provides persistent storage of network parameters for clients. Because DHCP is an extension of BOOTP, DHCP servers can handle BOOTP requests.

The DHCP server includes IPv4 address assignment and commonly used DHCP options. The server is compatible with DHCP servers from other vendors on the network. The server does not support IPv6 address assignment, user class-specific configuration, DHCP failover protocol, dynamic DNS updates, or VPN connections. The Junos-FIPS software does not support the DHCP server.

NOTE: **You cannot configure a router as a DHCP server and a BOOTP relay agent at the same time.**

The following topics describe these concepts in detail:

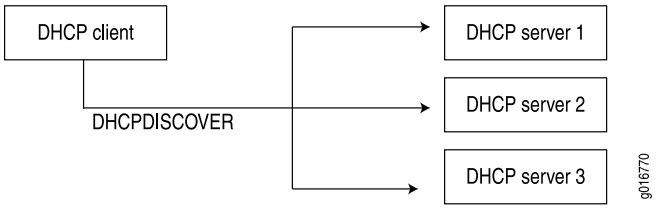
- Network Address Assignments (Allocating a New Address) on page 542
- Network Address Assignments (Reusing a Previously Assigned Address) on page 544
- Static and Dynamic Bindings on page 544
- Compatibility with Autoinstallation on page 545
- Conflict Detection and Resolution on page 545

Network Address Assignments (Allocating a New Address)

To receive configuration information and a network address assignment, a DHCP client negotiates with DHCP servers in a series of messages. The following steps show the messages exchanged between a DHCP client and servers to allocate a new network address. When allocating a new network address, the DHCP process can involve more than one server, but only one server is selected by the client.

1. When a client computer is started, it broadcasts a **DHCPDISCOVER** message on the local subnet, requesting a DHCP server. This request includes the hardware address of the requesting client.

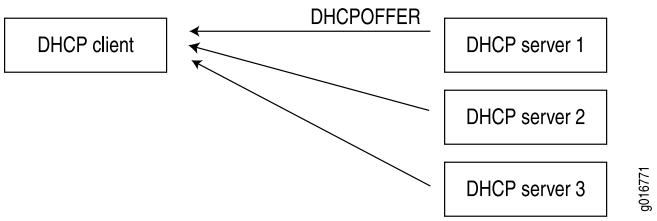
Figure 33: DHCP Discover



NOTE: For improved operation with DHCP clients that do not strictly conform to RFC 2131, the DHCP server accepts and processes **DHCPDISCOVER** messages even if the overload options in the messages are not properly terminated with an **end** statement.

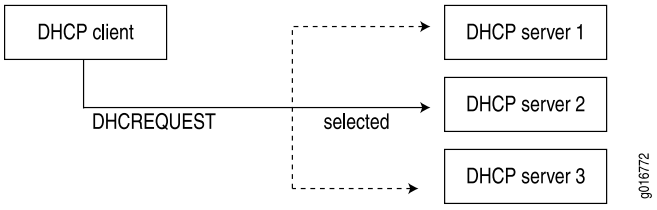
2. Each DHCP server receiving the broadcast sends a **DHCPOFFER** message to the client, offering an IP address for a set period of time, known as the lease period.

Figure 34: DHCP Offer



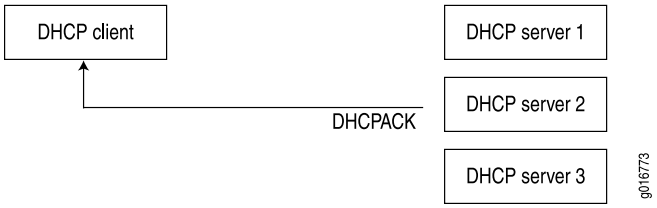
3. The client receives one or more **DHCPOFFER** messages from one or more servers and selects one of the offers received. Normally, a client looks for the longest lease period.
4. The client broadcasts a **DHCPREQUEST** message indicating the client has selected an offered leased IP address and identifies the selected server.

Figure 35: DHCP Request



5. Those servers not selected by the **DHCPREQUEST** message return the unselected IP addresses to the pool of available addresses.
6. The selected DHCP server sends a **DHCPACK** acknowledgment that includes configuration information such as the IP address, subnet mask, default gateway, and the lease period.

Figure 36: DHCP ACK

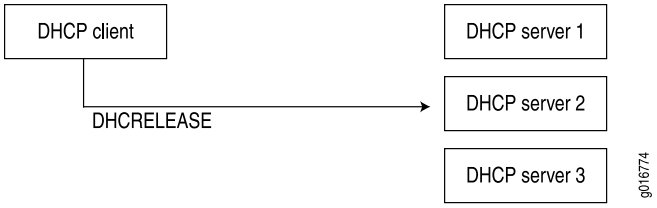


The information offered by the server is configurable.

7. The client receives the **DHCPACK** message with configuration information. The process is complete. The client is configured and has access to the network.

   - If the client receives a **DHCPNAK** message (for example, if the client has moved to a new subnet), the client restarts the negotiation process.
   - The client can relinquish its lease on a network address by sending a **DHCPRELEASE** message to the server (for example, when the client is restarted). When the server receives the **DHCPRELEASE** message, it marks the lease as free and the IP address becomes available again.

Figure 37: DHCP Release



Network Address Assignments (Reusing a Previously Assigned Address)

To enable reuse of a previously allocated network address, the following events occur:

1. A client that previously had a lease broadcasts a **DHCPREQUEST** message on the local subnet.
2. The server with knowledge of the client's configuration responds with a **DHCPACK** message.
3. The client verifies the DHCP configuration information sent by the server and uses this information to reestablish the lease.

Static and Dynamic Bindings

DHCP supports both dynamic and static bindings. For dynamic bindings, IP addresses are assigned to clients from a pool of addresses. Static bindings provide configuration information for a specific client and can include one or more fixed IP addresses for the client. You can configure a DHCP server to include both address pools and static bindings. For any individual client, static bindings take priority over address pools.

Compatibility with Autoinstallation

The DHCP server is compatible with the autoinstallation feature on J Series Services Routers. The server automatically checks autoinstallation settings for conflicts and gives autoinstallation settings priority over corresponding DHCP settings. For example, an IP address set by autoinstallation takes priority over an IP address set by the DHCP server.

NOTE: The autoinstallation feature includes a fixed address pool and a fixed lease time. With DHCP, you can create address pools and modify lease times.

Conflict Detection and Resolution

When a client receives an IP address from the DHCP server, the client performs a series of ARP tests to verify that the IP address is available and no conflicts exist. If the client detects an address conflict, the client notifies the DHCP server about the conflict and may request another IP address from the DHCP server.

The DHCP server keeps a log of all conflicts and removes addresses with conflicts from the pool. These addresses remain excluded until you manually clear the conflicts list with the **clear system services dhcp conflict** command.

DHCP Statement Hierarchy and Inheritance

DHCP configuration statements are organized hierarchically. Statements at the top of the hierarchy apply to the DHCP server and network, branches contain statements that apply to address pools in a subnetwork, and leaves contain statements that apply to static bindings for individual clients. See Table 40 on page 545.

The **pool** and **static-binding** statements appear at the **[edit system services dhcp]** hierarchy level. You can include the remaining statements at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

Table 40: Pool and Binding Statements

Statement	Description	Hierarchy Level
pool	Configure a pool of IP addresses for DHCP clients on a subnet. When a client joins the network, the DHCP server dynamically allocates an IP address from this pool.	**[edit system services dhcp]**
static-binding	Set static bindings for DHCP clients. A static binding is a mapping between a fixed IP address and the client's MAC address.	

To minimize configuration changes, include common configuration statements shown in Table 41 on page 546 (for example, the **domain-name** statement) at the highest

applicable level of the hierarchy (network or subnetwork). Configuration statements at lower levels of the hierarchy override statements inherited from a higher level. For example, if a statement appears at both the **[edit system services** dhcp**]** and **[edit system services dhcp pool]** hierarchy levels, the value assigned to the statement at the **[edit system services dhcp pool]** level takes priority.

Table 41: Common Configuration Statements

Statement	Description	Hierarchy Level
boot-file	Set the boot filename advertised to clients. The client uses the boot image stored in the boot file to complete configuration.	**[edit system services dhcp]** **[edit system services dhcp pool]** **[edit system services dhcp static-binding]**
boot-server	Set the server that contains the boot file.	
default-lease-time	Set the default lease time assigned to any client that does not request a specific lease time.	
domain-name	Configure the name of the domain in which clients will search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified.	
domain-search	Define a domain search list.	
maximum-lease-time	Set the maximum lease time allowed by the server.	
name-server	Specify the DNS server that maintains the database of client name to IP address mappings.	
option	Configure user-defined DHCP options.	
router	Specify IP address for routers on the client's subnetwork. Routers are listed in order of preference.	
server-identifier	Set the IP address of the DHCP server.	

Related Documentation

- DHCP Access Service Overview on page 542

DHCP Local Server

DHCP local server receives DHCP request and reply packets from DHCP clients and then responds with an IP address and other optional configuration information to the client. For more information, read this topic.

Configuring Address Pools for DHCP Dynamic Bindings

For dynamic bindings, set aside a pool of IP addresses that can be assigned to clients. Addresses in a pool must be available to clients on the same subnet.

To configure an address pool, include the following statements at the **[edit system services dhcp]** hierarchy level:

```
[edit system services dhcp]
pool address</prefix-length> {
   address-range {
      low address;
      high address;
   }
   exclude-address {
      address;
   }
}
```

The pool definition must include the client subnet number and prefix length (in bits). Optionally, the definition can include an address range and a list of excluded addresses.

The **address-range** statement defines the lowest and highest IP addresses in the pool that are available for dynamic address assignment. This statement is optional. If no range is specified, the pool will use all available addresses within the subnet specified. (Broadcast addresses, interface addresses, and excluded addresses are not available.)

The **exclude-address** statement specifies addresses within the range that are not used for dynamic address assignment. You can exclude one or more addresses within the range. This statement is optional.

The following is an example of a pool configuration.

```
[edit system services dhcp]
pool 10.3.3.0/24 {
   address-range low 10.3.3.2 high 10.3.3.254;
   exclude-address {
      10.3.3.33;
   }
}
```

For dynamic address assignment, configure an address pool for each client subnet the DHCP server supports. You can configure multiple address pools for a DHCP server, but only one address range per pool is supported.

DHCP maintains the state information for all pools configured. Clients are assigned addresses from pools with subnets that match the interface on which the **DHCPDISCOVER** packet is received. When more than one pool exists on the same interface, addresses are assigned on a rotating basis from all available pools.

See Also

- DHCP Access Service Overview on page 542

Configuring Manual (Static) DHCP Bindings Between a Fixed IP Address and a Client MAC Address

Static bindings provide configuration information for specific clients. This information can include one or more fixed Internet addresses, the client hostname, and a client identifier.

To configure static bindings, include the following statements at the **[edit system services dhcp]** hierarchy level:

```
[edit system services dhcp]
static-binding mac-address {
   fixed-address {
      address;
   }
   host client-hostname;
   client-identifier (ascii client-id | hexadecimal client-id);
}
```

A static binding defines a mapping between a fixed IP address and the client's MAC address.

The *mac-address* variable specifies the MAC address of the client. This is a hardware address that uniquely identifies each client on the network.

The **fixed-address** statement specifies the fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.

The **host** statement specifies the hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the **domain-name** statement.

The **client-identifier** statement is used by the DHCP server to index the database of address bindings. The client identifier is either an ASCII string or hexadecimal digits. It can include a type-value pair as specified in RFC 1700, *Assigned Numbers*. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.

NOTE: For each unique **client-identifier** ***client-id*** value, the DHCP server issues a unique lease and IP address from the pool. Previously, when the client provided an incorrect **client-identifier** ***client-id*** value, the DHCP server did not issue a lease.

The following is an example of a static binding configuration:

```
[edit system services dhcp]
static-binding 00:0d:56:f4:01:ab {
   fixed-address {
      10.5.5.5;
      10.6.6.6;
   }
   host-name "another-host.domain.tld";
   client-identifier hexadecimal 01001122aabbcc;
}
```

Specifying DHCP Lease Times for IP Address Assignments

For clients that do not request a specific lease time, the default lease time is one day. You can configure a maximum lease time for IP address assignments or change the default lease time.

To configure lease times, include the **maximum-lease-time** and **default-lease-time** statements:

```
maximum-lease-time;
default-lease-time;
```

You can include these statements at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

Lease times defined for static bindings and address pools take priority over lease times defined at the **[edit system services dhcp]** hierarchy level.

The **maximum-lease-time** statement configures the maximum length of time in seconds for which a client can request and hold a lease. If a client requests a lease longer than the maximum specified, the lease is granted only for the maximum time configured on the server. After a lease expires, the client must request a new lease.

NOTE: Maximum lease times do not apply to dynamic BOOTP leases. These leases are not specified by the client and can exceed the maximum lease time configured.

The following example shows a configuration for maximum and default lease times:

```
[edit system services dhcp]
maximum-lease-time 7200;
default-lease-time 3600;
```

Configuring a DHCP Boot File and DHCP Boot Server

When a DHCP client starts, it contacts a boot server to download the boot file.

To configure a boot file and boot server, include the **boot-file** and **boot-server** statements:

```
boot-file filename;
boot-server (address | hostname);
```

You can include these statements at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

After a client receives a **DHCPOFFER** response from a DHCP server, the client can communicate directly with the boot server (instead of the DHCP server) to download the boot file. This minimizes network traffic and enables you to specify separate boot server/file pairs for each client pool or subnetwork.

The **boot-file** statement configures the name and location of the initial boot file that the DHCP client loads and executes. This file stores the boot image for the client. In most cases, the boot image is the operating system the client uses to load.

The **boot-server** statement configures the IP address of the TFTP server that contains the client's initial boot file. You must configure an IP address or a hostname for the server.

You must configure at least one boot file and boot server. Optionally, you can configure multiple boot files and boot servers. For example, you might configure two separate boot servers and files: one for static binding and one for address pools. Boot file configurations for pools or static bindings take precedence over boot file configurations at the **[edit system services dhcp]** hierarchy level.

The following example specifies a boot file and server for an address pool:

```
[edit system services dhcp]
pool 10.4.4.0/24 {
   boot-file "boot.client";
   boot-server 10.4.4.1;
}
```

Configuring a Static IP Address as DHCP Server Identifier

The host running the DHCP server must itself use a manually assigned, static IP address. It cannot send a request and receive an IP address from itself or another DHCP server.

To configure a DHCP server identifier, include the **server-identifier** statement:

```
server-identifier address;
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The **server-identifier** statement specifies the IP address of the DHCP server. The host must be a TFTP server that is accessible by all clients served within a range of IP addresses (based on either an address pool or static binding).

The following example shows a DHCP server identifier configured for an address pool:

```
[edit system services dhcp]
pool 10.3.3.0/24 {
   address-range low 10.3.3.2 high 10.3.3.254;
   exclude-address {
      10.3.3.33;
   }
   router {
      10.3.3.1;
   }
   server-identifier 10.3.3.1;
}
```

Configuring a Domain Name and Domain Search List for a DHCP Server Host

To configure the name of the domain in which clients search for a DHCP server host, include the **domain-name** statement:

```
domain-name domain;
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
```

```
[edit system services dhcp static-binding]
```

The **domain-name** statement sets the domain name that is appended to hostnames that are not fully qualified. This statement is optional. If you do not configure a domain name, the default is the client's current domain.

To configure a domain search list, include the **domain-search** statement:

```
domain-search [ domain-list ];
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The **domain-search** statement sets the order in which clients append domain names when searching for the IP address of a host. You can include one or more domain names in the list. For more information, see RFC 3397, *Dynamic Host Configuration Protocol (DHCP) Domain Search Option*.

The **domain-search** statement is optional, if you do not configure a domain search list, the default is the client's current domain.

Configuring Routers Available to the DHCP Client

After a DHCP client loads the boot image and has booted, the client sends packets to a router.

To configure routers available to the DHCP client, include the **router** statement:

```
router {
  address;
}
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The **router** statement specifies a list of IP addresses for routers on the client's subnet. List routers in order of preference. You must configure at least one router for each client subnet.

The following example shows routers configured at the **[edit system services dhcp]** hierarchy level:

```
[edit system services dhcp]
router {
  10.6.6.1;
  10.7.7.1;
```

```
}
```

Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server

You can configure one or more user-defined options that are not included in the Junos default implementation of the DHCP server. For example, if a client requests a DHCP option that is not included in the DHCP server, you can create a user-defined option that enables the server to respond to the client's request.

To configure a user-defined DHCP option, include the **option** statement:

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

The **option** statement specifies the following values:

- *id-number*—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.
- *option-type*—Any of the following types: **byte**, **byte-stream**, **flag**, **integer**, **ip-address**, **short**, **string**, **unsigned-integer**, **unsigned-short**.
- *array*—An option can include an array of values.
- *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).

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The following example shows user-defined DHCP options:

```
[edit system services dhcp]
option 19 flag off; # 19: "IP Forwarding" option
option 40 string "domain.tld"; # 40: "NIS Domain" option
option 16 ip-address 10.3.3.33; # 16: "Swap Server" option
```

User-defined options that conflict with DHCP configuration statements are ignored by the server. For example, in the following configuration, the DHCP server ignores the user-defined **option 3 router** statement and uses the **router** statement instead:

```
[edit system services dhcp]
option 3 router 10.7.7.2; # 3: "Default Router" option
router {
   10.7.7.1;
}
```

Example: Complete DHCP Server Configuration

This topic shows a complete DHCP server configuration with address pools, static bindings, and user-defined options.

The following example shows statements at the **[edit interfaces]** hierarchy level. The interface's primary address (**10.3.3.1/24**) has a corresponding address pool (**10.3.3.0/24**) defined at the **[edit system services]** hierarchy level.

```
[edit interfaces]
fe-0/0/1 {
   unit 0 {
      family inet {
         address 10.3.3.1/24;
      }
   }
}
```

NOTE: You can configure a DHCP server only on an interface's primary IP address. The primary address on an interface is the address that is used by default as the local address for broadcast and multicast packets sourced locally and sent out the interface.

Statements at the **[edit system services]** hierarchy level include the following:

```
[edit system services]
dhcp {
   domain-name "domain.tld";
   maximum-lease-time 7200;
   default-lease-time 3600;
   name-server {
      10.6.6.6;
      10.6.6.7;
   }
   domain-search [ subnet1.domain.tld subnet2.domain.tld ];
   wins-server {
      10.7.7.7;
      10.7.7.9;
   }
   router {
      10.6.6.1;
      10.7.7.1;
   }
   option 19 flag off; # 19: "IP Forwarding" option
   option 40 string "domain.tld"; # 40: "NIS Domain" option
   option 16 ip-address 10.3.3.33; # 16: "Swap Server" option
   pool 10.3.3.0/24 {
      address-range low 10.3.3.2 high 10.3.3.254;
      exclude-address {
         10.3.3.33;
      }
```

```
      router {
        10.3.3.1;
      }
      server-identifier 10.3.3.1;
    }
    pool 10.4.4.0/24 {
      boot-file "boot.client";
      boot-server 10.4.4.1;
    }
    static-binding 00:0d:56:f4:20:01 {
      fixed-address 10.4.4.4;
      host-name "host.domain.tld";
    }
    static-binding 00:0d:56:f4:01:ab {
      fixed-address {
        10.5.5.5;
        10.6.6.6;
      }
      host-name "another-host.domain.tld";
      client-identifier "01aa.001a.bc65.3e";
    }
  }
```

Verifying and Managing the DHCP Server Configuration

To display the client address bindings for the extended DHCP local server, use the following operational commands:

- **show dhcp server binding**
- **show dhcp server statistics**

To clear client address bindings and DHCP local server statistics, use the following operational commands:

- **clear dhcp server binding**
- **clear dhcp server statistics**

For information about using these operations commands, see the *Junos System Basics and Services Reference*.

Example: Viewing DHCP Bindings

Use the CLI command **show system services dhcp binding** to view information about DHCP address bindings, lease times, and address conflicts.

The following example shows the binding type and lease expiration times for IP addresses configured on a router that supports a DHCP server:

```
user@host> show system services dhcp binding
IP Address       Hardware Address     Type    Lease expires at
192.168.1.2      00:a0:12:00:12:ab       static      never
192.168.1.3      00:a0:12:00:13:02       dynamic     2004-05-03 13:01:42 PDT
```

Enter an IP address to show binding for a specific IP address:

```
user@host> show system services dhcp binding 192.168.1.3
DHCP binding information:
IP address      192.168.1.3
Hardware address      00:a0:12:00:12:ab
Client identifier
61 63 65 64 2d 30 30 3a 61 30 3a 31 32 3a 30 30 aced-00:a0:12:00
3a 31 33 3a 30 32
Lease information:
Type       dynamic
Obtained at       2004-05-02 13:01:42 PDT
Expires at       2004-05-03 13:01:42 PDT
```

Use the **detail** option to show detailed binding information:

```
user@host> show system services dhcp binding detail
DHCP binding information:
IP address                 192.168.1.3
Hardware address           00:a0:12:00:12:ab
Pool                       192.168.1.0/24
Interface                  fe-0/0/0, relayed by 192.168.4.254
Lease information:
Type                       dynamic
Obtained at                2004-05-02 13:01:42 PDT
Expires at                 2004-05-03 13:01:42 PDT
DHCP options:
name-server foo.mydomain.tld
domain-name mydomain.tld
option 19 flag off
```

Example: Viewing DHCP Address Pools

Use the CLI **show system services dhcp pool** command to view information about DHCP address pools.

The following example show address pools configured on a DHCP server:

```
user@ host> show system services dhcp pool
Pool name        Low address     High address     Excluded addresses
10.40.1.0/24     10.40.1.1       10.40.1.254      10.40.1.254
```

Example: Viewing and Clearing DHCP Conflicts

When the DHCP server provides an IP address, the client performs an ARP check to make sure the address is not being used by another client and reports any conflicts back to the server. The server keeps track of addresses with conflicts and removes them from the address pool. Use the CLI command **show system services dhcp conflict** to show conflicts.

```
user@host> show system services dhcp conflict
```

```
Detection time                  Detection method       Address
2004-08-03 19:04:00 PDT         client      192.168.1.5
2004-08-04 04:23:12 PDT         ping      192.168.1.8
```

Use the **clear system services dhcp conflicts** command to clear the conflicts list and return IP addresses to the pool. The following command shows how to clear an address on the server that has a conflict:

```
user@host> clear system services dhcp conflict 192.168.1.5
```

For more information about CLI commands you can use with the DHCP server, see the CLI Explorer.

Configuring Tracing Operations for DHCP Processes

DHCP tracing operations track all DHCP operations and record them to a log file. By default, no DHCP processes are traced. If you include the **traceoptions** statement at the **[edit system services dhcp]** hierarchy level, the default tracing behavior is the following:

- Important events are logged in a file called **dhcpd** located in the **/var/log** directory.
- When the file **dhcpd** reaches 128 kilobytes (KB), it is renamed **dhcpd.0**, then **dhcpd.1**, and so on, until there are three trace files. Then the oldest trace file (**dhcpd.2** is overwritten). For more information about how log files are created, see the System Log Explorer.
- Log files can be accessed only by the user who configures the tracing operation.

You cannot change the directory in which trace files are located. However, you can customize the other trace file settings by including the following statements at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file filename <files number> <match regex> <size size> <world-readable |
  no-world-readable>;
flag {
  all;
}
```

Tasks for configuring DHCP tracing operations are:

1. Configuring the DHCP Processes Log Filename on page 558
2. Configuring the Number and Size of DHCP Processes Log Files on page 558
3. Configuring Access to the DHCP Log File on page 558
4. Configuring a Regular Expression for Refining the Output of DHCP Logged Events on page 558
5. Configuring DHCP Trace Operation Events on page 559

Configuring the DHCP Processes Log Filename

By default, the name of the file that records trace output is **dhcpd**. You can specify a different name by including the file statement at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file filename;
```

Configuring the Number and Size of DHCP Processes Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed ***filename*.0**, then ***filename*.1**, and so on, until there are three trace files. Then the oldest trace file (***filename*.2**) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracking operation (***filename***) reaches 2 MB, ***filename*** is renamed ***filename*.0**, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename*.0** is renamed ***filename*.1** and ***filename*** is renamed ***filename*.0**. This process repeats until there are 20 trace files. Then the oldest file (***filename*.19**) is overwritten by the newest file (***filename*.0**).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10KB through 1 gigabyte (GB).

Configuring Access to the DHCP Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the **file world-readable** statement at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file world-readable;
```

To set the default behavior explicitly, include the **file no-world-readable statement** at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file no-world readable;
```

Configuring a Regular Expression for Refining the Output of DHCP Logged Events

By default, the trace operations output includes all lines relevant to the logged events.

You can refine the output by including the match statement at the **[edit system services dhcp traceoptions file *filename*]** hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system services dhcp traceoptions]
file filename match regex;
```

Configuring DHCP Trace Operation Events

By default, only important events are logged. You can configure the trace operations to be logged by including the following options at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit dhcp system services dhcp traceoptions]
flag {
   all;
   binding;
   config;
   conflict;
   event;
   ifdb;
   io;
   lease;
   main;
   misc;
   packet;
   options;
   pool;
   protocol;
   rtsock;
   scope;
   signal;
   trace;
   ui;
}
```

DHCP Processes Tracing Flags

Table 42 on page 559 describes which operation or event is recorded by each DHCP tracing flag. By default, all flags are disabled.

Table 42: DHCP Processes Tracing Flags

Flag	Operation or Event
all	All operations.
binding	Binding operations.
config	Logins to the configuration database.
conflict	Client-detected conflicts for IP addresses.

Table 42: DHCP Processes Tracing Flags (continued)

Flag	Operation or Event
event	Important events.
ifdb	Interface database operations.
io	I/O operations.
lease	Lease operations.
main	Main loop operations.
misc	Miscellaneous operations.
packet	DHCP packets.
options	DHCP options.
pool	Address pool operations.
protocol	Protocol operations.
rtsock	Routing socket operations.
scope	Scope operations.
signal	DHCP signal operations.
trace	Tracing operations.
ui	User interface operations.

Related Documentation

- DHCP for Switches on page 581
- DHCP Overview on page 713

Extended DHCP Local Server

An extended DHCP local server enhances traditional DHCP server operation by providing additional address assignment and client configuration functionality. For more information, read this topic.

- Extended DHCP Local Server Overview on page 562
- Configuring the Router as an Extended DHCP Local Server on page 567
- Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools on page 569

Extended DHCP Local Server Overview

Junos OS includes an extended DHCP local server that enhances traditional DHCP server operation by providing additional address assignment and client configuration functionality and flexibility in a subscriber-aware environment. The extended DHCP local server enables service providers to take advantage of external address-assignment pools and integrated RADIUS-based configuration capabilities in addition to the continued support of traditional local address pools. The address-assignment pools are considered external because they are external to the DHCP local server. The pools are managed independently of the DHCP local server, and can be shared by different client applications, such as DHCP or PPPoE access. Table 43 on page 563 provides a comparison of the extended DHCP local server and a traditional DHCP local server.

The extended DHCP local server provides an IP address and other configuration information in response to a client request. The server supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide DHCP client authentication. You can configure the dynamic profile and authentication support on a global basis or for a specific group of interfaces.

Table 43: Comparing the Extended DHCP Local Server to the Traditional DHCP Local Server

Feature	Extended DHCP Local Server	Traditional DHCP Local Server
Local address pools	X	X
External, centrally-managed address pools	X	–
Local configuration	X	X
External configuration using information from address-assignment pools or RADIUS servers	X	–
Dynamic-profile attachment	X	–
RADIUS-based subscriber authentication, and configuration using RADIUS attributes and Juniper Networks VSAs	X	–
IPv6 client support	X	–
Default minimum client configuration	X	X

You can also configure the extended DHCP local server to support IPv6 clients. Both DHCP local server and DHCPv6 local server support the specific address request feature, which enables you to assign a particular address to a client.

NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the clear dhcp server binding command before you delete the DHCP server configuration.

This overview covers:

Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools

The pattern of interaction between the DHCP local server, the DHCP client, and address-assignment pools is the same regardless of whether you are using a router or a switch. However, there are some differences in the details of usage.

- On routers—In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer or customer premises equipment (CPE), and the DHCP local server is configured on the router.
- On switches—In a typical network configuration, the DHCP client is on an access device, such as a personal computer, and the DHCP local server is configured on the switch.

The following steps provide a high-level description of the interaction among the DHCP local server, DHCP client, and address-assignment pools:

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber (or DHCP client).

2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.

3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server selected to grant the address and configuration information.

4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server also installs the host route and ARP entry, and then monitors the lease state.

Providing DHCP Client Configuration Information

When the extended DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet mask. The extended DHCP application uses the information from the authentication grant for the response the DHCP application sends to the DHCP client. The DHCP application can either send the information in its original form or the application might merge the information with local configuration specifications. For example, if the authentication grant includes an address pool name and a local configuration specifies DHCP attributes for that pool (such as, DNS server address), the extended DHCP application merges the authentication results and the attributes in the reply that the server sends to the client.

A local configuration is optional — a client can be fully configured by the external authentication service. However, if the external authentication service does not provide client configuration, you might need to configure the local address-assignment pool to provide the configuration information, such as DNS server, for the client. When a local configuration specifies options, the extended DHCP application adds the local configuration options to the offer PDU the server sends to the client. If the two sets of options overlap, the options in the authentication response from the external service take precedence.

When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. Table 44 on page 565 lists the information that RADIUS might include in the authentication grant. See *RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework* for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management or DHCP management.

Table 44: Information in Authentication Grant

Attribute Number	Attribute Name	Description
RADIUS attribute 8	Framed-IP-Address	Client IP address
RADIUS attribute 9	Framed-IP-Netmask	Subnet mask for client IP address (DHCP option 1)
Juniper Networks VSA 26-4	Primary-DNS	Primary domain server (DHCP option 6)
Juniper Networks VSA 26-5	Secondary-DNS	Secondary domain server (DHCP option 6)
Juniper Networks VSA 26-6	Primary-WINS	Primary WINS server (DHCP option 44)
Juniper Networks VSA 26-7	Secondary-WINS	Secondary WINS server (DHCP option 44)
RADIUS attribute 27	Session-Timeout	Lease time

Table 44: Information in Authentication Grant (continued)

Attribute Number	Attribute Name	Description
RADIUS attribute 88	Framed-Pool	Address assignment pool name
Juniper Networks VSA 26-109	DHCP-Guided-Relay-Server	DHCP relay server

Minimal Configuration for Clients

The extended DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:

- **router**—A router located on the client's subnet. This statement is the equivalent of DHCP option 3.
- **domain name**—The name of the domain in which the client searches 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.
- **domain name server**—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

DHCP Local Server and Address-Assignment Pools

In the traditional DHCP server operation, the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in external address-assignment pools (external to the DHCP local server). The external address-assignment pools are managed by the **authd** process, independently of the DHCP local server, and can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients.

NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

Configuring the Router as an Extended DHCP Local Server

You can enable the router to function as an extended DHCP local server and configure the extended DHCP local server options on the router. The extended DHCP local server provides an IP address and other configuration information in response to a client request.

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients. See *Address-Assignment Pool Configuration Overview* for details about creating and using address-assignment pools.

NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

You cannot configure the extended DHCP local server and extended DHCP relay on the same interface.

To configure the extended DHCP local server on the router, include the **dhcp-local-server** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
dhcp-local-server {
  authentication {
    password password-string;
    username-include {
```

```
        circuit-type;
        delimiter delimiter-character;
        domain-name domain-name-string;
        logical-system-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        routing-instance-name;
        user-prefix user-prefix-string;
      }
    }
    group group-name {
      authentication {
        password password-string;
        username-include {
          circuit-type;
          delimiter delimiter-character;
          domain-name domain-name-string;
          logical-system-name;
          mac-address;
          option-60;
          option-82 <circuit-id> <remote-id>;
          routing-instance-name;
          user-prefix user-prefix-string;
        }
      }
      interface interface-name <upto upto-interface-name> <exclude>;
    }
    pool-match-order {
      ip-address-first;
      option-82;
    }
}
```

You can also include these statements at the following hierarchy levels:

- **[edit logical-systems *logical-system-name* system services]**
- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services]**
- **[edit routing-instances *routing-instance-name* system services]**

In addition, you can configure tracing for DHCP local server operations by including the **traceoptions** statement at the **[edit system processes dhcp-service]** hierarchy level:

```
[edit system processes]
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  level  (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools

In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer, and the DHCP local server is configured on the router. The following steps provide a high-level description of the interaction among the DHCP local server, DHCP client, and address-assignment pools:

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber.

2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.

3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server that will grant the address and configuration information.

4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server also installs the host route and ARP entry, and then monitors the lease state.

Extended DHCP Local Server and Address-Assignment Pools

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients. See *Address-Assignment Pool Configuration Overview* for details about creating and using address-assignment pools.

NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

Methods Used by the Extended DHCP Local Server to Determine Which Address-Assignment Pool to Use

You can specify the method that the extended DHCP local server uses to determine which address-assignment pool provides the IP address and configuration for a DHCP client. By default, the server matches the IP address in the client DHCP request to the address of the address-assignment pool.

The following sections describe the methods used by the DHCP local server to determine which address-assignment pool to use:

- Matching the Client IP Address to the Address-Assignment Pool on page 570
- Matching Option 82 Information to Named Address Ranges on page 570

Matching the Client IP Address to the Address-Assignment Pool

In the default configuration, the server selects the address-assignment pool to use by matching the IP address in the client DHCP request with the network address of the address-assignment pool. If the client request contains the gateway IP address (giaddr), the local server matches the giaddr to the address-assignment pool's address. If there is no giaddr in the request, the DHCP local server matches the IP address of the receiving interface to the address of the address-assignment pool.

Matching Option 82 Information to Named Address Ranges

You can also configure the extended DHCP local server to match the DHCP relay agent information option (option 82) in the client DHCP packets to a named range in the address-assignment pool used for the client. Named ranges are subsets within the overall address-assignment pool address range, and are configured when you create the address-assignment pool. To use the DHCP local server option 82 matching feature, you must ensure that the **option-82** statement is included in the **dhcp-attributes** statement for the address-assignment pool.

NOTE: To enable the option 82 matching method, you must first specify the **ip-address-first** statement in the **pool-match-order** statement, and then specify the **option-82** statement.

Default Options Provided by the Extended DHCP Server for the DHCP Client

The extended DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:

- **router**—A router located on the client's subnet. This statement is the equivalent of DHCP option 3.
- **domain name**—The name of the domain in which the client searches 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.
- **domain name server**—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

Using External AAA Authentication Services to Authenticate DHCP Clients

Both the extended DHCP local server and the extended DHCP relay agent support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. When the extended DHCP local server or relay agent receives a discover PDU from a client, the extended DHCP application contacts the AAA server to authenticate the DHCP client. The extended DHCP application can obtain client addresses and DHCP configuration options from the external AAA authentication server.

NOTE: This topic uses the term extended DHCP application to refer to both the extended DHCP local server and the extended DHCP relay agent.

The external authentication feature also supports AAA directed logout. If the external AAA service supports a user logout directive, the extended DHCP application honors the logout and views it as if it was requested by a CLI management command. All of the client state information and allocated resources are deleted at logout. The extended DHCP application supports directed logout using the list of configured authentication servers you specify with the **authentication-server** statement at the **[edit access profile *profile-name*]** hierarchy level.

Tasks for configuring External AAA authentication services are:

1. Configuring Authentication Support for an Extended DHCP Application on page 572
2. Grouping Interfaces with Common DHCP Configurations on page 573
3. Configuring Passwords for Usernames the DHCP Application Presents to the External AAA Authentication Service on page 574
4. Creating Unique Usernames the Extended DHCP Application Passes to the External AAA Authentication Service on page 574

Configuring Authentication Support for an Extended DHCP Application

To configure authentication support for an extended DHCP application, include the **authentication** statement at these hierarchy levels. You can configure either global authentication support or group-specific support.

You must configure the **username-include** statement to enable the use of authentication. The **password** statement is not required and does not cause DHCP to use authentication if the **username-include** statement is not included.

Extended DHCP local server hierarchies:

- [edit system services dhcp-local-server]
- [edit system services dhcp-local-server group *group-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*]
- [edit logical-systems *logical-system-name* system services dhcp-local-server]
- [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*]
- [edit routing-instances *routing-instance-name* system services dhcp-local-server]
- [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*]

Extended DHCP relay agent hierarchies:

- [edit forwarding-options dhcp-relay]
- [edit forwarding-options dhcp-relay group *group-name*]
- [edit logical-systems *logical-system-name* forwarding-options dhcp-relay]
- [edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name*]

- [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay]
- [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name*]

```
authentication {
  password password-string;
  username-include {
    circuit-type;
    delimiter delimiter-character;
    domain-name domain-name-string;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    routing-instance-name;
    user-prefix user-prefix-string;
  }
}
```

Grouping Interfaces with Common DHCP Configurations

The extended DHCP applications enable you to group together a set of interfaces and apply a common DHCP configuration to the named interface group.

To configure an interface group, use the **group** statement.

```
group group-name {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  interface interface-name <upto upto-interface-name> <exclude>;
}
```

You can specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the **interface *interface-name*** statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. For example:

```
group boston {
  interface 192.168.10.1;
  interface 192.168.15.5;
```

```
}
```

You can use the *upto* option to specify a range of interfaces on which the extended DHCP application is enabled. For example:

```
group quebec {
   interface 192.168.10.1 upto 192.168.10.255;
}
```

You can use the **exclude** option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
group paris {
   interface 192.168.100.1 exclude;
   interface 192.168.100.100 upto 192.168.100.125 exclude;
}
```

Configuring Passwords for Usernames the DHCP Application Presents to the External AAA Authentication Service

You can configure an optional password that the extended DHCP application presents to the external AAA authentication service to authenticate the specified username.

To configure a password that authenticates the username, use the **password** statement. For example:

```
authentication {
   password myPassworD1234;
}
```

Creating Unique Usernames the Extended DHCP Application Passes to the External AAA Authentication Service

You can configure the extended DHCP application to include additional fields in the username passed to the external AAA authentication service when the DHCP client logs in. This additional information enables you to construct usernames that uniquely identify subscribers.

NOTE: No authentication is performed if you do not include a username in the authentication configuration; however, the IP address is provided by the local pool if it is configured.

To configure unique usernames, use the **username-include** statement. You can include any or all of the additional statements.

```
authentication {
   username-include {
      circuit-type;
      delimiter delimiter-character;
```

```
    domain-name domain-name-string;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    routing-instance-name;
    user-prefix user-prefix-string;
  }
}
```

The following list describes the attributes that can be included as part of the username:

- **circuit-type**—The circuit type used by the DHCP client, for example **enet**.
- **delimiter**—The delimiter character that separates components that make up the concatenated username. The semicolon (;) is not supported as a delimiter character.
- **domain-name**—The client domain name as string. The router adds the @ delimiter to the username.
- **logical-system-name**—The name of the logical system, if the receiving interface is in a logical system.
- **mac-address**—The client MAC address, in a string of format ***xxxx.xxxx.xxxx***.
- **option-60**—The portion of the option 60 payload that follows the length field.
- **option-82 <circuit-id> <remote-id>**—The specified contents of the option 82 payload.
  - **circuit-id**—The payload of the agent circuit ID suboption.
  - **remote-id**—The payload of the Agent Remote ID suboption.
  - Both **circuit-id** and **remote-id**—The payloads of both suboptions, in the format: **circuit-id[delimiter]remote-id**.
  - Neither **circuit-id** or **remote-id**—The raw payload of the option 82 from the PDU is concatenated to the username.
- **routing-instance-name**—The name of the routing instance, if the receiving interface is in a routing instance.
- **user-prefix**—A string indicating the user prefix.

The router creates the unique username by including the specified additional information in the following order, with the fields separated by a delimiter. The default delimiter is a period (.). You can specify a different delimiter; however, the semicolon character (;) is not allowed.

```
user-prefix[delimiter]mac-address[delimiter]logical-system-name[delimiter]
routing-instance-name[delimiter]circuit-type[delimiter]option-82[delimiter]
option-60@domain-name
```

The following example shows a sample configuration that creates a unique username. The username is shown after the configuration.

```
authentication {
   username-include {
      circuit-type;
      domain-name isp55.com;
      mac-address;
      user-prefix wallybrown;
   }
}
```

The resulting unique username is:

```
wallybrown.0090.1a01.1234.enet@isp55.com
```

Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client

When the extended DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet mask. The extended DHCP application uses the information from the authentication grant for the response the DHCP application sends to the DHCP client. The DHCP application can either send the information in its original form or the application might merge the information with local configuration specifications. For example, if the authentication grant includes an address pool name and a local configuration specifies DHCP attributes for that pool, the extended DHCP application merges the authentication results and the attributes in the reply that the server sends to the client.

A local configuration is optional—a client can be fully configured by the external authentication service. However, if the external authentication service does not provide client configuration, you must configure the local address assignment pool to provide the configuration for the client. When a local configuration specifies options, the extended DHCP application adds the local configuration options to the offer PDU the server sends to the client. If the two sets of options overlap, the options in the authentication response from the external service take precedence.

When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. The following list shows the information that RADIUS might include in the authentication grant. See *RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework* for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management.

- Client IP address—RADIUS attribute 8, Framed-IP-Address
- Subnet mask for client IP address (DHCP option 1)—RADIUS attribute 9, Framed-IP-Netmask
- Primary domain server (DHCP option 6)—VSA 26-4, Primary-DNS
- Secondary domain server (DHCP option 6)—VSA 26-5 Secondary-DNS

- Primary WINS server (DHCP option 44)—VSA 26-6, Primary-WINS
- Secondary WINS server (DHCP option 44)—VSA 26-7, Secondary-WINS
- Address assignment pool name—RADIUS attribute 88, Framed-Pool
- Lease time—RADIUS attribute 27, Session-Timeout
- DHCP relay server—VSA 26-109, DHCP-Guided-Relay-Server

Example: Configuring the Minimum Extended DHCP Local Server Configuration

The following example shows the minimum configuration you need to use the extended DHCP local server on the router:

This example creates the server group named **group_one**, and specifies that the DHCP local server is enabled on interface **fe-0/0/2.0** within the group. The DHCP local server uses the default pool match configuration of **ip-address-first.**

```
[edit system services]
dhcp-local-server {
   group group_one {
      interface fe-0/0/2.0;
   }
}
```

Example: Extended DHCP Local Server Configuration with Optional Pool Matching

The following example shows an extended DHCP local server configuration that includes optional pool matching and interface groups. This configuration specifies that the DHCP local server uses option 82 information to match the named address range for client IP address assignment. The option 82 matching must also be included in the address-assignment pool configuration.

```
[edit system services]
dhcp-local-server {
   group group_one {
      interface fe-0/0/2.0;
      interface fe-0/0/2.1;
   }
   group group_two {
      interface fe-0/0/3.0;
      interface fe-0/0/3.1;
   }
   pool-match-order {
      ip-address-first:
      option-82:
   }
}
```

Tracing Extended DHCP Local Server Operations

The extended DHCP tracing operations track the extended DHCP local server operations and record them in a log file. By default, no extended DHCP local server processes are

traced. If you include the **traceoptions** statement at the **[edit system processes dhcp-service]** hierarchy level, the default tracing behavior is the following:

- Important extended DHCP local server events are logged in a file called **jdhcpd** located in the **/var/log** directory.
- When the file **jdhcpd** reaches 128 kilobytes (KB), it is renamed **jdhcpd.0**, then **jdhcpd.1**, and so on, until there are three trace files. Then the oldest trace file (**jdhcpd.2**) is overwritten. For more information about how log files are created, see the *Junos System Log Messages Reference*.
- Log files can be accessed only by the user who configures the tracing operation.

NOTE: In software releases earlier than Junos OS 11.4, you configured tracing statements at the **[edit system services dhcp-local-server]** and **[edit forwarding-options dhcp-relay]** hierarchy levels. Starting in Junos OS Release 11.4, these statements have been deprecated and hidden in favor of a new statement at the **[edit system processes dhcp-service]** hierarchy level. The deprecated statements may be removed from a future release; we recommend that you transition to the new statement.

To trace DHCP local server operations, include the **traceoptions** statement at the **[edit system processes dhcp-service]** hierarchy level:

```
traceoptions {
   file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
   flag flag;
   level  (all | error | info | notice | verbose | warning);
   no-remote-trace;
}
```

The following topics describe the tracing operation configuration statements:

1. Configuring the Filename of the Extended DHCP Local Server Processes Log on page 578
2. Configuring the Number and Size of Extended DHCP Local Server Processes Log Files on page 579
3. Configuring Access to the Log File on page 579
4. Configuring a Regular Expression for Lines to Be Logged on page 579
5. Configuring Trace Option Flags on page 580

Configuring the Filename of the Extended DHCP Local Server Processes Log

By default, the name of the file that records trace output is **jdhcpd**. You can specify a different name by including the **file** statement at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-servicetraceoptions]
file filename;
```

Configuring the Number and Size of Extended DHCP Local Server Processes Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed **jdhcpd.0**, then **jdhcpd.1**, and so on, until there are three trace files. Then the oldest trace file (**jdhcpd.2**) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracking operation (**jdhcpd**) reaches 2 MB, **jdhcpd** is renamed **jdhcpd.0**, and a new file called **jdhcpd** is created. When the new **jdhcpd** reaches 2 MB, **jdhcpd.0** is renamed **jdhcpd.1** and ***filename*** is renamed **jdhcpd.0**. This process repeats until there are 20 trace files. Then the oldest file (**jdhcpd.19**) is overwritten by the newest file (**jdhcpd.0**).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10KB through 1 gigabyte (GB).

Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the **file world-readable** statement at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename world-readable;
```

To set the default behavior explicitly, include the **file no-world-readable** statement at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename no-world readable;
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operations output includes all lines relevant to the logged events.

You can refine the output by including the **match** statement at the **[edit system processes dhcp-service traceoptions]** hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system processes dhcp-service traceoptions]
file filename match regex;
```

Configuring Trace Option Flags

By default, only important events are logged. You can configure the trace operations to be logged by including extended DHCP local server tracing flags at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-service traceoptions]
flag flag;
```

You can configure the following tracing flags:

- **all**—Trace all operations.
- **auth**—Trace authentication operations.
- **database**—Trace database events.
- **fwd**—Trace firewall process events.
- **general**—Trace miscellaneous events.
- **ha**—Trace high availability-related events.
- **interface**—Trace interface operations.
- **io**—Trace I/O operations.
- **packet**—Trace packet decoding operations.
- **performance**—Trace performance measurement operations.
- **profile**—Trace profile operations.
- **rpd**—Trace routing protocol process events.
- **rtsock**—Trace routing socket operations.
- **session-db**—Trace session database operations.
- **state**—Trace changes in state.
- **statistics**—Trace baseline statistics.
- **ui**—Trace user interface operations.

Related Documentation

- Extended DHCP Local Server on Switching Devices on page 602

CHAPTER 12

DHCP for Switches

DHCP for Switches

A Dynamic Host Configuration Protocol (DHCP) server provides a framework to pass configuration information to client hosts on a TCP/IP network. A switch acting as a DHCP server can dynamically allocate IP addresses and other configuration parameters, minimizing the overhead that is required to add clients to the network. You can configure a switch either as a DHCP server or as a DHCP relay server, but not both. for more information, read this topic.

Understanding DHCP Services for Switches

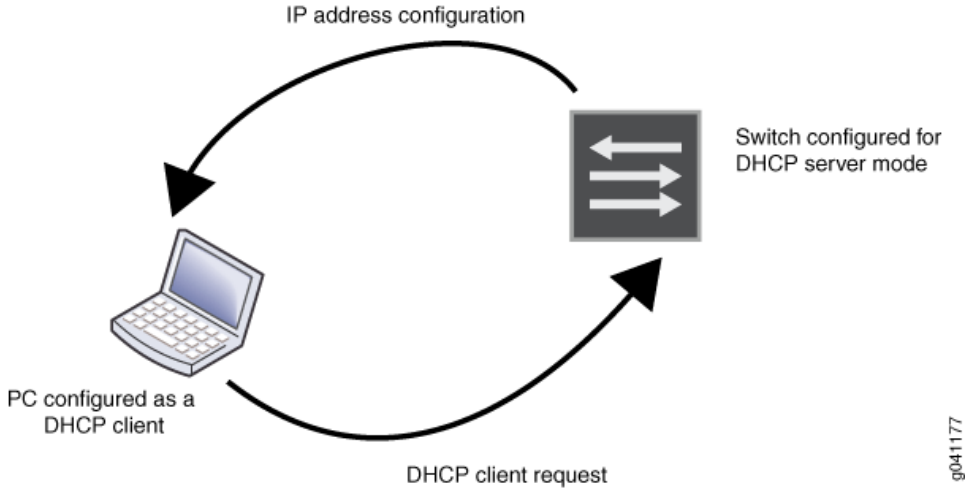
A Dynamic Host Configuration Protocol (DHCP) server on a switch can provide many valuable TCP/IP network services. For example, DHCP can dynamically allocate the four required IP parameters to each computer on the LAN: IP address, network mask, switch address, and name server address. Additionally, DHCP on the switch can automatically upgrade software on client systems.

This topic describes:

DHCP Client/Server Model

DHCP IP address allocation works on a client/server model in which the server, in this case a switch, assigns the client reusable IP information from an address pool. A DHCP client might receive offer messages from multiple DHCP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. See Figure 38 on page 582.

Figure 38: DHCP Client/Server Model



Using DHCP

DHCP automates network-parameter assignment to network devices. Even in small networks, DHCP is useful because it makes it easy to add new machines to the network.

DHCP access service minimizes the overhead required to add clients to the network by providing a centralized, server-based setup, which means that you do not have to manually create and maintain IP address assignments for clients. In addition, when you use DHCP to manage a pool of IP addresses among hosts, you reduce the number of IP addresses needed on the network. DHCP does this by leasing an IP address to a host for a limited period of time, allowing the DHCP server to share a limited number of IP addresses. DHCP also provides a central database of devices that are connected to the network and eliminates duplicate resource assignments. In addition to IP addresses for clients, DHCP provides other configuration information, particularly the IP addresses of local caching Domain Name System (DNS) resolvers, network boot servers, or other service hosts.

Another valuable DHCP feature is automatic software download for installation of software packages on switches. DHCP clients configured for automatic software download receive messages as part of the DHCP message exchange process—when the software package name in the DHCP server message is different from that of the software package that booted the DHCP client switch, the new software is downloaded and installed. See *Upgrading Software by Using Automatic Software Download for Switches*.

DHCP Relay Servers and DHCP Servers

You can configure a switch either as a DHCP server or as a DHCP relay server, but not both. Whereas a DHCP server replies to a client with an IP address, a DHCP relay server relays DHCP messages to and from the configured DHCP server, even if the client and server are on different IP networks.

Configure a switch to be a DHCP relay agent if you have locally attached hosts and a remote DHCP server.

Legacy DHCP and Extended DHCP for Server Versions

Two versions of both DHCP server and DHCP relay agent are available on EX Series, QFX Series, and OCX Series switches. The original legacy DHCP server and legacy DHCP relay agent can be used in the same network as the extended DHCP servers and extended DHCP relay agent—extended DHCP is also referred to as virtual router (VR) aware DHCP.

You cannot configure legacy DHCP and extended DHCP versions on the same switch. Because the newer extended DHCP server version has more features, we recommend that you configure the extended DHCP server if it is supported by the switch.

The extended DHCP server version has the following added features:

- Graceful Routing Engine switchover (GRES), which provides mirroring support for clients.
- Virtual routing and forwarding (VRF), which allows multiple instances of a routing table to simultaneously coexist on the same switch. For details, see *Understanding Virtual Routing Instances on EX Series Switches* .

NOTE: Legacy DHCP supports the circuit ID and the remote ID fields for the relay agent option (option 82). Extended DHCP for the relay agent option supports only circuit ID. See *EX Series Switch Software Features Overview* for a list of switches that support extended DHCP (VR-aware DHCP).

Legacy DHCP and extended DHCP servers can be configured at the hierarchy levels shown in Table 45 on page 584:

Table 45: Legacy DHCP and Extended DHCP Server Hierarchy Levels

DHCP Service	Hierarchy
Extended DHCP server	**edit system services dhcp-local-server**
Extended DHCP address pool	**edit access address-assignment pool**
Legacy DHCP server	**edit system services dhcp**
Legacy DHCP relay	**edit forwarding-options helpers bootp**
Extended DHCP relay	**edit forwarding-options dhcp-relay**
Legacy DHCP address pool	**edit system services dhcp pool**

DHCP clients on a switch are always configured at the hierarchy level **[edit interfaces *interface-name* family dhcp]**.

Configuring DHCP on a Switch

A DHCP configuration consists of two parts: the configuration for a DHCP server and the configuration for DHCP clients. The DHCP server configuration is simple if you accept the default configurations.

When you configure a legacy DHCP server, you only need to define the DHCP server name and the interface on the switch. You can use the default configuration for the rest of the settings. When you configure an extended DHCP server, you need to only define a DHCP pool, indicate IP addresses for the pool, and create a server group. You can use the default configuration for the rest of the settings.

For directions for configuring either a legacy DHCP server or an extended DHCP server, see "Configuring a DHCP Server on Switches (CLI Procedure)" on page 588.

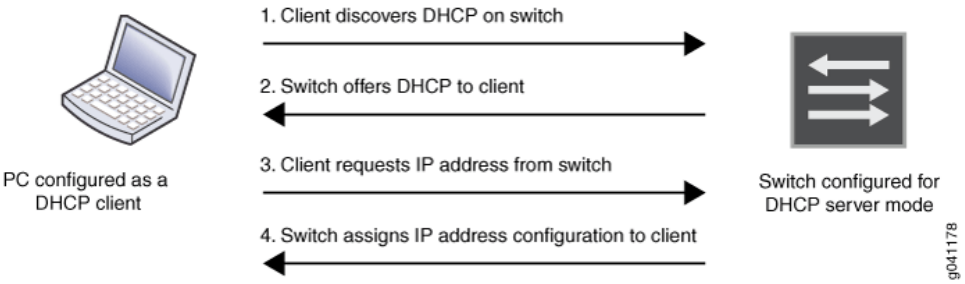
To configure a DHCP client, set the client's DHCP interface address in the **[edit interfaces interface-name unit 0 family inet dhcp]** hierarchy. For directions for configuring a DHCP client on a switch, see "Configuring a DHCP Client (CLI Procedure)" on page 591.

How DHCP Works

DHCP consists of a four-step transfer process beginning with a broadcast DHCP discovery message from the client. As the second step, the client receives a DHCP offer message

from the server. This message includes the IP address and mask, and some other specific parameters. The client then sends a DHCP request message to accept the IP address and other parameters that it received from the server in the previous step. The DHCP server sends a DHCP response message and removes the now-allocated address from the DHCP address pool. See Figure 39 on page 585.

Figure 39: DHCP Four-Step Transfer



NOTE: Because the DHCP discovery message from the client is a broadcast message and because broadcast messages cross other segments only when they are explicitly routed, you might have to configure a DHCP relay agent on the switch interface so that all DHCP discovery messages from the clients are forwarded to one DHCP server.

See Also

- *Upgrading Software by Using Automatic Software Download for Switches*

Configuring a Switch as a DHCP Server (CLI Procedure)

NOTE: This topic applies to Junos OS for EX Series switches and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Configuring a DHCP Server on Switches (CLI Procedure)" on page 588. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

A Dynamic Host Configuration Protocol (DHCP) server provides a framework to pass configuration information to client hosts on a TCP/IP network. A switch acting as a DHCP server can dynamically allocate IP addresses and other configuration parameters, minimizing the overhead that is required to add clients to the network.

A DHCP configuration consists of two components—an optional reconfiguration of default settings on DHCP clients and the configuration of a DHCP server. This topic covers configuration of the switch as a local DHCP server using DHCP for IPv4 (DHCPv4). For information about DHCPv6 local server, see "DHCPv6 Local Server Overview" on page 613.

This topic describes the following task:

1. Configuring the Switch as a Local DHCP Server on page 586

Configuring the Switch as a Local DHCP Server

To configure a switch as a local DHCP server, you must configure a DHCP address pool and indicate IP addresses for the pool. The switch, operating as the DHCP server, dynamically distributes the IP addresses from this pool. The switch can dynamically assign additional configuration parameters, such as default gateway, to provide the client with information about the network.

Multiple address pools can be configured for a DHCP server. DHCP maintains the state information about all configured pools. Clients are assigned addresses from pools with subnets that match the interface on which the DHCPDISCOVER packet sent by the client is received on the server. When more than one pool exists on the same interface, addresses are assigned on a rotating basis from all available pools.

You must ensure that you do not assign addresses that are already in use in the network to the address pools. The DHCP server does not check whether the addresses are already in use in the network before it assigns them to clients.

1. Configure a Layer 3 interface with an IP address on which the DHCP server will be reachable:

   ```
   [edit]
   user@switch# set interfaces interface-name unit unit-number family family  address
     address/prefix-length
   user@switch# set vlans vlan-name vlan-id vlan-id
   user@switch# set vlans vlan-name l3-interface irb-name
   user@switch# set interfaces irb-name family family address address/prefix-length
   ```

   For example:

   ```
   [edit]
   user@switch# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.1/24
   user@switch# set vlans server vlan-id 301
   user@switch# set vlans server l3-interface irb.301
   user@switch# set interfaces irb.301 family inet address 192.0.2.2/24
   ```

2. Configure the DHCP server for the Layer 3 interface:

   ```
   [edit]
   user@switch# set system services dhcp-local-server group-name interface
     interface-name
   ```

   For example:

   ```
   [edit]
   user@switch# set system services dhcp-local-server group server1 interface ge-0/0/1
   user@switch# set system services dhcp-local-server group server1 interface irb.301
   ```

3. Create an address pool for IPv4 addresses that can be assigned to clients. The addresses in the pool must be on the subnet in which the DHCP clients reside. Do not include addresses that are already in use on the network.

```
[edit]
user@switch# set access address-assignment pool pool-name family family network
  address/prefix-length
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet network
  198.51.100.0/24
```

4. (Optional) Define a range of addresses in the address-assignment pool. The range is a subset of addresses within the pool that can be assigned to clients. If no range is specified, then all addresses within the pool are available for assignment. Configure the name of the range and the lower and upper boundaries of the addresses in the range:

```
[edit]
user@switch# set access address-assignment pool pool-name family family range
  range-name low  low-IP-address
user@switch# set access address-assignment pool pool-name family family range
  range-name high  high-IP-address
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet range range1 low
  198.51.100.1
user@switch# set access address-assignment pool pool1 family inet range range1 high
  198.51.100.2
```

5. (Optional) Configure one or more routers as the default gateway on the client's subnet:

```
[edit]
user@switch# set access address-assignment pool pool-name family family
  dhcp-attributes router gateway-ip-address
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet dhcp-attributes
  router 198.1.1.254
```

6. (Optional) Configure the IP address that is used as the source address for the DHCP server in messages exchanged with the client. Clients use this information to distinguish between lease offers.

```
[edit]
user@switch# set access address-assignment pool pool-name family family
  dhcp-attributes server-identifier ip-address
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet dhcp-attributes
  server-identifier 198.51.100.254
```

7. (Optional) Specify the maximum time period, in seconds, that a client holds the lease for an assigned IP address if the client does not renew the lease:

```
[edit]
user@switch# set access address-assignment pool pool-name family family
  dhcp-attributes maximum-lease-time seconds
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet dhcp-attributes
  maximum-lease-time 43,200
```

8. (Optional) Specify user-defined options to be included in DHCP packets:

```
[edit]
user@switch# set access address-assignment pool pool-name family family
  dhcp-attributes option option-id-number option-type option-value
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet dhcp-attributes
  option 98 string test98
```

Configuring a DHCP Server on Switches (CLI Procedure)

NOTE: This task uses Junos OS for EX Series switches that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see "Configuring a Switch as a DHCP Server (CLI Procedure)" on page 585. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

A Dynamic Host Configuration Protocol (DHCP) server can provide two valuable TCP/IP network services. DHCP can dynamically allocate IP parameters, such as an IP address, to clients and it can also deliver software upgrades to clients.

A DHCP configuration consists of two components—an optional reconfiguration of default settings on DHCP clients and the configuration of a DHCP server. This topic covers configuration of the DHCP server. For information about reconfiguring a DHCP client, see "Configuring a DHCP Client (CLI Procedure)" on page 591.

You can configure either of two versions of a DHCP server on a switch— the extended server version or the legacy server version. We recommend that you configure the extended server unless you need to keep your DHCP server configuration backward-compatible with the legacy server version.

This topic includes the following tasks:

1. Configuring an Extended DHCP Server on a Switch on page 589
2. Configuring a Legacy DHCP Server on a Switch (CLI Procedure) on page 590

Configuring an Extended DHCP Server on a Switch

To configure an extended DHCP server, you must configure a DHCP pool, indicate IP addresses for the pool, and create a server group. Additional configurations are optional.

Do not assign addresses that are already in use in the network to address pools. The extended DHCP server does not check whether addresses are already in use before it assings them to clients.

1. Create an address pool for DHCP IP addresses:

```
[edit]
user@switch# set access address-pool address-pool
```

2. Configure an address-assignment pool that can be used by different client applications for DHCP dynamic assignment:

```
[edit access address-assignment]
user@switch# set pool address-pool-name
```

3. Create a server group on the switch, providing a group name and an interface name for DHCP:

```
[edit system services dhcp-local-server]
user@switch# set group group-name interface interface-name
```

4. (Optional) Process the information protocol data units (PDUs):

```
[edit system services dhcp-local-server]
user@switch# set overrides process-inform
```

5. (Optional) Redefine the order of attribute matching for pool selection:

```
[edit system services dhcp-local-server]
user@switch# set pool-match-order ip-address-first
```

6. (Optional) Enable dynamic reconfiguration triggered by the DHCP extended server for all DHCP clients or only for the DHCP clients serviced by the specified group of interfaces:

```
[edit system services dhcp-local-server]
user@switch# set reconfigure
```

```
[edit system services dhcp-local-server group group-name]
user@switch# set reconfigure
```

Configuring a Legacy DHCP Server on a Switch (CLI Procedure)

To configure a legacy DHCP server, you must configure a pool of IP addresses for dynamic assignment. You only need to supply a series of network addresses. Additional configurations are optional.

1. Configure a pool of IP addresses for dynamic assignment:

```
[edit system services dhcp]
user@switch# set pool network-range
```

NOTE: Step 2 through Step 15 are for assigning global values at the **[edit system services dhcp]** hierarchy level. You can also assign the same values to a specific pool by using those same commands at the **[edit system services dhcp pool *network-range*]** hierarchy level.

2. (Optional) Change the domain search list used to resolve hostnames:

```
[edit system services dhcp]
user@switch# set domain-search [ domain-list ]
```

3. (Optional) Change the domain name server (DNS) name that the DHCP server advertises to clients:

```
[edit system services dhcp]
user@switch# set name-server address
```

4. (Optional) Change the DHCP options:

```
[edit system services dhcp]
user@switch# set option id-number
```

5. (Optional) Change the devices advertised to clients:

```
[edit system services dhcp]
user@switch# set router address
```

6. (Optional) Configure the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete the DHCP setup. This configuration step is equivalent to DHCP Option 66:

```
[edit system services dhcp]
user@switch# set boot-server (address | hostname)
```

7. (Optional) 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 configuration step is equivalent to DHCP Option 67:

```
[edit system services dhcp]
user@switch# set boot-file filename
```

8. (Optional) Change the SIP server:

```
[edit system services dhcp]
user@switch# set sip-server addresses-or-names
```

For more information, see "Configuring a DHCP SIP Server (CLI Procedure)" on page 592.

9. (Optional) Change the DHCP client's hardware address:

```
[edit system services dhcp]
user@switch# set static-binding mac-address
```

10. (Optional) Change the NetBIOS name server:

```
[edit system services dhcp]
user@switch# set wins-server address
```

Configuring a DHCP Client (CLI Procedure)

A Dynamic Host Configuration Protocol (DHCP) server can provide many valuable TCP/IP network services. DHCP can dynamically allocate IP parameters, such as an IP address, to clients, and it can also deliver software upgrades to clients.

DHCP configuration consists of two components, configuration of DHCP clients and configuration of a DHCP server. Client configuration determines how clients send a message requesting an IP address, whereas a DHCP server configuration enables the server to send an IP address configuration back to the client. This topic describes configuring a DHCP client. For directions for configuring a DHCP server, see "Configuring a DHCP Server on Switches (CLI Procedure)" on page 588 or "Configuring a Switch as a DHCP Server (CLI Procedure)" on page 585.

You can change DHCP client configurations from the switch, using client identifiers to indicate which clients you want to configure.

To configure a DHCP client, you configure an interface to belong to the DHCP family and specify additional attributes, as desired:

```
[edit]
user@switch# set interfaces interface-name unit number family  inet dhcp
 configuration-statement
```

NOTE: Starting in Junos OS Release 18.1R1, DHCPv4 and DHCPv6 clients are supported on management interfaces (fxp0 and em0) configured in the non-default management routing instance, mgmt_junos.

The options that you can configure are listed in Table 46 on page 592. Replace the variable *configuration-statement* with one or more of the statements listed in this table. If you do not explicitly configure these options, the switch uses default values for them.

Table 46: DHCP Client Settings

Configuration Statement	Description
client-identifier	Unique client ID—By default this consists of the hardware type (01 for Ethernet) and the MAC address (a.b.c.d). For this example, the value would be 01abcd.
lease-time	Time in seconds that a client holds the lease for an IP address assigned by a DHCP server. If a client does not request a specific lease time, then the server sends the default lease time. The default lease time on a Junos OS DHCP server is 1 day.
retransmission-attempt	Number of times the client attempts to retransmit a DHCP packet.
retransmission-interval	Time between transmission attempts.
server-address	IP address of the server that the client queries for an IP address.
update-server	TCP/IP settings learned from an external DHCP server to the DHCP server running on the switch are propagated.
vendor-option	Vendor class ID (CPU's manufacturer ID string) for the DHCP client.

Configuring a DHCP SIP Server (CLI Procedure)

You can use the **sip-server** statement on the EX Series switch to configure option 120 on a DHCP server. The DHCP server sends configured option values—Session Initiation Protocol (SIP) server addresses or names—to DHCP clients when they request them. Previously, you were only allowed to specify a SIP server by address using **[edit system services dhcp option 120]**. You specify either an IPv4 address or a fully qualified domain name to be used by SIP clients to locate a SIP server. You cannot specify both an address and name in the same statement.

To configure a SIP server using the ***address*** option:

```
[edit system services dhcp]
```

```
user@switch# set sip-server address
```

For example, to configure one address:

```
[edit system services dhcp]
user@switch set sip-server 192.168.0.11
```

To configure a SIP server using the *name* option:

```
[edit system services dhcp]
user@switch# set sip-server name
```

For example, to configure a name:

```
[edit system services dhcp]
user@switch set sip-server abc.example.com
```

DHCP and BOOTP Relay Overview

You can configure a Juniper Networks switch to act as a Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP) relay agent. This means that if the switch receives a broadcast DHCP or BOOTP request from a locally attached host (client), it relays the message to a specified DHCP or BOOTP server. You should configure the switch to be a DHCP/BOOTP relay agent if you have locally attached hosts and a distant DHCP or BOOTP server.

You can configure the switch to use the gateway IP address (giaddr) as the source IP address of the switch for relayed DHCP packets when the switch is used as the DHCP relay agent. For information on configuring this option, see the source-address-giaddr configuration statement.

You can also use smart DHCP relay, which enables you to configure alternative IP addresses for the gateway interface so that if the server fails to reply to the requests sent from the primary gateway address, the switch can resend the requests using the alternative gateway addresses. To use this feature, you must configure a Layer 3 interface, Layer 3 subinterface, or IRB interface with multiple IP addresses and configure that interface to be a relay agent.

NOTE: Because DHCP and BOOTP messages are broadcast and are not directed to a specific server, switch, or router, Juniper switches cannot function as both a DHCP server and a DHCP/BOOTP relay agent at the same time. The Junos operating system (Junos OS) generates a commit error if both options are configured at the same time, and the commit operation does not succeed until one of the options is removed.

Configuring DHCP and BOOTP

You can configure a switch to act as a Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) server or DHCP relay agent. When a switch is a relay agent,

if a locally attached host issues a DHCP or BOOTP request as a broadcast message, the switch relays the message to a specified DHCP or BOOTP server. You should configure a switch to be a DHCP and BOOTP relay agent if you have locally attached hosts and a remote DHCP or BOOTP server.

NOTE: This task uses the Enhanced Layer 2 Software (ELS) configuration style.If your switch runs software that does not support ELS, see "Configuring DHCP and BOOTP Relay" on page 594. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

To configure a switch to be a server, use the **dhcp-local-server** statement. To configure a switch to be a relay agent, use the **dhcp-relay** statement.

If you want to enable BOOTP support when the switch is configured to be a DHCP server, enter the following statement:

```
[edit system services dhcp-local-server]
user@switch# set overrides bootp-support
```

If you want to enable BOOTP support when the switch is configured to be a DHCP relay agent, enter the following statement:

```
[edit forwarding-options dhcp-relay]
user@switch# set overrides bootp-support
```

Configuring DHCP and BOOTP Relay

You can configure the QFX Series to act as a Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) relay agent. This means that if a locally attached host can issue a DHCP or BOOTP request as a broadcast message and the switch relays the message to a specified DHCP or BOOTP server. You should configure a switch to be a DHCP and BOOTP relay agent if you have locally attached hosts and a remote DHCP or BOOTP server.

NOTE: This task uses a release of Junos OS that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see "Configuring DHCP and BOOTP" on page 593. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

If you configure a switch to be a DHCP relay agent, you can also enable smart DHCP relay, which allows you to configure alternative gateway addresses for a DHCP server so that if the server fails to reply to the requests sent using the primary gateway address, the switch can resend the requests via the alternative gateway addresses. To use this feature, you must configure a routed VLAN interface or Layer 3 logical interface with multiple IP addresses and configure that interface to be a relay agent.

- Configuring a DHCP and BOOTP Relay Agent on page 595
- Configuring DHCP Smart Relay on page 596

Configuring a DHCP and BOOTP Relay Agent

To configure a switch to act as a DHCP and BOOTP relay agent, include the **bootp** statement at the **[edit forwarding-options helpers]** hierarchy level:

```
[edit forwarding-options helpers]
bootp {
   apply-secondary-as-giaddr text-description;
   client-response-ttl number;
   description text-description;
   interface (interface-name | interface-group) {
      client-response-ttl number;
      description text-description;
      maximum-hop-count number;
      minimum-wait-time seconds;
      no-listen;
      server address
      apply-secondary-as-giaddr
   }
   maximum-hop-count number;
   minimum-wait-time seconds;
   relay-agent-option;
   server server-identifier
}
```

To include a description of the BOOTP service, DHCP service, or interface, use the **description** statement.

To configure a logical interface or a group of logical interfaces with a specific DHCP relay or BOOTP configuration, include the **interface** statement.

To stop packets from being forwarded, include the **no-listen** statement.

To set the maximum allowed number in the hops field of the BOOTP message, include the **maximum-hop-count** statement. BOOTP messages that have a larger number in the hops field than the maximum allowed are not forwarded. If you omit the **maximum-hop-count** statement, the default maximum number of hops is four.

To set the minimum allowed number of seconds in the **secs** field of the BOOTP message, include the **minimum-wait-time** statement. This setting configures a minimum number of seconds since the client sent its first BOOTP request. BOOTP messages that have a smaller number in the **secs** field than the allowed minimum are not forwarded. The default value for the minimum wait time is zero (0).

To set the IP address that specify the DHCP or BOOTP server for the router, switch, or interface, include the **server** statement. You can include multiple **server** statements.

To set an IP time-to-live (TTL) value for DHCP response packets sent to a DHCP client, include the **client-response-ttl** statement.

The following example demonstrates a BOOTP relay agent configuration.

```
user@host# show forwarding-options
helpers {
   bootp {
      description "dhcp relay agent global parameters";
      server 192.168.55.44;
      server 172.16.0.3 routing-instance c3;
      maximum-hop-count 10;
      minimum-wait-time 8;
      interface {
         xe-0/0/1 {
            description "use this info for this interface";
            server 10.10.10.10;
            server 192.168.14.14;
            maximum-hop-count 11;
            minimum-wait-time 3;
         }
         xe-0/0/2 {
            no-listen; ###ignore DHCPDISCOVER messages on this interface
         }
         all {
            description "globals apply to all other interfaces";
         }
      }
   }
}
```

See Also

- *bootp*

Configuring DHCP Smart Relay

You can use DHCP smart relay to provide redundancy and resiliency to your DHCP relay configuration. Smart relay provides additional relay functionality and requires all of the configuration settings required by DHCP relay. To use DHCP smart relay, you also need an interface with multiple IP addresses assigned to it. You can achieve this by doing either of the following tasks:

- Create a routed VLAN interface and assign at least two IP addresses to it. See *Configuring IRB Interfaces on Switches* and *Example: Configuring Routing Between VLANs on One Switch Using an IRB Interface* for information about this approach.
- Create a Layer 3 logical interface (by using VLAN tagging) and assign at least two IP addresses to it. See *Understanding Layer 3 Logical Interfaces* and *Configuring a Layer 3 Logical Interface* for information about this approach.

Once you have created an interface with multiple IP addresses, complete the smart relay configuration by entering one of the following statements:

- **set forwarding-options helpers bootp smart-relay-global**: Use this statement to enable smart relay on all the interfaces that are configured as relay agents.
- **set forwarding-options helpers bootp interface *interface-name* smart-relay-agent**: Use this statement to enable smart relay on a specific interface.

When smart relay is configured for an interface, the switch initially sends DHCP request (discover) messages out of that interface using the primary address of the interface as the gateway IP address (in the giaddr field) for the DHCP message. If no DHCP offer message is received from a server in reply, the switch allows the client to send as many as three more discover messages using the same gateway IP address. If no DHCP offer message is received after three retries, the switch resends the discover message using the alternate IP address as the gateway IP address. If you configure more than two IP addresses on the relay agent interface, the switch repeats this process until a DHCP offer message is received or all of the IP addresses have been used without success.

See Also
- *bootp*

Graceful Routing Engine Switchover for DHCP

For EX Series switches, only extended DHCP local server maintains the state of active DHCP client leases. The DHCP local server supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication. You can configure dynamic profile and authentication support on a global basis or for a specific group of interfaces. The extended DHCP local server also supports the use of Junos address-assignment pools or external authorities, such as RADIUS, to provide the client address and configuration information.

For MX Series routers, the extended DHCP local server and the DHCP relay agent applications both maintain the state of active DHCP client leases in the session database. The extended DHCP application can recover this state if the DHCP process fails or is manually restarted, thus preventing the loss of active DHCP clients in either of these circumstances. However, the state of active DHCP client leases is lost if a power failure occurs or if the kernel stops operating (for example, when the router is reloaded) on a single Routing Engine.

You can enable graceful switchover support on both EX Series switches and MX Series routers. To enable graceful switchover support for the extended DHCP local server or extended DHCP relay agent on a switch, include the **graceful-switchover** statement at the **[edit chassis redundancy]** hierarchy level. To enable graceful Routing Engine switchover support on MX Series routers, include the **graceful-switchover** statement at the **[edit chassis redundancy]** hierarchy level. You cannot disable graceful Routing Engine switchover support for the extended DHCP application when the router is configured to support graceful Routing Engine switchover.

For more information about using graceful Routing Engine switchover, see *Understanding Graceful Routing Engine Switchover*.

See Also
- Extended DHCP Local Server Overview on page 562
- Extended DHCP Relay Agent Overview on page 618
- *Unified ISSU for High Availability in Subscriber Access Networks*

Centrally Configured Opaque DHCP Options

Subscriber management (on the routers) or DHCP management (on the switches) enables you to centrally configure DHCP options on a RADIUS server and then distribute the options on a per-subscriber or per DHCP-client basis. This method results in RADIUS-sourced DHCP options—the DHCP options originate at the RADIUS server and are sent to the subscriber (or DHCP client). This differs from the traditional client-sourced method (also called DHCP-sourced) of configuring DHCP options, in which the options originate at the client and are sent to the RADIUS server. The subscriber management (DHCP management) RADIUS-sourced DHCP options are also considered to be *opaque*, because DHCP local server performs minimal processing and error checking for the DHCP options string before passing the options to the subscriber (DHCP client).

Subscriber management (or DHCP management) uses Juniper Networks VSA 26-55 (DHCP-Options) to distribute the RADIUS-sourced DHCP options. The RADIUS server includes VSA 26-55 in the Access-Accept message that the server returns during subscriber authentication or DHCP client authentication. The RADIUS server sends the Access-Accept message to the RADIUS client, and then on to DHCP local server for return to the DHCP subscriber. The RADIUS server can include multiple instances of VSA 26-55 in a single Access-Accept message. The RADIUS client concatenates the multiple instances and uses the result as a single instance.

There is no CLI configuration required to enable subscriber management (DHCP management) to use the centrally configured DHCP options—the procedure is triggered by the presence of VSA 26-55 in the RADIUS Access-Accept message.

When building the offer packet for the DHCP client, DHCP local server uses the following sequence:

1. Processes any RADIUS-configured parameters that are passed as separate RADIUS attributes; for example, RADIUS attribute 27 (Session Timeout).
2. Processes any client-sourced parameters; for example, RADIUS attributes 53 (DHCP Message Type) and 54 (Server Identifier).
3. Appends (without performing any processing) the opaque DHCP options string contained in the VSA 26-55 received from the RADIUS server.

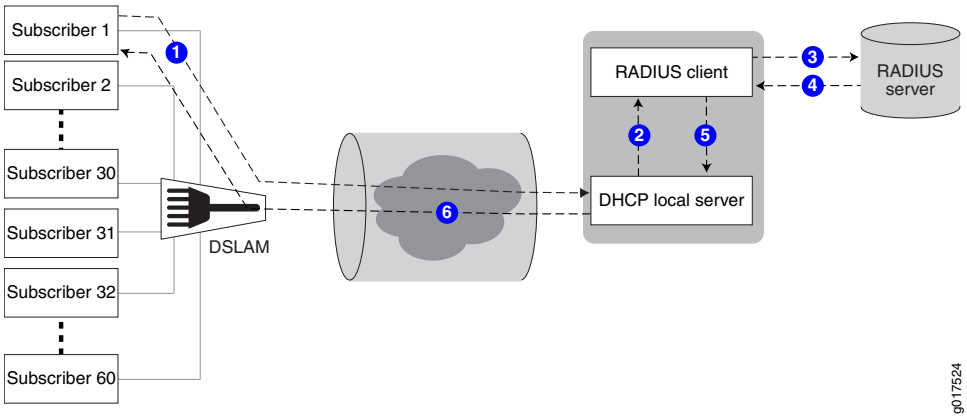
In addition to supporting central configuration of DHCP options directly on the RADIUS server (RADIUS-sourced options), subscriber management (DHCP management) also supports the traditional client-sourced options configuration, in which the router's (switch's) DHCP component sends the options to the RADIUS server. The client-sourced DHCP options method is supported for both DHCP local server and DHCP relay agent; however, the RADIUS-sourced central configuration method is supported on DHCP local server only. Both the RADIUS-sourced and client-sourced methods support DHCPv4 and DHCPv6 subscribers (clients).

NOTE: You can use the RADIUS-sourced and client-sourced methods simultaneously on DHCP local server. However, you must ensure that the central configuration method does not include options that override client-sourced DHCP options, because this can create unpredictable results.

Data Flow for RADIUS-Sourced DHCP Options

Figure 40 on page 600 shows the procedure subscriber management (DHCP management) uses when configuring DHCP options for subscribers (DHCP clients).

Figure 40: DHCP Options Data Flow



The following general sequence describes the data flow when subscriber management (DHCP management) uses RADIUS-sourced DHCP options and VSA 26-55 to configure a DHCP subscriber (client):

1. The subscriber (DHCP client) sends a DHCP discover message (or DHCPv6 solicit message) to the DHCP local server. The message includes client-sourced DHCP options.

2. The DHCP local server initiates authentication with the Junos OS RADIUS client.

3. The RADIUS client sends an Access-Request message on behalf of the subscriber (DHCP client) to the external RADIUS server. The message includes the subscriber's (DHCP client's) client-sourced DHCP options.

4. The external RADIUS server responds by sending an Access-Accept message to the RADIUS client. The Access-Accept message includes the RADIUS-sourced opaque DHCP options in VSA 26-55.

5. The RADIUS client sends the DHCP options string to DHCP local server. If there are multiple VSA 26-55 instances, the RADIUS client first assembles them into a single options string.

6. DHCP local server processes all options into the DHCP offer (or DHCPv6 reply) message, except for the RADIUS-sourced VSA 26-55 DHCP options. After processing

all other options, DHCP local server then appends the unmodified VSA 26-55 DHCP options to the message and sends the message to the subscriber (DHCP client).

7. The subscriber (DHCP client) is configured with the DHCP options.

8. The following operations occur after the subscriber (DHCP client) receives the DHCP options:

   - Accounting—The RADIUS client sends Acct-Start and Interim-Accounting requests to the RADIUS server, including the RADIUS-sourced DHCP options in VSA 26-55. By default, the DHCP options are included in accounting requests.
   - Renewal—When the subscriber (DHCP client) renews, the cached DHCP options value is returned in the DHCP renew (or DHCPv6 ACK) message. The originally assigned DHCP options cannot be modified during a renew cycle.
   - Logout—When the subscriber (DHCP client) logs out, the RADIUS client sends an Acct-Stop message to the RADIUS server, including the RADIUS-sourced VSA 26-55.

Multiple VSA 26-55 Instances Configuration

VSA 26-55 supports a maximum size of 247 bytes. If your RADIUS-sourced DHCP options field is greater than 247 bytes, you must break the field up and manually configure multiple instances of VSA 26-55 for the RADIUS server to return. When using multiple instances for an options field, you must place the instances in the packet in the order in which the fragments are to by reassembled by the RADIUS client. The fragments can be of any size of 247 bytes or less.

BEST PRACTICE: For ease of configuration and management of your DHCP options, you might want to have one DHCP option per VSA 26-55 instance, regardless of the size of the option field.

When the RADIUS client returns a reassembled opaque options field in an accounting request to the RADIUS server, the client uses 247-byte fragments. If you had originally created instances of fewer than 247 bytes, the returned fragments might not be the same as you originally configured on the RADIUS server.

NOTE: If you are configuring Steel-Belted Radius (SBR) to support multiple VSA 26-55 instances, ensure that you specify VSA 26-55 with the RO flags in the Subscriber Management RADIUS dictionary file. The R value indicates a multivalued reply attribute and the O value indicates an ordered attribute.

DHCP Options That Cannot Be Centrally Configured

Table 47 on page 602 shows the DHCP options that you must not centrally configure on the RADIUS server.

Table 47: Unsupported Opaque DHCP Options

DHCP Option	Option Name	Comments
Option 0	Pad Option	Not supported.
Option 51	IP Address Lease Time	Value is provided by RADIUS attribute 27 (Session-Timeout).
Option 52	Option Overload	Not supported.
Option 53	DHCP Message Type	Value is provided by DHCP local server.
Option 54	Server Identifier	Value is provided by DHCP local server.
Option 55	Parameter Request List	Value is provided by DHCP local server.
Option 255	End	Value is provided by DHCP local server.
–	DHCP magic cookie	Not supported.

Related Documentation

- DHCP for Routing Devices on page 541

Extended DHCP Local Server

The extended DHCP local server provides an IP address and other configuration information in response to a client request. Extended DHCP local server enhances traditional DHCP server operation by providing additional address assignment and client configuration functionality and flexibility in a subscriber-aware environment. For information, read this topic.

- Extended DHCP Local Server Overview on page 603
- Example: Minimum Extended DHCP Local Server Configuration on page 608
- Disabling Automatic Binding of Stray DHCP Requests on page 608
- Configuring a Token for DHCP Local Server Authentication on page 610
- Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure) on page 611
- Verifying and Managing DHCP Local Server Configuration on page 612

Extended DHCP Local Server Overview

Junos OS includes an extended DHCP local server that enhances traditional DHCP server operation by providing additional address assignment and client configuration functionality and flexibility in a subscriber-aware environment. The extended DHCP local server enables service providers to take advantage of external address-assignment pools and integrated RADIUS-based configuration capabilities in addition to the continued support of traditional local address pools. The address-assignment pools are considered external because they are external to the DHCP local server. The pools are managed independently of the DHCP local server, and can be shared by different client applications, such as DHCP or PPPoE access. Table 43 on page 563 provides a comparison of the extended DHCP local server and a traditional DHCP local server.

The extended DHCP local server provides an IP address and other configuration information in response to a client request. The server supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide DHCP client authentication. You can configure the dynamic profile and authentication support on a global basis or for a specific group of interfaces.

Table 48: Comparing the Extended DHCP Local Server to the Traditional DHCP Local Server

Feature	Extended DHCP Local Server	Traditional DHCP Local Server
Local address pools	X	X
External, centrally-managed address pools	X	–
Local configuration	X	X
External configuration using information from address-assignment pools or RADIUS servers	X	–
Dynamic-profile attachment	X	–
RADIUS-based subscriber authentication, and configuration using RADIUS attributes and Juniper Networks VSAs	X	–
IPv6 client support	X	–
Default minimum client configuration	X	X

You can also configure the extended DHCP local server to support IPv6 clients. Both DHCP local server and DHCPv6 local server support the specific address request feature, which enables you to assign a particular address to a client.

NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the clear dhcp server binding command before you delete the DHCP server configuration.

This overview covers:

Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools

The pattern of interaction between the DHCP local server, the DHCP client, and address-assignment pools is the same regardless of whether you are using a router or a switch. However, there are some differences in the details of usage.

- On routers—In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer or customer premises equipment (CPE), and the DHCP local server is configured on the router.
- On switches—In a typical network configuration, the DHCP client is on an access device, such as a personal computer, and the DHCP local server is configured on the switch.

The following steps provide a high-level description of the interaction among the DHCP local server, DHCP client, and address-assignment pools:

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber (or DHCP client).

2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.

3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server selected to grant the address and configuration information.

4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server also installs the host route and ARP entry, and then monitors the lease state.

Providing DHCP Client Configuration Information

When the extended DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet mask. The extended DHCP application uses the information from the authentication grant for the response the DHCP application sends to the DHCP client. The DHCP application can either send the information in its original form or the application might merge the information with local configuration specifications. For example, if the authentication grant includes an address pool name and a local configuration specifies DHCP attributes for that pool (such as, DNS server address), the extended DHCP application merges the authentication results and the attributes in the reply that the server sends to the client.

A local configuration is optional — a client can be fully configured by the external authentication service. However, if the external authentication service does not provide client configuration, you might need to configure the local address-assignment pool to provide the configuration information, such as DNS server, for the client. When a local configuration specifies options, the extended DHCP application adds the local configuration options to the offer PDU the server sends to the client. If the two sets of options overlap, the options in the authentication response from the external service take precedence.

When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. Table 44 on page 565 lists the information that RADIUS might include in the authentication grant. See *RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework* for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management or DHCP management.

Table 49: Information in Authentication Grant

Attribute Number	Attribute Name	Description
RADIUS attribute 8	Framed-IP-Address	Client IP address
RADIUS attribute 9	Framed-IP-Netmask	Subnet mask for client IP address (DHCP option 1)
Juniper Networks VSA 26-4	Primary-DNS	Primary domain server (DHCP option 6)
Juniper Networks VSA 26-5	Secondary-DNS	Secondary domain server (DHCP option 6)
Juniper Networks VSA 26-6	Primary-WINS	Primary WINS server (DHCP option 44)
Juniper Networks VSA 26-7	Secondary-WINS	Secondary WINS server (DHCP option 44)
RADIUS attribute 27	Session-Timeout	Lease time

Table 49: Information in Authentication Grant (continued)

Attribute Number	Attribute Name	Description
RADIUS attribute 88	Framed-Pool	Address assignment pool name
Juniper Networks VSA 26-109	DHCP-Guided-Relay-Server	DHCP relay server

Minimal Configuration for Clients

The extended DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:

- **router**—A router located on the client's subnet. This statement is the equivalent of DHCP option 3.
- **domain name**—The name of the domain in which the client searches 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.
- **domain name server**—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

DHCP Local Server and Address-Assignment Pools

In the traditional DHCP server operation, the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in external address-assignment pools (external to the DHCP local server). The external address-assignment pools are managed by the **authd** process, independently of the DHCP local server, and can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients.

NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

Example: Minimum Extended DHCP Local Server Configuration

This example shows the minimum configuration you need to use for the extended DHCP local server on the router or switch:

```
[edit system services]
dhcp-local-server {
   group group_one {
      interface fe-0/0/2.0;
   }
}
```

NOTE: The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.

This example creates the server group named **group_one**, and specifies that the DHCP local server is enabled on interface **fe-0/0/2.0** within the group. The DHCP local server uses the default pool match configuration of **ip-address-first.**

NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the **clear dhcp server binding** command before you delete the DHCP server configuration.

Disabling Automatic Binding of Stray DHCP Requests

DHCP requests that are received but have no entry in the database are known as stray requests. By default, DHCP relay, DHCP relay proxy, and DHCPv6 relay agent attempt to bind the requesting client by creating a database entry and forwarding the request to the DHCP server. If the server responds with an ACK, the client is bound and the ACK is forwarded to the client. If the server responds with a NAK, the database entry is deleted and the NAK is forwarded to the client. This behavior occurs regardless of whether authentication is configured.

You can override the default configuration at the global level, for a named group of interfaces, or for a specific interface within a named group. Overriding the default causes DHCP relay, DHCP relay proxy, and DHCPv6 relay agent to drop all stray requests instead of attempting to bind the clients.

NOTE: Automatic binding of stray requests is enabled by default.

- To disable automatic binding behavior, include the **no-bind-on-request** statement when you configure DHCP overrides at the global, group, or interface level.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set no-bind-on-request
```

- To override the default behavior for DHCPv6 relay agent, configure the override at the **[edit forwarding-options dhcp-relay dhcpv6]** hierarchy level.

```
[edit forwarding-options dhcp-relay dhcpv6 overrides]
user@host# set no-bind-on-request
```

The following two examples show a configuration that disables automatic binding of stray requests for a group of interfaces and a configuration that disables automatic binding on a specific interface.

To disable automatic binding of stray requests on a group of interfaces:

1. Specify the named group.

```
[edit forwarding-options dhcp-relay]
user@host# edit group boston
```

2. Specify that you want to configure overrides.

```
[edit forwarding-options dhcp-relay group boston]
user@host# edit overrides
```

3. Disable automatic binding for the group.

```
[edit forwarding-options dhcp-relay group boston overrides]
user@host# set no-bind-on-request
```

To disable automatic binding of stray requests on a specific interface:

1. Specify the named group of which the interface is a member.

```
[edit forwarding-options dhcp-relay]
user@host# edit group boston
```

2. Specify the interface on which you want to disable automatic binding.

```
[edit forwarding-options dhcp-relay group boston]
user@host# edit interface fe-1/0/1.2
```

3. Specify that you want to configure overrides.

```
[edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2]
```

```
user@host# edit overrides
```

4. Disable automatic binding on the interface.

```
[edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2 overrides]
user@host# set no-bind-on-request
```

Configuring a Token for DHCP Local Server Authentication

You can configure an authentication token to provide rudimentary protection against inadvertently instantiated DHCP servers. You can configure the local server to include a constant, unencoded token in the DHCP forcerenew message as part of the authentication option it sends to clients. If the service provider has previously configured the DHCP client with a token, then the client can compare that token against the newly received token. If the tokens do not match, the DHCP client discards the forcerenew message. This functionality corresponds to RFC 3118, *Authentication for DHCP Messages*, section 4.

(Optional) To configure the DHCP local server to include a token in the forcerenew message sent to the client, for all clients:

- Specify the token.

  For DHCPv4:

  ```
  [edit system services dhcp-local-server reconfigure]
  user@host# set token token-value
  ```

  For DHCPv6:

  ```
  [edit system services dhcp-local-server dhcpv6 reconfigure]
  user@host# set token token-value
  ```

(Optional) For only a particular group of clients:

- Specify the token.

  For DHCPv4:

  ```
  [edit system services dhcp-local-server group group-name reconfigure]
  user@host# set token token-value
  ```

  For DHCPv6:

  ```
  [edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
  user@host# set token token-value
  ```

Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure)

You can configure an EX Series switch to act as an extended DHCP relay agent. This means that a locally attached host can issue a DHCP request as a broadcast message and the switch configured for DHCP relay relays the message to a specified DHCP server. Configure a switch to be a DHCP relay agent if you have locally attached hosts and a remote DHCP server.

Before you begin:

- Ensure that the switch can connect to the DHCP server.

To configure a switch to act as an extended DHCP relay agent server:

1. Create at least one DHCP server group, which is a group of 1 through 5 DHCP server IP addresses:

```
[edit forwarding-options dhcp-relay]
user@switch# set server-group server-group-name  ip-address
```

2. Set the global active DHCP server group. The DHCP relay server relays DHCP client requests to the DHCP servers defined in the active server group:

```
[edit forwarding-options dhcp-relay]
user@switch# set active-server-group  server-group-name
```

3. Create a DHCP relay group that includes at least one interface. DHCP relay runs on the interfaces defined in DHCP groups:

```
[edit forwarding-options dhcp-relay]
user@switch# set group group-name interface  interface-name
```

4. (Optional) Configure overrides of default DHCP relay behaviors, at the global level. See the override options in the overrides statement.

```
[edit forwarding-options dhcp-relay]
user@switch# set overrides
```

5. (Optional) Configure DHCP relay to use the DHCP vendor class identifier option (option 60) in DHCP client packets, at the global level:

```
[edit forwarding-options dhcp-relay]
user@switch# set relay-option option-number 60
```

6. (Optional) Configure settings for a DHCP relay group that override the settings at the global level, using these statements:

```
[edit forwarding-options dhcp-relay group group-name]
user@switch# set active-server-group server-group-name
user@switch# set overrides
user@switch# set relay-option option-number 60
```

7. (Optional) Configure settings for a DHCP relay group interface that override the settings at the global and **group** levels, using these statements:

```
[edit forwarding-options dhcp-relay group group-name  interface interface-name]
user@switch# exclude
user@switch# set overrides
user@switch# set trace
user@switch# set upto upto-interface-name
```

See Also
- *Understanding the Extended DHCP Relay Agent for EX Series Switches*

Verifying and Managing DHCP Local Server Configuration

Purpose View or clear information about client address bindings and statistics for the extended DHCP local server.

NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the **clear dhcp server binding** command before you delete the DHCP server configuration.

Action
- To display the address bindings in the client table on the extended DHCP local server:

  ```
  user@host> show dhcp server binding routing-instance customer routing instance
  ```

- To display extended DHCP local server statistics:

  ```
  user@host> show dhcp server statistics routing-instance customer routing instance
  ```

- To clear the binding state of a DHCP client from the client table on the extended DHCP local server:

  ```
  user@host> clear dhcp server binding routing-instance customer routing instance
  ```

- To clear all extended DHCP local server statistics:

  ```
  user@host> clear dhcp server statistics routing-instance customer routing instance
  ```

Related Documentation
- Extended DHCP Local Server On Routing Devices on page 560

DHCPv6 Local Server

Junos OS device can act as a DHCPv6 server and allocates IP addresses to IPv6 clients. DHCPv6 server also delivers configuration settings to client hosts on a subnet or to the requesting devices that need an IPv6 prefix. The DHCPv6 local server sends and receives packets using the IPv6 protocol and informs IPv6 of the routing requirements of router clients. For more information, read this topic.

DHCPv6 Local Server Overview

The DHCPv6 local server is compatible with the DHCP local server and the DHCP relay agent, and can be enabled on the same interface as either the extended DHCP local server or DHCP relay agent.

The DHCPv6 local server provides many of the same features as the DHCP local server, including:

- Configuration for a specific interface or for a group of interfaces
- Site-specific usernames and passwords
- Numbered Ethernet interfaces
- Statically configured CoS and filters
- AAA directed login
- Use of the IA_NA option to assign a specific address to a client

When a DHCPv6 client logs in, the DHCPv6 local server can optionally use the AAA service framework to interact with the RADIUS server. The RADIUS server, which is configured independently of DHCP, authenticates the client and supplies the IPv6 prefix and client configuration parameters.

The client username, which uniquely identifies a subscriber or a DHCP client, must be present in the configuration in order for DHCPv6 local server to use RADIUS authentication.

You can configure DHCPv6 local server to communicate the following attributes to the AAA service framework and RADIUS at login time:

- Client username
- Client password

Based on the attributes that the DHCPv6 local server provides, RADIUS returns the information listed in Table 50 on page 614 to configure the client:

Table 50: RADIUS Attributes and VSAs for DHCPv6 Local Server

Attribute Number	Attribute Name	Description
27	Session-Timeout	Lease time, in seconds. If not supplied, the lease does not expire
123	Delegated-IPv6-Prefix	Prefix that is delegated to the client
26-143	Max-Clients-Per-Interface	Maximum number of clients allowed per interface

To configure the extended DHCPv6 local server on the router (or switch), you include the **dhcpv6** statement at the **[edit system services dhcp-local-server]** hierarchy level.

You can also include the **dhcpv6** statement at the following hierarchy levels:

- **[edit logical-systems *logical-system-name* system services dhcp-local-server]**
- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server]**
- **[edit routing-instances *routing-instance-name* system services dhcp-local-server]**

Specifying the Delegated Address Pool for IPv6 Prefix Assignment

You can explicitly specify a delegated address pool:

- On routers—Subscriber management uses the pool to assign IPv6 prefixes for subscribers. You can specify the delegated address pool globally, for a specific group of interfaces, or for a particular interface.
- On switches—DHCP management uses the pool to assign IPv6 prefixes for DHCP clients. You can specify the delegated address pool globally, for a specific group of interfaces, or for a particular interface.

NOTE: You can also use by Juniper Networks VSA 26-161 to specify the delegated address pool. The VSA-specified value always takes precedence over the **delegated-address** statement.

To configure the delegated address pool for DHCPv6 local server:

1. Specify that you want to configure override options.

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit overrides
```

2. Configure the delegated address pool.

```
[edit system services dhcp-local-server dhcpv6 overrides]
user@host# set delegated-pool paris-cable-12
```

See Also

- Overriding the Default DHCP Local Server Configuration Settings Overview on page 630
- Extended DHCP Local Server Overview on page 562
- Extended DHCP Relay Agent Overview on page 618

Preventing Binding of Clients That Do Not Support Reconfigure Messages

The DHCPv6 client and server negotiate the use of reconfigure messages. When the client can accept reconfigure messages from the server, then the client includes the Reconfigure Accept option in both solicit and request messages sent to the server.

By default, the DHCPv6 server accepts solicit messages from clients regardless of whether they support reconfiguration. You can specify that the server require clients to accept reconfigure messages. In this case, the DHCPv6 server includes the Reconfigure Accept option in both advertise and reply messages when reconfiguration is configured for the client interface. Solicit messages from nonsupporting clients are discarded and the clients are not allowed to bind.

To configure the DHCPv6 local server to bind only clients that support client-initiated reconfiguration:

- Specify strict reconfiguration.

  For all DHCPv6 clients:

  ```
  [edit system services dhcp-local-server dhcpv6 reconfigure]
  user@host# set strict
  ```

  For only a particular group of DHCPv6 clients:

  ```
  [edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
  user@host# set strict
  ```

The **show dhcpv6 server statistics** command displays a count of solicit messages that the server has discarded.

See Also

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview on page 662
- Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients on page 659

Configuring DHCPv6 Rapid Commit (MX, EX)

You can configure the DHCPv6 local server to support the DHCPv6 Rapid Commit option (DHCPv6 option 14). When rapid commit is enabled, the server recognizes the Rapid

Commit option in Solicit messages sent from the DHCPv6 client. (DHCPv6 clients are configured separately to include the DHCPv6 Rapid Commit option in the Solicit messages.) The server and client then use a two-message exchange (Solicit and Reply) to configure clients, rather than the default four-message exchange (Solicit, Advertise, Request, and Reply). The two-message exchange provides faster client configuration, and is beneficial in environments in which networks are under a heavy load.

You can configure the DHCPv6 local server to support the Rapid Commit option globally, for a specific group, or for a specific interface. By default, rapid commit support is disabled on the DHCPv6 local server.

To configure the DHCPv6 local server to support the DHCPv6 Rapid Commit option:

1. Specify that you want to configure the **overrides** options:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit overrides
```

2. Enable rapid commit support:

```
[edit system services dhcp-local-server dhcpv6 overrides]
user@host# set rapid-commit
```

See Also

- Overriding the Default DHCP Local Server Configuration Settings Overview on page 630

Verifying and Managing DHCPv6 Local Server Configuration

Purpose View or clear information about client address bindings and statistics for the DHCPv6 local server.

Action

- To display the address bindings in the client table on the DHCPv6 local server:

```
user@host> show dhcpv6 server binding
```

- To display DHCPv6 local server statistics:

```
user@host> show dhcpv6 server statistics
```

- To clear all DHCPv6 local server statistics:

```
user@host> clear dhcpv6 server binding
```

- To clear all DHCPv6 local server statistics:

```
user@host> clear dhcpv6 server statistics
```

Related Documentation

- DHCP for Switches on page 581
- Extended DHCP Local Server on page 602

Extended DHCP Relay Agent

A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server. Extended DHCP local server enhances traditional DHCP relay agent operation.

- Extended DHCP Relay Agent Overview on page 618
- Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets on page 620
- Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent on page 620
- Replacing the DHCP Relay Request and Release Packet Source Address on page 621
- Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings on page 621
- Example: Minimum JDHCP Relay Agent Configuration on page 625
- Verifying and Managing DHCP Relay Configuration on page 626
- Overriding the Default DHCP Relay Configuration Settings on page 627
- Overriding the Default DHCP Local Server Configuration Settings Overview on page 630
- Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally on page 632

Extended DHCP Relay Agent Overview

You can configure extended DHCP relay options on the router or on the switch and enable the router (or switch) to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.

DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication or DHCP client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.

NOTE: **The PTX Series Packet Transport Routers do not support authentication for DHCP relay agents.**

On the routers, you can use DHCP relay in carrier edge applications such as video/IPTV to obtain configuration parameters, including an IP address, for your subscribers.

On the switches, you can use DHCP relay to obtain configuration parameters including an IP address for DHCP clients.

NOTE: **The extended DHCP relay agent options configured with the dhcp-relay statement are incompatible with the DHCP/BOOTP relay agent options configured with the bootp statement. As a result, you cannot enable both the extended DHCP relay agent and the DHCP/BOOTP relay agent on the router at the same time.**

For information about the DHCP/BOOTP relay agent, see *Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents*.

You can also configure the extended DHCP relay agent to support IPv6 clients. See"DHCPv6 Relay Agent Overview" on page 648 for information about the DHCPv6 relay agent feature.

To configure the extended DHCP relay agent on the router (or switch), include the dhcp-relay statement at the **[edit forwarding-options]** hierarchy level.

You can also include the **dhcp-relay** statement at the following hierarchy levels:

- **[edit logical-systems *logical-system-name* forwarding-options]**
- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options]**
- **[edit routing-instances *routing-instance-name* forwarding-options]**

- Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers on page 619
- DHCP Liveness Detection on page 620

Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers

The pattern of interaction among the DCHP Relay agent, DHCP client, and DHCP servers is the same regardless of whether the software installation is on a router or a switch. However, there are some difference in the details of usage.

On routers—In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer, and the DHCP relay agent is configured on the router between the DHCP client and one or more DHCP servers.

On switches—In a typical network configuration, the DHCP client is on an access device such as a personal computer and the DHCP relay agent is configured on the switch between the DHCP client and one or more DHCP servers.

The following steps describe, at a high level, how the DHCP client, DHCP relay agent, and DHCP server interact in a configuration that includes two DHCP servers.

1. The DHCP client sends a discover packet to find a DHCP server in the network from which to obtain configuration parameters for the subscriber (or DHCP client), including an IP address.
2. The DHCP relay agent receives the discover packet and forwards copies to each of the two DHCP servers. The DHCP relay agent then creates an entry in its internal client table to keep track of the client's state.
3. In response to receiving the discover packet, each DHCP server sends an offer packet to the client. The DHCP relay agent receives the offer packets and forwards them to the DHCP client.
4. On receipt of the offer packets, the DHCP client selects the DHCP server from which to obtain configuration information. Typically, the client selects the server that offers the longest lease time on the IP address.
5. The DHCP client sends a request packet that specifies the DHCP server from which to obtain configuration information.
6. The DHCP relay agent receives the request packet and forwards copies to each of the two DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client's configuration parameters.
8. The DHCP relay agent receives the ACK packet and forwards it to the client.
9. The DHCP client receives the ACK packet and stores the configuration information.
10. If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.
11. After establishing the initial lease on the IP address, the DHCP client and the DHCP server use unicast transmission to negotiate lease renewal or release. The DHCP relay agent "snoops" on all of the packets unicast between the client and the server that pass through the router (or switch) to determine when the lease for this client has expired or been released. This process is referred to as *lease shadowing* or *passive snooping*.

DHCP Liveness Detection

Liveness detection for DHCP subscriber or DHCP client IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients are expected to respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

NOTE: DHCP liveness detection either globally or per DHCP group.

Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets

You can configure the DHCP relay agent to override the setting of the broadcast bit in DHCP request packets. DHCP relay agent then instead uses the Layer 2 unicast transmission method to send DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.

To override the default setting of the broadcast bit in DHCP request packets:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the DHCP relay agent uses the Layer 2 unicast transmission method.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set layer2-unicast-replies
```

Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent

You can configure the DHCP relay agent to change the gateway IP address (giaddr) field in packets that it forwards between a DHCP client and a DHCP server.

To overwrite the giaddr of every DHCP packet with the giaddr of the DHCP relay agent before forwarding the packet to the DHCP server:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the giaddr of DHCP packets is overwritten.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set always-write-giaddr
```

Replacing the DHCP Relay Request and Release Packet Source Address

You can configure the DHCP relay agent to replace request and release packets with the gateway IP address (giaddr) before forwarding the packet to the DHCP server.

To replace the source address with giaddr:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that you want to replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

```
[edit forwarding-options dhcp-relay overrides]
user@host# set replace-ip-source-with giaddr
```

Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings

This example shows how to configure DHCP relay agent to use DHCP option strings to selectively identify, filter, and process client traffic.

Requirements

This example uses the following hardware and software components:

- MX Series 5G Universal Routing Platforms or EX Series Switches

Before you configure DHCP relay agent selective processing support, be sure you:

- Configure DHCP relay agent.

  See "Extended DHCP Relay Agent Overview" on page 618.

- (Optional) Configure a named DHCP local server group if you want to forward client traffic to a server group.

  See "Grouping Interfaces with Common DHCP Configurations" on page 670.

Overview

In this example, you configure DHCP relay agent to use DHCP option strings in client packets to selectively identify, filter, and process client traffic. To configure selective processing, you perform the following procedures:

1. Identify the client traffic—Specify the DHCP option that DHCP relay agent uses to identify the client traffic you want to process. The option you specify matches the option in the client traffic.
2. Configure a default action—Specify the default processing action, which DHCP relay uses for identified client traffic that does not satisfy any configured match criteria.
3. Create match filters and associate an action with each filter—Specify match criteria that filter the client traffic. The criteria can be an exact match or a partial match with the option string in the client traffic. Associate a processing action with each match criterion.

Configuration

To configure DHCP relay agent selective processing based on DHCP option information, perform these tasks:

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the **[edit]** hierarchy level.

```
set forwarding-options dhcp-relay relay-option option-number 60
set forwarding-options dhcp-relay relay-option equals ascii video-gold forward-only
set forwarding-options dhcp-relay relay-option equals ascii video-bronze local-server-group
   servergroup-15
set forwarding-options dhcp-relay relay-option starts-with hexadecimal fffff
   local-server-group servergroup-east
set forwarding-options dhcp-relay relay-option default-action drop
```

Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings

Step-by-Step Procedure

To configure DHCP relay selective processing:

1. Specify that you want to configure DHCP relay agent support.

```
[edit forwarding-options]
user@host# edit dhcp-relay
```

2. Specify the DHCP option that DHCP relay agent uses to identify incoming client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option option-number 60
```

3. Configure a default action, which DHCP relay agent uses when the incoming client traffic does not satisfy any configured match criteria.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option default-action drop
```

4. Configure an exact match condition and associated action that DHCP relay uses to process the identified client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option equals ascii video-gold forward-only
```

5. Configure a second exact match condition and associated action that DHCP relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option equals ascii video-bronze local-server-group
  servergroup-15
```

6. Configure a partial match criteria and associated action that DHCP relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option starts-with hexadecimal fffff local-server-group
  servergroup-east
```

Results

From configuration mode, confirm the results of your configuration by issuing the **show** statement at the **[edit forwarding-options]** hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit forwarding-options]
user@host# show
dhcp-relay {
  relay-option {
    option-number 60;
    equals {
      ascii video-gold {
        forward-only;
      }
    }
    equals {
      ascii video-bronze {
        local-server-group servergroup-15;
      }
    }
    default-action {
```

```
        drop;
      }
      starts-with {
        hexadecimal fffff {
          local-server-group servergroup-east;
        }
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To verify the status of DHCP relay agent selective traffic processing, perform this task:

- Verifying the Status of DHCP Relay Agent Selective Traffic Processing on page 624

Verifying the Status of DHCP Relay Agent Selective Traffic Processing

Purpose Verify the DHCP relay agent selective traffic processing status.

Action Display statistics for DHCP relay agent.

```
user@host> show dhcp relay statistics
Packets dropped:
    Total                     30
    Bad hardware address      1
    Bad opcode                1
    Bad options               3
    Invalid server address    5
    No available addresses    1
    No interface match        2
    No routing instance match 9
    No valid local address    4
    Packet too short          2
    Read error                1
    Send error                1
    Option 60                 1
    Option 82                 2

Messages received:
    BOOTREQUEST               116
    DHCPDECLINE               0
    DHCPDISCOVER              11
    DHCPINFORM                0
    DHCPRELEASE               0
    DHCPREQUEST               105

Messages sent:
    BOOTREPLY                 0
    DHCPOFFER                 2
    DHCPACK                   1
    DHCPNAK                   0
    DHCPFORCERENEW            0

Packets forwarded:
    Total                     4
    BOOTREQUEST               2
    BOOTREPLY                 2
```

Meaning The **Packets forwarded** field in the **show dhcp relay statistics** command output displays the number of client packets that have been forwarded as a result of the selective traffic processing configuration. In this example, the output indicates the total number of packets that DHCP relay agent has forwarded, as well as a breakdown for the number of **BOOTREQUEST** and **BOOTREPLY** packets forwarded.

Example: Minimum JDHCP Relay Agent Configuration

This example shows the minimum configuration you need to use the extended DHCP relay agent on the router or switch:

```
[edit forwarding-options]
dhcp-relay {
  server-group {
```

```
    test 203.0.113.21;
  }
  active-server-group test;
  group all {
    interface fe-0/0/2.0;
  }
}
```

NOTE: The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.

This example creates a server group and an active server group named **test** with IP address 203.0.113.21. The DHCP relay agent configuration is applied to a group named **all**. Within this group, the DHCP relay agent is enabled on interface fe-0/0/2.0.

Verifying and Managing DHCP Relay Configuration

Purpose View or clear address bindings or statistics for DHCP relay agent clients.

Action

- To display the address bindings for DHCP relay agent clients:

  ```
  user@host> show dhcp relay binding
  ```

- To display DHCP relay agent statistics:

  ```
  user@host> show dhcp relay statistics
  ```

- To clear the binding state of DHCP relay agent clients:

  ```
  user@host> clear dhcp relay binding
  ```

- To clear all DHCP relay agent statistics:

  ```
  user@host> clear dhcp relay statistics
  ```

To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- **show dhcp relay binding routing instance** *<routing-instance name>*
- **show dhcp relay statistics routing instance** *<routing-instance name>*
- **clear dhcp relay binding routing instance** *<routing-instance name>*
- **clear dhcp relay statistics routing instance** *<routing-instance name>*

NOTE: On all SRX Series devices, DHCP relay is unable to update the binding status based on DHCP_RENEW and DHCP_RELEASE messages.

See Also
- *Minimum DHCP Relay Agent Configuration*

Overriding the Default DHCP Relay Configuration Settings

You can override the default DHCP relay configuration settings at the global level, for a named group of interfaces, or for a specific interface within a named group.

- To override global default DHCP relay agent configuration options, include the **overrides** statement and its subordinate statements at the **[edit forwarding-options dhcp-relay]** hierarchy level.
- To override DHCP relay configuration options for a named group of interfaces, include the statements at the **[edit forwarding-options dhcp-relay group *group-name*]** hierarchy level.
- To override DHCP relay configuration options for a specific interface within a named group of interfaces, include the statements at the **[edit forwarding-options dhcp-relay group *group-name* interface *interface-name*]** hierarchy level.
- To configure overrides for DHCPv6 relay at the global level, group level, or per-interface, use the corresponding statements at the **[edit forwarding-options dhcp-relay dhcpv6]** hierarchy level.

To override default DHCP relay agent configuration settings:

1. (DHCPv4 and DHCPv6) Specify that you want to configure override options.

   - DHCPv4 overrides.

     Global override:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit overrides
     ```

     Group-level override:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit group group-name overrides
     ```

     Per-interface override:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit group group-name interface interface-name overrides
     ```

   - DHCPv6 overrides.

     Global override:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit overrides
     ```

     Group-level override:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit group group-name overrides
     ```

     Per-interface override:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit group group-name interface interface-name overrides
     ```

2. (DHCPv4 only) Enable DHCP relay proxy mode.

   See "Enabling DHCP Relay Proxy Mode" on page 647.

3. (DHCPv4 only) Overwrite the giaddr in DHCP packets that the DHCP relay agent forwards.

   See "Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent" on page 620.

4. (DHCPv4 only) Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

   See "Replacing the DHCP Relay Request and Release Packet Source Address" on page 621.

5. (DHCPv4 only) Override the DHCP relay agent information option (option 82) in DHCP packets.

   See "Overriding Option 82 Information" on page 636.

6. (DHCPv4 only) Override the setting of the broadcast bit in DHCP request packets and use the Layer 2 unicast transmission method.

   See "Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets" on page 620.

7. (DHCPv4 only) Trust DHCP client packets that have a giaddr of 0 and that contain option 82 information.

   See "Enable Processing of Untrusted Packets So Option 82 Information Can Be Used" on page 642.

8. (DHCPv4 and DHCPv6) Override the maximum number of DHCP clients allowed per interface.

   See "Specifying the Maximum Number of DHCP Clients Per Interface" on page 656.

9. (DHCPv4 only) Configure client auto logout.

   See "DHCP Auto Logout Overview" on page 643.

10. (DHCPv4 and DHCPv6) Enable or disable support for DHCP snooped clients on interfaces.

    See *Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent*.

11. (DHCPv4 and DHCPv6) Delay authentication of subscribers until the DHCP client sends a Request packet.

    See the *delay-authentication*.

12. (DHCPv4 and DHCPv6) Send release messages to the DHCP server when clients are deleted.

    See "Sending Release Messages When Clients Are Deleted" on page 659.

13. (Optional) Specify that when the DHCP or DHCPv6 relay agent receives a Discover or Solicit message that has a client ID that matches the existing client entry, the relay agent deletes the existing client entry.

    See *DHCP Behavior When Renegotiating While in Bound State*.

14. (DHCPv6 only) Automatically log out existing client when new client solicits on same interface.

    See *Automatically Logging Out DHCPv6 Clients*.

15. (DHCPv4 only) Disable the DHCP relay agent on specific interfaces.

    See "Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally" on page 632.

16. (DHCPv4 and DHCPv6) Disable automatic binding of stray DHCP requests.

    See "Disabling Automatic Binding of Stray DHCP Requests" on page 608.

17. (DHCPv4 and DHCPv6) Assign a single-session DHCP dual-stack group to a specified group of subscribers. You must assign the group to both legs of the DHCP dual stack.

    See *Configuring Single-Session DHCP Dual-Stack Support*.

18. (Optional, DHCPv4 and DHCPv6l) Specify that a short lease be sent to the client.

    See *Configuring DHCP Asymmetric Leasing*.

Overriding the Default DHCP Local Server Configuration Settings Overview

Subscriber management enables you to override certain default DHCP local server configuration settings. You can override the configuration settings at the global level, for a named group of interfaces, or for a specific interface within a named group.

- To override global default DHCP local server configuration options, include the **overrides** statement and its subordinate statements at the **[edit system services dhcp-local-server]** hierarchy level.
- To override DHCP local server configuration options for a named group of interfaces, include the statements at the **[edit system services dhcp-local-server group *group-name*]** hierarchy level.
- To override DHCP local server configuration options for a specific interface within a named group of interfaces, include the statements at the **[edit system services dhcp-local-server group *group-name* interface *interface-name*]** hierarchy level.
- To configure overrides for DHCPv6 local server at the global level, group level, or per-interface, use the corresponding statements at the **[edit system services dhcp-local-server dhcpv6]** hierarchy level.

To override default DHCP local server configuration settings:

1. (DHCPv4 and DHCPv6) Specify that you want to configure override options.

   - DHCPv4 overrides.

     Global override:

     ```
     [edit system services dhcp-local-server]
     user@host# edit overrides
     ```

     Group-level override:

     ```
     [edit system services dhcp-local-server]
     user@host# edit group group-name overrides
     ```

     Per-interface override:

     ```
     [edit system services dhcp-local-server]
     user@host# edit group group-name overrides interface interface-name
     ```

     DHCPv6 overrides.

     Global override:

     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit overrides
     ```

     Group level override:

     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit group group-name overrides
     ```

     Per-interface override:

     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit group group-name overrides interface interface-name
     ```

2. (Optional) Override the maximum number of DHCP clients allowed per interface.

   See "Specifying the Maximum Number of DHCP Clients Per Interface" on page 656.

3. (Optional) Configure DHCP client auto logout.

   See "Automatically Logging Out DHCP Clients" on page 645.

4. (Optional) Enable processing of information requests from clients.

   See "Enabling Processing of Client Information Requests" on page 658.

5. (Optional) Specify that DHCP NAK and FORCERENEW messages support option 82 information.

See *Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances*.

6. (Optional, DHCPv6 only) Specify a delegated pool name to use for DHCPv6 multiple address assignment.

   See *Specifying the Delegated Address-Assignment Pool to Be Used for DHCPv6 Prefix Delegation*.

7. (Optional, DHCPv6 only) Enable DHCPv6 rapid commit support.

   See "Configuring DHCPv6 Rapid Commit (MX, EX)" on page 615.

8. (Optional, DHCPv6 only) Specify that DHCPv6 local server return DNS server addresses as IA_NA or IA_PD suboptions rather than as a global DHCPv6 option.

   See *Overriding How the DNS Server Address Is Returned in a DHCPv6 Multiple Address Environment*.

9. (Optional, DHCPv6 only) Automatically log out existing client when new client solicits on same interface.

   See *Automatically Logging Out DHCPv6 Clients*.

10. (Optional) Specify that when the DHCP or DHCPv6 local server receives a Discover or Solicit message that has a client ID that matches the existing client entry, the local server deletes the existing client entry.

    See *DHCP Behavior When Renegotiating While in Bound State*.

11. (Optional, DHCPv4 and DHCPv6) Specify that a short lease be sent to the client.

    See *Configuring DHCP Asymmetric Leasing*.

12. (Optional, DHCPv4 and DHCPv6) Specify DHCP attributes globally or for groups.

    See *Configuring DHCP Attributes for All Clients or a Group of Clients*.

13. Load balance traffic by allowing some local servers to respond to specific clients while preventing other local servers from responding immediately to these clients.

    See *Delaying DHCP Offer and Advertise Responses to Load Balance DHCP Servers*.

Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally

You can disable DHCP relay on all interfaces or a group of interfaces.

To disable DHCP relay agent:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Disable the DHCP relay agent.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set disable-relay
```

Related Documentation

- DHCP for Switches on page 581
- Extended DHCP Local Server on page 602

DHCP Relay Agent Information Option (Option 82)

The DHCP relay agent information option (option 82) enables you to include additional useful information in the client-originated DHCP packets that the DHCP relay forwards to a DHCP server. You can configure the option 82 support globally or for a named group of interfaces. For more information, read this topic.

- Using DHCP Relay Agent Option 82 Information on page 633
- How DHCP Relay Agent Uses Option 82 for Auto Logout on page 641
- Enable Processing of Untrusted Packets So Option 82 Information Can Be Used on page 642
- DHCP Auto Logout Overview on page 643
- Automatically Logging Out DHCP Clients on page 645

Using DHCP Relay Agent Option 82 Information

Subscriber management enables you to configure the DHCP relay agent to include additional option 82 information in the DHCP packets that the relay agent receives from clients and forwards to a DHCP server. The DHCP server uses the additional information to determine the IP address to assign to the client. The server might also use the information for other purposes—for example, to determine which services to grant the client, or to provide additional security against threats such as address spoofing. The DHCP server sends its reply back to the DHCP relay agent, and the agent removes the option 82 information from the message and forwards the packet to the client.

To configure support for the DHCP relay agent information option 82, you use the **relay-option-82** statement. You can configure the DHCP relay agent to include the following suboptions in the packet the relay agent sends to the DHCP server:

- Agent Circuit ID (suboption 1)—An ASCII string that identifies the interface on which the client DHCP packet is received.
- Agent Remote ID (suboption 2)—An ASCII string assigned by the DHCP relay agent that securely identifies the client.

You can configure the option 82 support globally or for a named group of interfaces.

To restore the default behavior, in which option 82 information is not inserted into DHCP packets, you use the **delete relay-option-82** statement.

NOTE: The DHCPv6 relay agent provides similar Agent Circuit ID and Agent Remote ID support for DHCPv6 clients. For DHCPv6, subscriber management uses DHCPv6 option 18 to include the circuit ID in the packets that the relay agent sends to a DHCPv6 server, and option 37 to include the remote ID in the packets. See *DHCPv6 Relay Agent Options*.

The following sections describe the option 82 operations you can configure:

- Configuring Option 82 Information on page 634
- Overriding Option 82 Information on page 636
- Including a Prefix in DHCP Options on page 637
- Including a Textual Description in DHCP Options on page 639

Configuring Option 82 Information

You use the **relay-option-82** statement to configure the DHCP relay agent to insert option 82 information in DHCP packets that the relay agent receives from clients and forwards to a DHCP server. When you configure option 82, you can include one of the suboption statements to specify the type of information you want to include in the DHCP packets. If you configure option 82 without including one of the suboption statements, the Agent Circuit ID option is included by default. Use the **circuit-id** statement to include the Agent Circuit ID (suboption 1) in the packets, or the **remote-id** statement to include the Agent Remote ID (suboption 2).

You can optionally configure DHCP relay agent to include a prefix or the interface description as part of the suboption information. If you specify the **circuit-id** or **remote-id** statement without including any of the optional **prefix**, **use-interface-description**, **use-vlan-id**, **include-irb-and-l2**, or **no-vlan-interface-name** statements, the format of the Agent Circuit ID or Agent Remote ID information for Fast Ethernet (fe), Gigabit Ethernet (ge), and integrated routing and bridging (irb) interfaces is one of the following, depending on your network configuration:

- For Fast Ethernet or Gigabit Ethernet interfaces that do not use VLANs, stacked VLANs (S-VLANs), or bridge domains:

  ```
  (fe | ge)-fpc/pic/port.subunit
  ```

  NOTE: For remote systems, the *subunit* is required and is used to differentiate an interface.

- For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs:

  ```
  (fe | ge)-fpc/pic/port:vlan-id
  ```

- For Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs:

  (fe | ge)-*fpc/pic/port*:*svlan-id-vlan-id*

NOTE: Integrated routing and bridging (IRB) provides simultaneous support for Layer 2 bridging and Layer 3 IP routing on the same interface. IRB enables you to route local packets to another routed interface or to another bridging domain that has a Layer 3 protocol configured.

The interface to bridge domain relationship might be implicit (the interface is mapped to the bridge domain by the system based on the VLAN tag) or explicit (the interface is mapped to the bridge domain by configuring it in the bridge domain definition). For the explicit case, tagging might not be relevant for the mapping.

In the case of an IRB interface, the format displays the Layer 2 interface instead of the IRB interface along with the bridge domain name. For IRB interfaces (or other pseudo devices) the default format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

  (fe | ge)-*fpc/pic/port.subunit*:*bridge-domain-name*

- IRB interfaces that use VLANs:

  (fe | ge)-*fpc/pic/port.subunit*:*vlan-name*

To include the IRB interface name with the Layer 2 interface name, configure the **include-irb-and-l2** statement. The format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

  (fe | ge)-*fpc/pic/port*:*bridge-domain-name*+irb.*subunit*

- IRB interfaces that use VLANs:

  (fe | ge)-*fpc/pic/port*:*vlan-name*+irb.*subunit*

To include only the IRB interface name without the Layer 2 interface and bridge domain or VLAN, configure the **no-vlan-interface-name** statement. The format is as follows:

irb.*subunit*

To enable insertion of option 82 information:

1. Specify that you want to configure option 82 support.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit relay-option-82
   ```

2. Configure the DHCP relay agent to insert the Agent Circuit ID suboption, the Agent Remote ID suboption, or both.

   - To insert the Agent Circuit ID:

     ```
     [edit forwarding-options dhcp-relay relay-option-82]
     user@host# set circuit-id
     ```

   - To insert the Agent Remote ID:

     ```
     [edit forwarding-options dhcp-relay relay-option-82]
     user@host# set remote-id
     ```

   - To insert both, configure both set commands.

3. (Optional) Configure a prefix that is used in the option 82 information in the DHCP packets.

   See *Including a Prefix in DHCP Options*.

4. (Optional) Configure the DHCP relay agent to include the interface's textual description instead of the interface identifier in the option 82 information.

   See *Including a Textual Description in DHCP Options*.

Overriding Option 82 Information

You can configure the DHCP relay agent to add or remove the DHCP relay agent information option (option 82) in DHCP packets.

This feature causes the DHCP relay agent to perform one of the following actions, depending on the configuration:

- If the DHCP relay agent is configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the DHCP packets and inserts the new values before forwarding the packets to the DHCP server.
- If the DHCP relay agent is not configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the packets, but does not add any new values before forwarding the packets to the DHCP server.

To override the default option 82 information in DHCP packets destined for a DHCP server:

1. Specify that you want to configure override options.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit overrides
   ```

2. Specify that the option 82 information in DHCP packets is overwritten.

   ```
   [edit forwarding-options dhcp-relay overrides]
   user@host# set always-write-option-82
   ```

Including a Prefix in DHCP Options

When you configure the DHCP relay agent to include DHCP options in the packets that the relay agent sends to a DHCP server, you can specify that the relay agent add a prefix to the DHCP option. You can add a prefix to the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

The prefix is separated from the DHCP option information by a colon (:), and it can include any combination of the **host-name**, **logical-system-name**, and **routing-instance-name** options. The DHCP relay agent obtains the values for the **host-name**, **logical-system-name**, and **routing-instance-name** as follows:

- If you include the **host-name** option, the DHCP relay agent uses the hostname of the device configured with the **host-name** statement at the **[edit system]** hierarchy level.
- If you include the **logical-system-name** option, the DHCP relay agent uses the logical system name configured with the **logical-system** statement at the **[edit logical-system]** hierarchy level.
- If you include the **routing-instance-name** option, the DHCP relay agent uses the routing instance name configured with the **routing-instance** statement at the **[edit routing-instances]** hierarchy level or at the **[edit logical-system *logical-system-name* routing-instances]** hierarchy level.

If you include the hostname and either or both of the logical system name and the routing instance name in the prefix, the hostname is followed by a forward slash (/). If you include both the logical system name and the routing instance name in the prefix, these values are separated by a semicolon (;).

The following examples show several possible formats for the DHCP option information when you specify the **prefix** statement for Fast Ethernet (fe) or Gigabit Ethernet (ge) interfaces with S-VLANs.

- If you include only the hostname in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

  ```
  hostname:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
  ```

- If you include only the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

  ```
  logical-system-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
  ```

- If you include only the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include both the hostname and the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
host-name/logical-system-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include both the logical system name and the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
logical-system-name;routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include the hostname, logical system name, and routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
host-name/logical-system-name;routing-instance-name:(fe |
  ge)-fpc/pic/port:svlan-id-vlan-id
```

For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs but not S-VLANs, only the ***vlan-id*** value appears in the DHCP option format.

(DHCPv4) To configure a prefix with the option 82 information:

1. Specify that you want to configure option 82 support.

```
[edit forwarding-options dhcp-relay]
user@host# edit relay-option-82
```

2. Configure DHCP relay agent to insert the Agent Circuit ID, the Agent Remote ID, or both.

   - To configure the Agent Circuit ID:

```
[edit forwarding-options dhcp-relay relay-option-82]
user@host# edit circuit-id
```

   - To configure the Agent Remote ID:

```
[edit forwarding-options dhcp-relay relay-option-82]
user@host# edit remote-id
```

3. Specify that the prefix be included in the option 82 information. In this example, the prefix includes the hostname and logical system name.

   - To include the prefix with the Agent Circuit ID:

```
[edit forwarding-options dhcp-relay relay-option-82 circuit-id]
user@host# set prefix host-name logical-system-name
```

   - To include the prefix with the Agent Remote ID:

```
[edit forwarding-options dhcp-relay relay-option-82 remote-id]
```

```
user@host# set prefix host-name logical-system-name
```

(DHCPv6) To use a prefix with the DHCPv6 option 18 or option 37 information:

1. Specify that you want to configure DHCPv6 relay agent support.

```
[edit forwarding-options dhcp-relay]
user@host# edit dhcpv6
```

2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.

   - To configure option 18:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

   - To configure option 37:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-remote-id
```

3. Specify that the prefix is included in the option information. In this example, the prefix includes the hostname and logical system name

   - To include the prefix with option 18:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set prefix host-name logical-system-name
```

   - To include the prefix with option 37:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set prefix host-name logical-system-name
```

Including a Textual Description in DHCP Options

By default, when DHCP relay agent inserts option information in the packets sent to a DHCP server, the options include the interface identifier. However, you can configure the DHCP relay agent to include the textual description that is configured for the interface instead of the interface identifier. You can use the textual description for either the logical interface or the device interface.

You can include the textual interface description in the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

The textual description is configured separately, using the **description** statement at the **[edit interfaces *interface-name*]** hierarchy level. If you specify that the textual description is used and no description is configured for the interface, DHCP relay defaults to using the Layer 2 interface name.

In the case of integrated routing and bridging (IRB) interfaces, the textual description of the Layer 2 interface is used instead of the textual description of the IRB interface. If there is no description configured, the Layer 2 logical interface name is used.

NOTE: For IRB interfaces, the option 82 field must be able to uniquely identify the incoming interface based on either the Agent Circuit ID or Agent Remote ID . You can modify the information in the textual interface description to match the raw IFD (physical interface without a subunit) name and configure the option 82 field to use the interface description.

You can use the textual description with the following DHCP options:

- DHCPv4 Option 82 Agent Circuit ID (suboption 1)
- DHCPv4 Option 82 Agent Remote ID (suboption 2)
- DHCPv6 Relay Agent Interface-ID (option 18)
- DHCPv6 Relay Agent Remote-ID (option 37)

(DHCPv4) To configure the DHCP relay option 82 suboption to include the textual interface description:

1. Specify that you want to configure option 82 support.

```
[edit forwarding-options dhcp-relay]
user@host# edit relay-option-82
```

2. Configure DHCP relay agent to insert the Agent Circuit ID, Agent Remote ID, or both.

```
[edit forwarding-options dhcp-relay relay-option-82]
user@host# edit circuit-id
```

3. Specify that the textual description is included in the option 82 information. In this example, the option 82 information includes the description used for the device interface.

```
[edit forwarding-options dhcp-relay relay-option-82 circuit-id]
user@host# set use-interface-description device
```

(DHCPv6) To configure the DHCPv6 option 18 or option 37 to include the textual interface description:

1. Specify that you want to configure DHCPv6 relay agent support.

```
[edit forwarding-options dhcp-relay]
user@host# edit dhcpv6
```

2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.

   - To configure option 18:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit relay-agent-interface-id
     ```

   - To configure option 37:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit relay-agent-remote-id
     ```

3. Specify that the textual description is included in the option information. In the following example, the option information includes the description used for the device interface.

   - To include the textual description in option 18:

     ```
     [edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
     user@host# set use-interface-description device
     ```

   - To include the textual description in option 37:

     ```
     [edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
     user@host# set use-interface-description device
     ```

See Also

- *Configuring Interface Description*

How DHCP Relay Agent Uses Option 82 for Auto Logout

Table 51 on page 641 indicates how the DHCP relay agent determines the option 82 value used for the client auto logout feature. Depending on the configuration settings, DHCP relay agent takes the action indicated in the right column.

Table 51: DHCP Relay Agent Option 82 Value for Auto Logout

DHCP Relay Agent Configuration Settings					
DHCP Relay Configured with Option 82	Discover Packet Contains Option 82	Override "trust-option-82"	Override "always-write-option-82"	giaddr in non-snooped packet	Action Taken
No	No	–	–	–	No secondary search performed

Table 51: DHCP Relay Agent Option 82 Value for Auto Logout (continued)

DHCP Relay Agent Configuration Settings					
DHCP Relay Configured with Option 82	Discover Packet Contains Option 82	Override "trust-option-82"	Override "always-write-option-82"	giaddr in non-snooped packet	Action Taken
No	Yes	Yes	–	–	Use option 82 from packet
No	Yes	No	–	Zero	Drop packet
No	Yes	No	–	Non-zero	Use option 82 from packet
Yes	No	–	–	–	Use configured option 82
Yes	Yes	No	–	Zero	Drop packet
Yes	Yes	No	No	Non-zero	Use option 82 from packet
Yes	Yes	No	Yes	Non-zero	Overwrite the configured option 82
Yes	Yes	Yes	No	–	Use option 82 from packet
Yes	Yes	Yes	Yes	–	Overwrite the configured option 82

Enable Processing of Untrusted Packets So Option 82 Information Can Be Used

By default, the DHCP relay agent treats client packets with a giaddr of 0 (zero) and option 82 information as if the packets originated at an untrusted source, and drops them without further processing. You can override this behavior and specify that the DHCP relay agent process DHCP client packets that have a giaddr of 0 (zero) and contain option 82 information.

To configure DHCP relay agent to trust option 82 information:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the DHCP relay agent process DHCP client packets with a giaddr of 0 and that contain option 82 information.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set trust-option-82
```

DHCP Auto Logout Overview

This topic provides an introduction to the DHCP auto logout feature and includes the following sections:

Auto Logout Overview

Auto logout is supported for DHCP local server and DHCP relay agent. It improves the efficiency of DHCP IP address assignment by allowing IP addresses to be immediately released and returned to the address pool when DHCP clients are no longer using the addresses. DHCP can then assign the addresses to other clients. Without auto logout, an IP address is blocked for the entire lease period, and DHCP must wait until the address lease time expires before reusing the address.

Auto logout is particularly useful when DHCP uses long lease times for IP address assignments and to help avoid allocating duplicate IP addresses for a single client.

For example, you might have an environment that includes set-top boxes (STB) that are often upgraded or replaced. Each time a STB is changed, the new STB repeats the DHCP discover process to obtain client configuration information and an IP address. DHCP views the new STB as a completely new client and assigns a new IP address— the previous IP address assigned to the client (the old STB) remains blocked and unavailable until the lease expires. If auto logout is configured in this situation, DHCP recognizes that the new STB is actually the same client and then immediately releases the original IP address. DHCP relay agent acts as a proxy client for auto logout and sends a DHCP release message to the DHCP server.

How DHCP Identifies and Releases Clients

The auto logout feature requires that DHCP explicitly identify clients. By default, DHCP local server and DHCP relay agent identify clients based on MAC address or Client Identifier, and subnet. However, in some cases this type of identification might not be sufficient. For example, in the previous STB example, each STB has a different MAC address, so DHCP incorrectly assumes that an upgraded or replacement STB is a new client.

In order to explicitly identify clients, auto logout uses a secondary identification method when the primary identification method is unsuccessful— the primary method is considered unsuccessful if the MAC address or Client Identifier does not match that of an existing client. Subscriber management supports two secondary identification methods that you can configure.

- Incoming interface method— DHCP views a new client connection on the interface as if it comes from the same client. DHCP deletes the existing client binding before creating a binding for the newly connected device. This method allows only one client device to connect on the interface.

  NOTE: **The incoming interface method differs from the overrides interface-client-limit 1 statement, which retains the existing binding and rejects the newly connected client.**

- Option 60 and option 82 method— DHCP considers two clients as different if they have the same option 60 and option 82 information, but different subnets.

DHCP local server and DHCP relay agent perform the following operations when auto logout is enabled and the secondary identification method identifies a duplicate client (that is, the Discover packet is from an existing client).

- DHCP local server immediately releases the existing address.
- DHCP relay agent immediately releases the existing client and then sends a DHCP release packet to the DHCP server. Sending the release packet ensures that DHCP relay and the DHCP server are synchronized.

  If the DHCP relay receives a Discover message from an existing client, the DHCP relay forwards the Discover message to the DHCP server. The DHCP relay preserves the binding if the client' s existing IP address is returned by the DHCP server. This behavior is not applicable if the proxy-mode override or client-discover-match functionality are enabled.

  NOTE: **If the DHCP relay agent is in snoop mode, DHCP relay releases the client but does not send a release packet to the DHCP server if the discover packet is for a passive client (a client added as a result of snooped packets) or if the discover packet is a snooped packet.**

Option 60 and Option 82 Requirements

DHCP local server requires that the received discover packet include both DHCP option 60 and option 82. If either option is missing, DHCP local server cannot perform the secondary identification method and auto logout is not used.

DHCP relay agent requires that the received discover packet contain DHCP option 60. DHCP relay determines the option 82 value based on the guidelines provided in "DHCP Relay Agent Option 82 Value for Auto Logout" on page 641.

Automatically Logging Out DHCP Clients

You can configure the extended DHCP local server and extended DHCP relay to automatically log out DHCP clients. Auto logout immediately releases an existing client when DHCP receives a discover packet from a client whose identity matches an existing client. DHCP then releases the existing client IP address without waiting for the normal lease expiration.

NOTE: When the existing client is released, the new client undergoes the normal authentication process. The new client might not receive the same IP address as the original client.

To configure DHCP client auto logout:

1. Specify that you want to configure override options.
   - For DHCP local server:

     ```
     [edit system services dhcp-local-server]
     user@host# edit overrides
     ```

   - For DHCP relay agent:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit overrides
     ```

2. Enable auto logout and specify the secondary identification method you want to use when the primary identification method is unsuccessful.
   - For example, to configure DHCP local server to use the incoming interface method:

     ```
     [edit system services dhcp-local-server overrides]
     user@host# set client-discover-match incoming-interface
     ```

   - For example, to configure DHCP relay agent to use the option 60 and option 82 method:

     ```
     [edit forwarding-options dhcp-relay overrides]
     user@host# set client-discover-match option60-and-option82
     ```

NOTE: If you change the auto logout configuration, existing clients continue to use the auto logout setting that was configured when they logged in. New clients use the new setting.

Related Documentation

- DHCP for Switches on page 581

DHCP Relay Proxy

A DHCP relay is transparent to DHCP clients and DHCP servers, and simply forwards messages between DHCP clients and servers. The DHCP relay agent is configured on the router or switch, which operates between the DHCP client and one or more DHCP servers. For more information, read this topic.

DHCP Relay Proxy Overview

DHCP relay proxy mode is an enhancement to extended DHCP relay. DHCP relay proxy supports all DHCP relay features while providing additional features and benefits.

Normally, extended DHCP relay operates as a helper application for DHCP operations. Except for the ability to add DHCP relay agent options and the gateway address (giaddr) to DHCP packets, DHCP relay is transparent to DHCP clients and DHCP servers, and simply forwards messages between DHCP clients and servers.

When you configure DHCP relay to operate in proxy mode, the relay is no longer transparent. In proxy mode, DHCP relay conceals DHCP server details from DHCP clients, which interact with a DHCP relay in proxy mode as though it is the DHCP server. For DHCP servers there is no change, because proxy mode has no effect on how the DHCP server interacts with the DHCP relay.

NOTE: **You cannot configure both DHCP relay proxy and extended DHCP local server on the same interface.**

Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers

The DHCP relay agent is configured on the router (or switch), which operates between the DHCP client and one or more DHCP servers.

The following steps provide a high-level description of how DHCP relay proxy interacts with DHCP clients and DHCP servers.

1. The DHCP client sends a discover packet to locate a DHCP server in the network from which to obtain configuration parameters for the subscriber.
2. The DHCP relay proxy receives the discover packet from the DHCP client and forwards copies of the packet to each supporting DHCP server. The DHCP relay proxy then creates a client table entry to keep track of the client state.
3. In response to the discover packet, each DHCP server sends an offer packet to the client, which the DHCP relay proxy receives. The DHCP relay proxy does the following:
   a. Selects the first offer received as the offer to sent to the client
   b. Replaces the DHCP server address with the address of the DHCP relay proxy

c. Forwards the offer to the DHCP client.

4. The DHCP client receives the offer from the DHCP relay proxy.
5. The DHCP client sends a request packet that indicates the DHCP server from which to obtain configuration information—the request packet specifies the address of the DHCP relay proxy.
6. The DHCP relay proxy receives the request packet and forwards copies, which include the address of selected server, to all supporting DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client configuration parameters.
8. The DHCP relay proxy receives the ACK packet, replaces the DHCP server address with its own address, and forwards the packet to the client.
9. The DHCP client receives the ACK packet and stores the configuration information.
10. If configured to do so, the DHCP relay proxy installs a host route and Address Resolution Protocol (ARP) entry for the DHCP client.
11. After the initial DHCP lease is established, the DHCP relay proxy receives all lease renewals and lease releases from the DHCP client and forwards them to the DHCP server.

Benefits of Using DHCP Relay Proxy

DHCP relay proxy provides the following benefits:

- DHCP server isolation and DoS protection—DHCP clients are unable to detect the DHCP servers, learn DHCP server addresses, or determine the number of servers that are providing DHCP support. Server isolation also provides denial-of-service (DoS) protection for the DHCP servers.
- Multiple lease offer selection—DHCP relay proxy receives lease offers from multiple DHCP servers and selects a single offer to send to the DHCP client, thereby reducing traffic in the network. Currently, the DHCP relay proxy selects the first offer received.
- Support for both numbered and unnumbered Ethernet interfaces—For DHCP clients connected through Ethernet interfaces, when the DHCP client obtains an address, the DHCP relay proxy adds an access internal host route specifying that interface as the outbound interface. The route is automatically removed when the lease time expires or when the client releases the address.
- Logical system support—DHCP relay proxy can be configured in a logical system, whereas a non-proxy mode DHCP relay cannot.

Enabling DHCP Relay Proxy Mode

You can enable DHCP relay proxy mode on all interfaces or a group of interfaces.

To enable DHCP relay proxy mode:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Enable DHCP relay proxy mode.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set proxy-mode
```

Related Documentation

- DHCP for Switches on page 581

DHCPv6 Relay Agent

The DHCP relay agent operates as the interface between DHCP clients and the server. The DHCPv6 Relay Agent relays DHCP messages between DHCPv6 clients and DHCPv6 servers in an IPv6 network. For more information, read this topic.

- DHCPv6 Relay Agent Overview on page 648
- Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets on page 649
- Verifying and Managing DHCPv6 Relay Configuration on page 650

DHCPv6 Relay Agent Overview

The DHCPv6 relay agent enhances the DHCP relay agent by providing support in an IPv6 network. The DHCPv6 relay agent passes messages between the DHCPv6 client and the DHCPv6 server, similar to the way DHCP relay agent supports an IPv4 network. DHCPv6 relay agents eliminate the necessity of having a DHCPv6 server on each physical network.

When a DHCPv6 client logs in, the DHCPv6 relay agent uses the AAA service framework to interact with the RADIUS server to provide authentication and accounting. The RADIUS server, which is configured independently of DHCP, authenticates the client and supplies the IPv6 prefix and client configuration parameters, such as session timeout and the maximum number of clients allowed per interface.

NOTE: The PTX Series Packet Transport Routers do not support authentication for DHCPv6 relay agents.

NOTE:
The following DHCPv6 functionalities are not supported on ACX Series routers:

- Subscriber authentication for DHCPv6 relay agents
- DHCP snooping
- DHCPv6 client
- Liveness detection
- Dynamic profiles
- Option 37 support for remote ID insertion
- Bidirectional Forwarding Detection (BFD) for DHCPv6 relay
- DHCPv6 relay persistence on router reboot, crash, or power failure

The DHCPv6 relay agent is compatible with the DHCP local server and the DHCP relay agent, and can be enabled on the same interface as either the DHCP local server or DHCP relay agent.

To configure the DHCPv6 relay agent on the router (or switch), you include the **dhcpv6** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level.

You can also include the **dhcpv6** statement at the following hierarchy levels:

- **[edit logical-systems *logical-system-name* forwarding-options dhcp-relay]**
- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay]**
- **[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay]**

See *DHCPv6 Monitoring and Management* for commands specific to viewing and clearing DHCPv6 bindings and statistics.

Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets

You can configure DHCPv6 relay agent to insert the DHCPv6 Interface-ID (option 18) in the packets that the relay sends to a DHCPv6 server. You can configure the option 18 support at either the DHCPv6 global or group level.

When you configure option 18 support, you can optionally include the following additional information:

- Prefix—Specify the **prefix** option to add a prefix to the interface identifier. The prefix can be any combination of hostname, logical system name, and routing instance name.
- Interface description—Specify the **use-interface-description** option to include the textual interface description instead of the interface identifier. You can include either the device interface description or the logical interface description.

- Option 82 Agent Circuit ID suboption (suboption 1)—Specify the **use-option-82** option to include the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1). This configuration is useful in a dual-stack environment, which has both DHCPv4 and DHCPv6 subscribers that reside over the same underlying logical interface. The router checks for the option 82 suboption 1 value and inserts it into the outgoing packets. If no DHCPv4 binding exists or if the binding does not have an option 82 suboption 1 value, the router sends the packets without adding an option 18.

NOTE: If you specify one of the optional configurations, and the specified information does not exist (for example, there is no interface description), DHCPv6 relay ignores the optional configuration and inserts the default interface identifier in the packets.

To insert the DHCPv6 Interface-ID option (option 18) in DHCPv6 packets:

1. Configure the DHCPv6 relay to include option 18.

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

2. (Optional) Specify the prefix to include in option 18.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set prefix prefix
```

3. (Optional) Specify that option 18 include the textual description of the interface. You can specify either the **logical** interface description or the **device** interface description.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-interface-description (logical | device)
```

4. (Optional) Specify that option 18 use the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1) value.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-option-82
```

See Also

- *Including a Prefix in DHCP Options*
- *Including a Textual Description in DHCP Options*

Verifying and Managing DHCPv6 Relay Configuration

Purpose View or clear address bindings or statistics for extended DHCPv6 relay agent clients:

Action

- To display the address bindings for extended DHCPv6 relay agent clients:

```
user@host> show dhcpv6 relay binding
```

- To display extended DHCPv6 relay agent statistics:

```
user@host> show dhcpv6 relay statistics
```

- To clear the binding state of DHCPv6 relay agent clients:

```
user@host> clear dhcpv6 relay binding
```

- To clear all extended DHCPv6 relay agent statistics:

```
user@host> clear dhcpv6 relay statistics
```

Related Documentation

- DHCP for Switches on page 581

Managing DHCP Services on Switches

Junos OS allows you to perform different types of DHCP services such as attaching dynamic profiles, using external authentication services with DHCP, specifying maximum number of clients, managing client information request messages, dynamic reconfiguration of clients and so on. For more information, read this topic.

- Using External AAA Authentication Services with DHCP on page 651
- Creating Unique Usernames for DHCP Clients on page 653
- Specifying the Maximum Number of DHCP Clients Per Interface on page 656
- DHCP Local Server Handling of Client Information Request Messages on page 657
- Enabling Processing of Client Information Requests on page 658
- Sending Release Messages When Clients Are Deleted on page 659
- Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients on page 659
- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview on page 662
- Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings on page 664
- Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 664
- Configuring Deletion of the Client When Dynamic Reconfiguration Fails on page 665
- Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 666

Using External AAA Authentication Services with DHCP

The extended DHCP local server, including DHCPv6 local server, and the extended DHCP relay agent, including DHCPv6 relay agent, support the use of external AAA authentication

services, such as RADIUS, to authenticate DHCP clients. When the extended DHCP local server or relay agent receives a discover PDU from a client, the extended DHCP application contacts the AAA server to authenticate the DHCP client. The extended DHCP application can obtain client addresses and DHCP configuration options from the external AAA authentication server.

NOTE: This section uses the term *extended DHCP application* to refer to both the extended DHCP local server and the extended DHCP relay agent.

The external authentication feature also supports AAA directed logout. If the external AAA service supports a user logout directive, the extended DHCP application honors the logout and responds as though it were requested by a CLI management command. All of the client state information and allocated resources are deleted at logout. The extended DHCP application supports directed logout using the list of configured authentication servers you specify with the **authentication-server** statement at the **[edit access profile *profile-name*]** hierarchy level.

You can configure either global authentication support or group-specific support.

You must configure the **username-include** statement to enable the use of authentication. The **password** statement is not required and does not cause DHCP to use authentication if the **username-include** statement is not included.

To configure DHCP local server and DHCP relay agent authentication support:

1. Specify that you want to configure authentication options.
   - For DHCP local server:

     ```
     [edit system services dhcp-local-server]
     user@host# edit authentication
     ```

   - For DHCP relay agent:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit authentication
     ```

   - For DHCPv6 local server:

     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit authentication
     ```

   - For DHCPv6 relay agent:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit authentication
     ```

2. (Optional) Configure a password that authenticates the username to the external authentication service.

   See *Configuring Passwords for Usernames*.

3. (Optional) Configure optional features to create a unique username.

   See "Creating Unique Usernames for DHCP Clients" on page 653.

Creating Unique Usernames for DHCP Clients

You can configure the extended DHCP application to include additional information in the username that is passed to the external AAA authentication service when the DHCP client logs in. This additional information enables you to construct usernames that uniquely identify subscribers (DHCP clients).

NOTE: If you do not include a username in the authentication configuration, the router (or switch) does not perform authentication; however, the IP address is provided by the local pool if it is configured.

When you use the DHCPv6 local server, you must configure authentication and the client username; otherwise client login fails.

The following list describes the optional information that you can include as part of the username:

- **circuit-type**—The circuit type used by the DHCP client, for example **enet**.
- **client-id**—The client identifier option (option 1). (DHCPv6 local server DHCPv6 relay agent only)
- **delimiter**—The delimiter character that separates components that make up the concatenated username. The default delimiter is a period (.). The semicolon (;) is not supported as a delimiter character.
- **domain-name**—The client domain name as a string. The router adds the @ delimiter to the username.
- **interface-description**—The description of the device (physical) interface or the logical interface.
- **interface-name**—The interface name, including the interface device and associated VLAN IDs.
- **logical-system-name**—The name of the logical system, if the receiving interface is in a logical system.
- **mac-address**—The client MAC address, in a string of the format ***xxxx.xxxx.xxxx***.

  For DHCPv6 clients, because the DHCPv6 packet format has no specific field for the client MAC address, the MAC address is derived from among several sources with the following priority:

  - Client DUID Type 1 or Type 3.
  - Option 79 (client link-layer address), if present.
  - The packet source address if the client is directly connected.
  - The link local address.

- **option-60**—The portion of the option 60 payload that follows the length field. (Not supported for DHCPv6 local server)
- **option-82 <circuit-id> <remote-id>**—The specified contents of the option 82 payload. (Not supported for DHCPv6 local server)
  - **circuit-id**—The payload of the Agent Circuit ID suboption.
  - **remote-id**—The payload of the Agent Remote ID suboption.
  - Both **circuit-id** and **remote-id**—The payloads of both suboptions, in the format: **circuit-id[delimiter]remote-id**.
  - Neither **circuit-id** or **remote-id**—The raw payload of the option 82 from the PDU is concatenated to the username.

NOTE: For DHCP relay agent, the option 82 value used in creating the username is based on the option 82 value that is encoded in the outgoing (relayed) PDU.

- **relay-agent-interface-id**—The Interface-ID option (option 18). (DHCPv6 local server or DHCPv6 relay agent only)
- **relay-agent-remote-id**—The DHCPv6 Relay Agent Remote-ID option (option 37). (DHCPv6 local server or DHCPv6 relay agent only)
- **relay-agent-subscriber-id**—(On routers only) The DHCPv6 Relay Agent Subscriber-ID option (option 38). (DHCPv6 local server or DHCPv6 relay agent only)
- **routing-instance-name**—The name of the routing instance, if the receiving interface is in a routing instance.
- **user-prefix**—A string indicating the user prefix.
- **vlan-tags**—The subscriber VLAN tags. Includes the outer VLAN tag and, if present, the inner VLAN tag. You can use this option instead of the **interface-name** option when the outer VLAN tag is unique across the system and you do not need the underlying physical interface name to be part of the format.

The router (switch) creates the unique username by including the specified additional information in the following order, with the fields separated by a delimiter.

For DHCP local server and DHCP relay agent:

```
user-prefix[delimiter]mac-address[delimiter]logical-system-name[delimiter]
routing-instance-name[delimiter]circuit-type[delimiter]interface-name[delimiter]option-82[delimiter]
option-60@domain-name
```

For DHCPv6 local server:

```
user-prefix[delimiter]mac-address[delimiter]logical-system-name[delimiter]routing-instance-name[delimiter]
circuit-type[delimiter]interface-name[delimiter]relay-agent-remote-id[delimiter]
relay-agent-subscriber-id[delimiter]relay-agent-interface-id[delimiter]client-id@domain-name
```

To configure a unique username:

1. Specify that you want to configure authentication.
   - For DHCP local server:

     ```
     [edit system services dhcp-local-server]
     user@host# edit authentication
     ```

   - For DHCPv6 local server:

     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit authentication
     ```

   - For DHCP relay agent:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit authentication
     ```

   - For DHCPv6 relay agent:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit authentication
     ```

   NOTE: You can also configure authentication and usernames for groups at additional hierarchy levels. See authentication (DHCP Local Server) and authentication (DHCP Relay Agent).

2. Specify that you want to include optional information in the username. (DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent all support the **username-include** statement.)

   ```
   [edit system services dhcp-local-server authentication]
   user@host# set username-include
   ```

3. (Optional) Specify the optional information you want to include in the username. DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent all support the **username-include** statement.

   The following sample configuration produces this unique username:

   wallybrown.00:00:5e:00:53:ff.enet@example.com

   ```
   [edit system services dhcp-local-server authentication username-include]
   user@host# set username-include circuit-type
   user@host# set username-include domain-name example.com
   user@host# set username-include mac-address
   user@host# set username-include user-prefix wallybrown
   ```

Specifying the Maximum Number of DHCP Clients Per Interface

By default, there is no limit to the number of DHCP local server or DHCP relay clients allowed on an interface. However, you can override the default setting and specify the maximum number of clients allowed per interface, in the range 1 through 500,000. When the number of clients on the interface reaches the specified limit, no additional DHCP Discover PDUs or DHCPv6 Solicit PDUs are accepted. When the number of clients subsequently drops below the limit, new clients are again accepted.

NOTE: The maximum number of DHCP (and DHCPv6) local server clients or DHCP (and DHCPv6) relay clients can also be specified by Juniper Networks VSA 26-143 during client login. The VSA-specified value always takes precedence if the **interface-client-limit** statement specifies a different number.

If the VSA-specified value differs with each client login, DHCP uses the largest limit set by the VSA until there are no clients on the interface.

To configure the maximum number of DHCP clients allowed per interface:

1. Specify that you want to configure override options.
   - For DHCP local server:

     ```
     [edit system services dhcp-local-server]
     user@host# edit overrides
     ```

   - For DHCPv6 local server:

     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit overrides
     ```

   - For DHCP relay agent:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit overrides
     ```

   - For DHCPv6 relay agent:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit overrides
     ```

2. Configure the maximum number of clients allowed per interface. (DHCP local server, DHCPv6 local server, DHCP relay agent and DHCPv6 relay agent all support the **interface-client-limit** statement.)

   ```
   [edit system services dhcp-local-server overrides]
   user@host# set interface-client-limit number
   ```

NOTE: For DHCP local server and DHCP relay agent, you can use either the **interface-client-limit** statement or the **client-discover-match incoming-interface** statement to set a limit of one client per interface. The **interface-client-limit** statement with a value of 1 retains the existing client and rejects any new client connections. The **client-discover-match incoming-interface** statement deletes the existing client and allows a new client to connect.

DHCP Local Server Handling of Client Information Request Messages

DHCP clients that already have externally provided addresses may solicit further configuration information from a DHCP server by sending a DHCP inform or DHCPv6 information-request message that indicates what information is desired. These message types can be collectively referred to as information request messages. By default, DHCP local server and DHCPv6 local server ignore any DHCP information requests that they receive. You can override this default behavior to enable processing of these messages.

If you enable processing of information requests, DHCP local server responds to the client with a DHCP acknowledgment message that includes the requested information—if it is available. DHCPv6 local server responds in the same manner but uses a DHCP reply message. No subscriber management or DHCP-management is applied as a result of the DHCP information request message.

By default, DHCP relay and DHCP relay proxy automatically forward DHCP information request messages without modification if the messages are received on an interface configured for a DHCP server group. DHCP relay and relay proxy drop information request messages received on any other interfaces. You cannot disable this default DHCP relay and relay proxy behavior.

The information requested by these clients is typically configured with the **dhcp-attributes** statement for an address pool defined by the **address-assignment pool** *pool-name* statement at the **[edit access]** hierarchy level.

When you enable processing of DHCP information requests, you can optionally specify the name of the pool from which the local server retrieves the requested configuration information for the client. If you do not do specify a local pool, then the local server requests that AAA selects and returns only the name of the relevant pool.

NOTE: PPP interfaces are not supported on EX Series switches.

When DHCPv6 is configured over PPP interfaces, the PPP RADIUS authentication data can be used to select the pool from which the response information is taken. Additionally other RADIUS attributes can also be inserted into the DHCPv6 reply message. If an overlap exists between RADIUS attributes and local pool attributes, the RADIUS values are used instead of the local configuration data. If no RADIUS information is received from the underlying PPP interface, then the behavior is the same as described previously for non-PPP interfaces.

Enabling Processing of Client Information Requests

By default, DHCP local server and DHCPv6 local server do not respond to information request (DHCP inform and DHCPv6 information-request) messages from the client. You can enable DHCP local server and DHCPv6 local server to process these messages and respond to them with an acknowledgment (ack or reply message, respectively) and the requested information.

DHCP relay agent automatically forwards the information request messages without modification to the configured server group by means of the interfaces configured for the respective server group. The messages are dropped if they are received on an unconfigured interface. DHCP relay proxy also supports forwarding these messages. You cannot disable forwarding of the information request messages.

Configure one or more local address pools if you want to use a local pool rather than one provided by AAA. See *Configuring an Address-Assignment Pool Name and Addresses*. For processing information request messages, the address configuration is not necessary. For DHCP local server, you must specify the IPv4 family; for DHCPv6 local server, you must specify the IPv6 family.

See *Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address* for details about how to configure the information sought by clients that send information request messages.

To enable processing of DHCP client information request messages:

1. Specify that you want to configure override options.
   - For DHCP local server:

     ```
     [edit system services dhcp-local-server overrides]
     user@host# set process-inform
     ```

   - For DHCPv6 local server:

     ```
     [edit system services dhcp-local-server dhcpv6 overrides]
     user@host# set process-inform
     ```

2. (Optional) Specify a pool name from which DHCP information is returned to the client.
   - For DHCP local server:

     ```
     [edit system services dhcp-local-server overrides process-inform]
     user@host# set pool pool-name
     ```

   - For DHCPv6 local server:

     ```
     [edit system services dhcp-local-server dhcpv6 overrides process-inform]
     user@host# set pool pool-name
     ```

Sending Release Messages When Clients Are Deleted

By default, when DHCP relay and relay proxy delete a client, they do not send a release message to the DHCP server. You can override the default behavior and configure DHCP relay and relay proxy to send a release message whenever they delete a client. The release message sent by DHCP relay and relay proxy includes option 82 information.

NOTE: You must include the **send-release-on-delete** statement to configure DHCP relay and relay proxy to send the release message when the **client-discover-match** statement is included.

You can use the **[edit forwarding-options dhcp-relay dhcpv6]** hierarchy level to override the default behavior for DHCPv6 relay agent.

To send a release message:

1. Specify that you want to configure override options.
   - For DHCP relay agent:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit overrides
     ```

   - For DHCPv6 relay agent:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit overrides
     ```

2. Specify that you want DHCP relay and relay proxy (or DHCPv6 relay agent) to send a release message when clients are deleted.

   ```
   [edit forwarding-options dhcp-relay overrides]
   user@host# set send-release-on-delete
   ```

Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients

Dynamic reconfiguration of clients enables the extended DHCP local server to initiate a client update without waiting for the client to initiate a request.

Default Client/Server Interaction

Typically the DHCP client initiates all of the basic DHCP client/server interactions. The DHCP server sends information to a client only in response to a request from that client. This behavior does not enable a client to be quickly updated with its network address and configuration in the event of server changes:

NOTE: Technically, the DHCP client/server interactions are the same on routers and switches. However, the primary usage of this technology on the routers is for subscriber management. The switches are not used for subscriber management. Therefore, this topic provides two sample scenarios. The actions are the same, but the implementation details are different.

- On routers—Suppose a service provider restructures its addressing scheme or changes the server IP addresses that it provided to clients. Without dynamic reconfiguration, the service provider typically clears the DHCP server binding table, but cannot inform the DHCP clients that their bindings have been cleared. Consequently, the DHCP client operates as though its IP address is still valid, but it is now unable to communicate over the access network, resulting in an outage. The DHCP local server needs to wait for the client to send a message to renew its lease or rebind to the server. In response, the server sends a NAK message to the client to force it to begin the DHCP connection process again. Alternatively, the provider can wait for customers to make a service call about the network failures and then instruct them to power cycle their customer premises equipment to reinitiate the connection. Neither of these actions is timely or convenient for customers.
- On switches—Suppose you restructure the addressing scheme or change the server IP addresses that the DHCP server provides to clients. Without dynamic reconfiguration, the network typically clears the DHCP server binding table, but cannot inform the DHCP clients that their bindings have been cleared. Consequently, the DHCP client operates as though its IP address is still valid, but it is now unable to communicate over the access network, resulting in an outage. The DHCP local server needs to wait for the client to send a message to renew its lease or rebind to the server. In response, the server sends a NAK message to the client to force it to begin the DHCP connection process again. Alternatively, you can wait for users to notify you of the network failures and then instruct them to power cycle their equipment to reinitiate the connection. Neither of these actions is timely or convenient for users.

Dynamic Client/Server Interaction for DHCPv4

Dynamic reconfiguration for DHCPv4 is available through a partial implementation of RFC 3203, *DHCP Reconfigure Extension* for DHCPv4. It enables the DHCPv4 local server to send a message to the client to force reconfiguration.

The server sends a forcerenew message to a DHCPv4 client, initiating a message exchange. In response, DHCPv4 clients that support the forcerenew message then send a lease renewal message to the server. The server rejects the lease renewal request and sends a NAK to the client, causing the client to reinitiate the DHCP connection. A successful reconnection results in the reconfiguration of the DHCP client. Only the exchange of forcerenew, renew, and NAK messages is supported from RFC 3202. DHCP relay and DHCP relay proxy do not participate in the client reconfiguration or react to forcerenew messages other than to forward them to the client.

When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfiguring state and the local server sends a forcerenew message to the client. Because the client was in the bound state before entering the

reconfiguring state, all subscriber services or DHCP-managed services, such as forwarding and statistics, continue to work. Client statistics are not maintained in the interval between a successful reconfiguration and the subsequent client binding. When the server responds to the client renewal request with a NAK, the client entry is removed from the binding table and final statistics are reported. New statistics are collected when the client sends a discover message to establish a new session.

Dynamic Client/Server Interaction for DHCPv6

Dynamic reconfiguration for DHCPv6 is available through a partial implementation of RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. It enables the DHCPv6 local server to send a message to the client to force reconfiguration.

DHCPv6 servers send reconfigure messages to DHCPv6 clients, initiating a message exchange. In response, DHCPv6 clients that support the reconfigure message transition to the renewing state and send a renew message to the server. The server returns a reply message with a lifetime of zero (0). The client transitions to the init state and sends a solicit message. The server sends an advertise message to indicate that it is available for service. The client sends a request for configuration parameters, which the server then includes in its reply. DHCP relay and DHCP relay proxy do not participate in the client reconfiguration or react to reconfigure messages other than to forward them to the client.

When a DHCPv6 server is triggered to initiate reconfiguration on a bound DHCPv6 client, the client transitions to the reconfigure state. All subscriber services, such as forwarding and statistics, continue to work. The server then sends the reconfigure message to the client. If the DHCPv6 client is already in the reconfigure state, the DHCPv6 server ignores the reconfiguration trigger. For clients in any state other than bound or reconfigure, the server clears the binding state of the client, as if the **clear dhcpv6 server binding** command had been issued.

Manually Forcing the Local Server to Initiate the Reconfiguration Process

You can force the local server to initiate the reconfiguration process for clients by issuing the **request dhcp server reconfigure** command for DHCPv4 clients, and the **request dhcpv6 server reconfigure** command for DHCPv6 clients. Command options determine whether reconfiguration is then attempted for all clients or specified clients.

Action Taken for Events That Occur During a Reconfiguration

Events that take place while a reconfiguration is in process take precedence over the reconfiguration. Table 52 on page 661 lists the actions taken in response to several different events.

Table 52: Action Taken for Events That Occur During a Reconfiguration

Event	Action
Server receives a discover (DHCPv4) or solicit (DHCPv6) message from the client.	Server drops packet and deletes client.

Table 52: Action Taken for Events That Occur During a Reconfiguration (continued)

Event	Action
Server receives a request, renew, rebind, or init-reboot message from the client.	DHCPv4—Server sends NAK message and deletes client. DHCPv6—Server drops packet and deletes client. Server replies to renew message with lease time of zero (0).
Server receives a release or decline message from the client.	Server deletes client.
The client lease times out.	Server deletes client.
The **clear dhcp server binding** command is issued.	Server deletes client.
The **request dhcp server reconfigure** (DHCPv4) or **request dhcpv6 server reconfigure** (DHCPv6) command is issued.	Command is ignored.
GRES or DHCP restart occurs.	Reconfiguration process is halted.

Benefits of Dynamic Reconfiguration of DHCP Local Server Clients

- Enable the DHCP local server to dynamically reconfigure DHCP clients, avoiding extended outages because of server configuration changes that otherwise require the server to wait for the client to renews its lease or rebind to the server.

Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview

The DHCP local server can initiate reconfiguration of its clients to avoid extended outages because of server configuration changes. You can enable dynamic reconfiguration for all DHCP clients or only the DHCP clients serviced by a specified group of interfaces, and you can modify the behavior accordingly.

Starting in Junos OS Release 14.1, you can modify the behavior of the process in which the DHCP local server initiates reconfiguration of its clients by including the appropriate configuration statements. You can provide the statements at the **[edit system services dhcp-local-server reconfigure]** hierarchy level for all DHCPv4 clients, and at the **[edit system services dhcp-local-server dhcpv6 reconfigure]** hierarchy level for all DHCPv6 clients. To override this global configuration for only the DHCP clients serviced by a specified group of interfaces, you can include the statements with different values at the **[edit system services dhcp-local-server group *group-name* reconfigure]** hierarchy level for DHCPv4 clients, and at the **[edit system services dhcp-local-server dhcpv6 group *group-name* reconfigure]** hierarchy level for DHCPv6 clients.

To configure dynamic reconfiguration of DHCP clients:

1. Enable dynamic reconfiguration with default values for all clients.

For DHCPv4:

```
[edit system services dhcp-local-server]
user@host# set reconfigure
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6]
user@host# set reconfigure
```

2. (Optional) Enable dynamic reconfiguration for only the clients serviced by a group of interfaces.

   For DHCPv4:

   ```
   [edit system services dhcp-local-server group-name]
   user@host# set reconfigure
   ```

   For DHCPv6:

   ```
   [edit system services dhcp-local-server dhcpv6 group group-name]
   user@host# set reconfigure
   ```

3. (Optional) Configure how the server attempts reconfiguration.

   See "Configuring Dynamic Reconfiguration Attempts for DHCP Clients" on page 664.

4. (Optional) Configure the response to a failed reconfiguration.

   See "Configuring Deletion of the Client When Dynamic Reconfiguration Fails" on page 665.

5. (Optional) Configure the behavior in response to a RADIUS-initiated disconnect.

   See "Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect" on page 666.

6. (Optional) Configure a token for rudimentary server authentication.

   See "Configuring a Token for DHCP Local Server Authentication" on page 610.

7. (Optional) Prevent DHCPv6 clients from binding if they do not support reconfigure messages.

   See "Preventing Binding of Clients That Do Not Support Reconfigure Messages" on page 615.

Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings

You can request that the DHCP local server initiate reconfiguration of all of clients or only specified clients.

To request reconfiguration of all clients:

- Specify the **all** option.

```
user@host> request dhcp server reconfigure all
```

You can use any of the following methods to request reconfiguration of specific clients:

- Specify the IP address of the DHCPv4 client.

```
user@host> request dhcp server reconfigure 192.168.27.3
```

- Specify the MAC address of a DHCPv4 client.

```
user@host> request dhcp server reconfigure 00:00:5E:00:53:67
```

- Specify an interface; reconfiguration is attempted for all clients on this interface.

```
user@host> request dhcp server reconfigure interface fe-0/0/0.100
```

- Specify a logical system; reconfiguration is attempted for all clients or the specified clients in this logical system.

```
user@host> request dhcp server reconfigure all logical-system ls-bldg5
```

- Specify a routing instance; reconfiguration is attempted for all clients or the specified clients in this routing instance.

```
user@host> request dhcp server reconfigure all routing-instance ri-boston
```

Configuring Dynamic Reconfiguration Attempts for DHCP Clients

You can configure how many attempts the local server makes to initiate reconfiguration of the DHCP client by sending forcerenew or reconfigure messages. You can also specify how long the server waits between attempts. By default, eight attempts are made and the initial interval is two seconds.

Each successive attempt doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.

(Optional) To configure DHCP local server reconfiguration behavior for all DHCP clients:

1. Specify the number of reconfiguration attempts.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set attempts 5
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set attempts 5
```

2. Specify the interval between reconfiguration attempts.

   For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set timeout 8
```

   For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set timeout 8
```

To override the global configuration for a particular group of clients, include the statements at the **[edit system services dhcp-local-server group *group-name* reconfigure]** hierarchy level or the **[edit system services dhcpv6 dhcp-local-server group *group-name* reconfigure]** hierarchy level.

Configuring Deletion of the Client When Dynamic Reconfiguration Fails

You can configure the local server to delete the client when the maximum number of reconfiguration attempts has been made without success. By default, the client's original configuration is restored.

(Optional) To configure the DHCP local server to delete the client when reconfiguration is not successful, for all clients:

- Specify the client deletion.

  For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set clear-on-abort
```

  For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set clear-on-abort
```

To override the global configuration for a particular group of clients, include the statement at the **[edit system services dhcp-local-server group *group-name* reconfigure]** hierarchy

level or the **[edit system services dhcpv6 dhcp-local-server group *group-name* reconfigure]** hierarchy level.

Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect

You can configure the local server to reconfigure the client when the client receives a RADIUS-initiated disconnect. By default, the client is deleted when a RADIUS-initiated disconnect is received.

(Optional) To configure the DHCP local server to reconfigure the client instead of deleting the client when a RADIUS-initiated disconnect is received, for all clients:

- Specify the RADIUS-initiated disconnect trigger.

  For DHCPv4:

  ```
  [edit system services dhcp-local-server reconfigure trigger]
  user@host# set radius-disconnect
  ```

  For DHCPv6:

  ```
  [edit system services dhcp-local-server dhcpv6 reconfigure trigger]
  user@host# set radius-disconnect
  ```

To override the global configuration for a particular group of clients, include the statement at the **[edit system services dhcp-local-server group *group-name* reconfigure trigger]** hierarchy level or the **[edit system services dhcpv6 dhcp-local-server group *group-name* reconfigure trigger]** hierarchy level.

Release History Table

Release	Description
14.1	Starting in Junos OS Release 14.1, you can modify the behavior of the process in which the DHCP local server initiates reconfiguration of its clients by including the appropriate configuration statements.

Related Documentation

- DHCP for Switches on page 581

Applying a Common DHCP Relay Agent Configuration to Groups of DHCP Servers

You can apply a common DHCP or DHCPv6 relay configuration to a set of DHCP server IP addresses configured as a server group. For this, you must configure a group of DHCP server addresses, and apply them as an active server group. For more information, read this topic.

- Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups on page 667

Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups

You can apply a common DHCP or DHCPv6 relay configuration to a set of DHCP server IP addresses configured as a server group, by specifying that group with the **active-server-group** statement globally or at the group level (configured with the group statement). When you apply the active server group at the group level, it overrides a global active server group configuration. An active server group is sometimes referred to as a trusted group of servers.

For example, you might want to direct certain DHCP clients to a different DHCP server than other clients, and you have different relay configurations for the clients. You can configure an interface group for each set of clients, specifying the DHCP relay interfaces for the group and any other relay configuration. In each of these groups, you specify an active server group to which each client groups traffic is forwarded.

To configure a group of DHCP server addresses and apply them as an active server group:

1. Specify the name of the server group.
   - For DHCPv4 servers:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# set server-group server-group-name
     ```

   - For DHCPv6 servers:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# set server-group server-group-name
     ```

2. Add the IP addresses of the DHCP servers belonging to the group.

   ```
   [edit forwarding-options dhcp-relay server-group server-group-name]
   user@host# set ip-address1
   user@host# set ip-address2
   ```

   NOTE: Starting in Junos OS Release 18.4R1, up to 32 server IP addresses are supported per DHCPv4 server group. In earlier releases, a maximum of 5 server IP addresses are supported for DHCPv4 servers. Configuring more than the maximum number of server addresses results in a commit check failure.

3. Apply the server group as an active server group.
   - For all DHCP clients, unless overridden:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# set active-server-group server-group-name
     ```

   - For a group of DHCP relay interfaces, overriding the global active server group:

```
[edit forwarding-options dhcp-relay group interface-group-name]
user@host# set active-server-group server-group-name
```

- For all DHCPv6 clients, unless overridden for a group:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# set active-server-group server-group-name
```

- For a group of DHCPv6 relay interfaces, overriding the global active server group:

```
[edit forwarding-options dhcp-relay dhcpv6 group interface-group-name]
user@host# set active-server-group server-group-name
```

Consider the following example. Three groups of DHCP server addresses are configured, Default, Campus-A, and Campus-B. The Default group is applied as the global active server group for the overall DHCP relay configuration.

The Campus-A server group is assigned as the active server group for interface group Campus-A-v10-DHCP-RELAY. DHCP traffic received on the interfaces in Campus-A-v10-DHCP-RELAY is forwarded to DHCP servers 198.51.100.100 and 198.51.100.101.

The Campus-B server group is assigned as the active server group for interface group Campus-B-v200-DHCP-RELAY. DHCP traffic received on the interfaces in Campus-B-v200-DHCP-RELAY is forwarded to DHCP servers 198.51.100.55 and 198.51.100.56.

All other DHCP traffic is forwarded to DHCP server 203.0.113.1.

```
[edit forwarding-options dhcp-relay]
#
# Server groups
user@host# set server-group Default 203.0.113.1
user@host# set server-group Campus-A 198.51.100.100
user@host# set server-group Campus-A 198.51.100.101
user@host# set server-group Campus-B 198.51.100.55
user@host# set server-group Campus-B 198.51.100.56
#
# Default server group applied globally.
user@host# set active-server-group Default
#
# Interface groups with application of active server groups
user@host# set group Campus-A-v10-DHCP-RELAY interface ge-1/1/0.1
user@host# set group Campus-A-v10-DHCP-RELAY interface ge-1/1/0.2
user@host# set group Campus-A-v10-DHCP-RELAY interface ge-1/1/0.3
user@host# set group Campus-A-v10-DHCP-RELAY active-server-group Campus-A
user@host# set group Campus-B-v200-DHCP-RELAY interface ge-2/2/0.4
user@host# set group Campus-B-v200-DHCP-RELAY interface ge-2/2/0.5
user@host# set group Campus-B-v200-DHCP-RELAY interface ge-2/1/0.6
user@host# set group Campus-B-v200-DHCP-RELAY active-server-group Campus-B
```

In some configurations, servers in an active server group maintain redundant information about the DHCP clients. If the binding server later becomes inaccessible, the client is

unable to renew the lease from that server. When the client attempts to rebind to a server, other servers in the group with the client information can reply with an ACK message. By default, instead of forwarding the ACK to the DHCP client, the relay agent drops any such ACKs that it receives from any server other than the binding server because the new server address does not match the expected server address in the DHCP client entry. Consequently the lease cannot be extended by any of the redundant servers.

Starting in Junos OS Release 16.2R1, you can enable a DHCPv4 relay agent to forward DHCP request (renew or rebind) ACKs from any server in the active server group (thus, any trusted server). The relay agent updates the client entry with the new server address. Because the servers in the group are expected to mirror the client information exactly, the lease option is expected to be the same as for the original server and the relay agent does not need to verify the lease option.

Starting in Junos OS Release 18.4R1, this capability is extended to allow a DHCP relay agent to forward DHCP information request (DHCPINFORM) ACK messages from any server in the active server group.

To enable ACK forwarding from any server in the active server group:

- Enable forwarding for the active server group.

```
[edit forwarding-options dhcp-relay active-server-group]
user@host# set allow-server-change
```

Release History Table

Release	Description
18.4R1	Starting in Junos OS Release 18.4R1
16.2R1	Starting in Junos OS Release 16.2R1

Related Documentation

- Grouping Interfaces and Applying a Common DHCP Configuration to the Group on page 669

Grouping Interfaces and Applying a Common DHCP Configuration to the Group

You use the group feature to group a set of interfaces and then apply a common DHCP configuration such as extended DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent to the named interface group. For more information, read this topic.

- Grouping Interfaces with Common DHCP Configurations on page 670
- Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces on page 670
- Configuring Group-Specific DHCP Local Server Options on page 672
- Configuring Group-Specific DHCP Relay Options on page 672

Grouping Interfaces with Common DHCP Configurations

You use the group feature to group a set of interfaces and then apply a common DHCP configuration to the named interface group. The extended DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent all support interface groups.

The following steps create a DHCP local server group; the steps are similar for the DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent.

To configure a DHCP local server interface group:

1. Specify that you want to configure DHCP local server.

```
[edit system services]
user@host# edit dhcp-local-server
```

2. Create the group and assign a name.

```
[edit system services dhcp-local-server]
user@host# edit group boston
```

3. Specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the interface ***interface-name*** statement to specify multiple interfaces within the group, but you cannot use the same interface in more than one group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1
user@host# set interface fe-1/0/1.2
```

4. (Optional) You can use the **upto** option to specify a range of interfaces for a group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9
```

5. (Optional) You can use the **exclude** option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1 upto fe-1/0/1.102
user@host# set interface fe-1/0/1.6 exclude
user@host# set interface fe-1/0/1.70 upto fe-1/0/1.80 exclude
```

Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces

This topic describes guidelines to consider when configuring interface ranges for named interface groups for DHCP local server and DHCP relay. The guidelines refer to the following configuration statement:

```
user@host# set interface interface-name upto upto-interface-name
```

- The start subunit, **interface *interface-name*** , serves as the key for the stanza. The remaining configuration settings are considered attributes.
- If the subunit is not included, an implicit **.0** subunit is enforced. The implicit subunit is applied to all interfaces when autoconfiguration is enabled. For example, **interface ge-2/2/2** is treated as **interface ge-2/2/2.0**.
- Ranged entries contain the **upto** option, and the configuration applies to all interfaces within the specified range. The start of a ranged entry must be less than the end of the range. Discrete entries apply to a single interface, except in the case of autoconfiguration, in which a **0** (zero) subunit acts as a wildcard.
- Interface stanzas defined within the same router or switch context are dependent and can constrain each other—both DHCP local server and DHCP relay are considered. Interface stanzas defined across different router (switch) contexts are independent and do not constrain one another.
- Each interface stanza, whether discrete or ranged, has a unique start subunit across a given router context. For example, the following configuration is not allowed within the same group because **ge-1/0/0.10** is the start subunit for both.

  ```
  interface ge-1/0/0.10 upto ge-1/0/0.30
  interface ge-1/0/0.10
  ```

- Two groups cannot share interface space. For example, the following configuration is not allowed because the three stanzas share the same space and interfere with one another—interface **ge-1/0/0.26** is common to all three.

  ```
  dhcp-relay group diamond interface ge-1/0/0.10 upto ge-1/0/0.30
  dhcp-local-server group ruby interface ge-1/0/0.26
  dhcp-relay group sapphire interface ge-1/0/0.25 upto ge-1/0/0.35
  ```

- Two ranges cannot overlap, either within a group or across groups. Overlapping occurs when two interface ranges share common subunit space but neither range is a proper subset of the other. The following ranges overlap:

  ```
  interface ge-1/0/0.10 upto ge-1/0/0.30
  interface ge-1/0/0.20 upto ge-1/0/0.40
  ```

- A range can contain multiple nested ranges. A nested range is a proper subset of another range. When ranges are nested, the smallest matching range applies.

  In the following example, the three ranges nest properly:

  ```
  interface ge-1/0/0.10 upto ge-1/0/0.30
  interface ge-1/0/0.12 upto ge-1/0/0.15 exclude
  interface ge-1/0/0.25 upto ge-1/0/0.29 exclude
  ```

- Discrete interfaces take precedence over ranges. In the following example, interface **ge-1/0/0.20** takes precedence and enforces an interface client limit of **5**.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.15 upto ge-1/0/0.25 exclude
interface ge-1/0/0.20 overrides interface-client-limit 5
```

Configuring Group-Specific DHCP Local Server Options

You can include the following statements at the **[edit system services dhcp-local-server group *group-name*]** hierarchy level to set group-specific DHCP local server configuration options. Statements configured at the **[edit system services dhcp-local-server group *group-name*]** hierarchy level apply only to the named group of interfaces, and override any global DHCP local server settings configured with the same statements at the **[edit system services dhcp-local-server]** hierarchy level.

DHCPv6 local server supports the same set of statements with the exception of the dynamic-profile statement.

- authentication—Configure the parameters the router sends to the external AAA server.
- dynamic-profile—Specify the dynamic profile that is attached to a group of interfaces.
- interface—Specify one or more interfaces, or a range of interfaces, that are within the specified group.
- liveness-detection—Configure bidirectional failure detection timers and authentication criteria for static routes, or Layer 2 liveness detection using ARP and Neighbor Discovery packets. For more information, see "DHCP Liveness Detection Overview" on page 674.
- overrides—Override the default configuration settings for the extended DHCP local server. For information, see "Overriding the Default DHCP Local Server Configuration Settings Overview" on page 630.

Configuring Group-Specific DHCP Relay Options

You can include the following statements at the **[edit forwarding-options dhcp-relay group *group-name*]** hierarchy level to set group-specific DHCP relay agent configuration options. Group-specific statements apply only to the named group of interfaces, and override any global DHCP relay agent settings for the same statement.

Include the statements at the **[edit forwarding-options dhcp-relay dhcpv6 group *group-name*]** hierarchy level to configure group-specific options for DHCPv6 relay agent.

- active-server-group—Configure an active server group to apply a common DHCP relay agent configuration for a named group of DHCP server addresses. For information, see "Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups" on page 667.
- authentication—Configure the parameters the router (or switch) sends to the external AAA server.
- dynamic-profile—Specify the dynamic profile that is attached to a group of interfaces.
- interface—Specify one or more interfaces, or a range of interfaces, that are within the specified group.

- liveness-detection—Configure bidirectional failure detection timers and authentication criteria for static routes, or Layer 2 liveness detection using ARP and Neighbor Discovery packets. For more information, see "DHCP Liveness Detection Overview" on page 674.
- overrides—Override the default configuration settings for the extended DHCP relay agent. For information, see "Overriding the Default DHCP Relay Configuration Settings" on page 627.
- relay-agent-interface-id—(DHCPv6 only) Insert the DHCPv6 Relay Agent Interface-ID option (option 18) in DHCPv6 packets destined for the DHCPv6 server.
- **relay-agent-remote-id**—(DHCPv6 only) Insert the DHCPv6 Relay Agent Remote-ID option (option 37) in DHCPv6 packets destined for the DHCPv6 server.
- relay-option—Configure selective processing, which uses DHCP options in client packets to identify and filter client traffic, and to specify the action DHCP relay agent takes with the traffic. For more information, see *Using DHCP Option Information to Selectively Process DHCP Client Traffic*.
- relay-option-82—(DHCPv4 only) Enable or disable the insertion of option 82 information in packets destined for a DHCP server. For information, see "Using DHCP Relay Agent Option 82 Information" on page 633.
- service-profile—Specify the default subscriber service, (or default profile) which is activated when the subscriber (or DHCP client) logs in and no other service is activated by a RADIUS server or a provisioning server. For more information, see *Default Subscriber Service Overview*.

Related Documentation

- Applying a Common DHCP Relay Agent Configuration to Groups of DHCP Servers on page 666
- DHCP for Switches on page 581

Connectivity Liveness Detection in the DHCP Access Network

DHCP Liveness Detection Overview

Unlike PPP, DHCP does not define a native keepalive mechanism as part of either the DHCPv4 or DHCPv6 protocols. Without a keepalive mechanism, DHCP local server, DHCP relay, and DHCP relay proxy are unable to quickly detect if any of them has lost connectivity with a subscriber or a DHCP client. Instead, they must rely on standard DHCP subscriber session or DHCP client session termination messages.

DHCP clients often do not send DHCP release messages before exiting the network. The discovery of their absence is dependent on existing DHCP lease time and release request mechanisms. These mechanisms are often insufficient when serving as session health checks for clients in a DHCP subscriber access or a DHCP-managed network. Because DHCP lease times are typically too long to provide an adequate response time for a session health failure, and configuring short DHCP lease times can pose an undue burden on control plane processing, implementing a DHCP liveness detection mechanism enables better monitoring of bound DHCP clients. When configured with a liveness detection protocol, if a given subscriber (or client) fails to respond to a configured number of consecutive liveness detection requests, the subscriber (or client) binding is deleted and its resources released.

DHCP liveness detection for DHCP subscriber IP or DHCP client IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

Using DHCP liveness detection, IP sessions are acted upon as soon as liveness detection checks fail. This faster response time serves to:

- Provide more accurate time-based accounting of subscriber (or DHCP client) sessions.
- Better preserve router (switch) resources.
- Help to reduce the window of vulnerability to some security attacks.

Examples of liveness detection protocols include Bidirectional Forwarding Detection (BFD) for both DHCPv4 and DHCPv6 subscribers, IPv4 Address Resolution Protocol (ARP) for DHCPv4 subscribers, and IPv6 Neighbor Unreachability Detection (NUD) using Neighbor Discovery (ND) packets for DHCPv6 subscribers.

Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection. In earlier releases, only BFD is supported for all platforms.

The two liveness detection methods are mutually exclusive.

When configuring BFD liveness detection, keep the following in mind:

- You can configure liveness detection for both DHCP local server and DHCP relay.
- You can configure DHCPv4 and DHCPv6 liveness detection either globally or per DHCPv4 or DHCPv6 group.
- DHCPv4 or DHCPv6 subscriber access clients that do not support BFD are not affected by the liveness detection configuration. These clients can continue to access the network (after they are validated) even if BFD liveness detection is enabled on the router (or switch).
- When configured, DHCPv4 or DHCPv6 initiates liveness detection checks for clients that support BFD when those clients enter a bound state.
- After protocol-specific messages are initiated for a BFD client, they are periodically sent to the subscriber (or client) IP address of the client and responses to those liveness detection requests are expected within a configured amount of time.
- If liveness detection responses are not received from clients that support BFD within the configured amount of time for a configured number of consecutive attempts, the liveness detection check is deemed to have failed. A configured failure action to clear the client binding is applied.
- The only failure action supported for Layer 2 Liveness detection is **clear-binding**.

When configuring DHCP ARP and ND Layer 2 liveness detection on MX Series, keep the following in mind:

- You can configure liveness detection for both DHCP local server and DHCP relay.
- You can configure DHCPv4 and DHCPv6 ARP and ND liveness detection globally, per DHCPv4 or DHCPv6 group, and per dual-stack group.
- ARP/ND liveness detection applies only to DHCP clients that:
  - Are directly connected over dynamic VLANs.
  - Have permanent Layer 2 entries.
- DHCPv6 clients must have a unique source MAC address and link-local address. Only single liveness detection entry is used for all IPv6 addresses associated with a specific client session.

Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD

You can configure liveness detection with Bidirectional Forwarding Detection (BFD) for DHCP subscriber IP sessions or DHCP client IP sessions to check the connectivity of DHCP relay clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

To configure liveness detection for DHCP relay:

1. Specify that you want to configure liveness detection.
   - For DHCP global configuration:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit liveness-detection
     ```

   - For DHCP group configuration:

     ```
     [edit forwarding-options dhcp-relay group group-name]
     user@host# edit liveness-detection
     ```

   NOTE: Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the liveness-detection statement, and any subsequent configuration statements, at the **[edit forwarding-options dhcp-relay dhcpv6]** or **[edit forwarding-options dhcp-relay dhcpv6 group *group-name*** hierarchy level.

2. (Optional) Specify that you want to use DHCP relay proxy mode.

   ```
   [edit forwarding-options dhcp-relay group group-name]
   user@host# set overrides proxy-mode
   ```

3. Specify that you want to configure the liveness detection method.
   - For DHCP global configuration:

     ```
     [edit forwarding-options dhcp-relay liveness-detection]
     user@host# edit method
     ```

   - For DHCP group configuration:

     ```
     [edit forwarding-options dhcp-relay group group-name liveness-detection]
     user@host# edit method
     ```

4. Specify the liveness detection method that you want DHCP to use.

   NOTE: In releases earlier than Junos OS Release 17.4R1, the only method supported for liveness detection on all platforms is BFD.

   Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection. The two liveness detection methods are mutually exclusive. See DHCP Liveness Detection Using ARP and Neighbor Discovery Packets for information about configuring ARP and ND Layer 2 liveness detection.

- For DHCP global configuration:

```
[edit forwarding-options dhcp-relay liveness-detection method]
user@host# edit bfd
```

- For DHCP group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection method]
user@host# edit bfd
```

5. Configure the liveness detection method as desired.

   See "Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients" on page 677 for an example of how to globally configure DHCP relay liveness detection with BFD.

6. Configure the action the router takes when a liveness detection failure occurs.

   - For DHCP global configuration:

```
[edit forwarding-options dhcp-relay liveness-detection]
user@host# edit failure-action action
```

   - For DHCP group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection]
user@host# edit failure-action action
```

Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

This example shows how to configure liveness detection for DHCP relay agent subscribers using Bidirectional Forwarding Detection (BFD) as the liveness detection method.

Requirements

This example uses the following hardware and software components:

- Juniper Networks MX Series routers.
- Junos OS Release 12.1 or later

Before you begin:

- Configure DHCP relay agent. See "Extended DHCP Relay Agent Overview" on page 618.

Overview

In this example, you configure liveness detection for DHCP relay agent subscribers by completing the following operations:

1. Enable liveness detection globally for DHCP relay subscribers.
2. Specify BFD as the liveness detection method for all dynamically created DHCP relay subscribers.
3. Configure BFD-specific statements to define how the protocol behaves.
4. Configure the action the router takes when a liveness detection failure occurs.

NOTE: This example explains how to configure liveness detection for a DHCPv4 network. Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the liveness-detection statement, and any subsequent configuration statements, at the **[edit forwarding-options dhcp-relay dhcpv6]** or **[edit forwarding-options dhcp-relay dhcpv6 group *group-name*]** hierarchy level.

Configuration

Step-by-Step Procedure

To configure liveness detection for DHCP relay:

1. Specify that you want to configure liveness detection.

```
[edit forwarding-options dhcp-relay]
user@host# edit liveness-detection
```

2. Specify that you want to configure the liveness detection method.

```
[edit forwarding-options dhcp-relay liveness-detection]
user@host# edit method
```

3. Specify BFD as the liveness detection method that you want DHCP to use.

```
[edit forwarding-options dhcp-relay liveness-detection method]
user@host# edit bfd
```

4. Configure the detection time threshold (in milliseconds) at which a trap is produced.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
```

```
user@host# set detection-time threshold 50000
```

5. Configure the time (in milliseconds) for which BFD holds a session up notification.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set holddown-interval 50
```

6. Configure the BFD minimum transmit and receive interval (in milliseconds).

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set minimum-interval 45000
```

7. Configure the minimum receive interval (in milliseconds).

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set minimum-receive-interval 60000
```

8. Configure a multiplier value for the detection time.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set multiplier 100
```

9. Disable the ability for BFD interval timers to change or adapt to network situations.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set no-adaptation
```

10. Configure the BFD session mode.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set session-mode automatic
```

11. Configure the threshold and minimum interval for the BFD transmit interval.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set transmit-interval threshold 60000 minimum-interval 45000
```

12. Configure the BFD protocol version you want to detect.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set version automatic
```

13. Configure the action the router takes when a liveness detection failure occurs. In this example, the failure action is to clear the client session only when a liveness detection failure occurs and the local interface is detected as being up.

```
[edit forwarding-options dhcp-relay liveness-detection]
user@host# edit failure-action action
```

Results From configuration mode, confirm your configuration by entering the **show forwarding-options** command. If the output does not display the intended configuration, repeat the instructions in this example to correct it. The following output also shows a range of configured interfaces in group frankfurt.

```
[edit]
user@host# show forwarding-options
dhcp-relay {
  liveness-detection {
    failure-action clear-binding-if-interface-up;
    method {
      bfd {
        version automatic;
        minimum-interval 45000;
        minimum-receive-interval 60000;
        multiplier 100;
        no-adaptation;
        transmit-interval {
          minimum-interval 45000;
          threshold 60000;
        }
        detection-time {
          threshold 50000;
        }
        session-mode automatic;
        holddown-interval 50;
      }
    }
  }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring Detection of DHCP Local Server Client Connectivity with BFD

You can configure liveness detection with Bidirectional Forwarding Detection (BFD) for DHCP subscriber IP sessions or DHCP client IP sessions to check the connectivity of DHCP local server clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

NOTE: You can also configure DHCP liveness detection for DHCP relay.

To configure liveness detection for DHCP local server:

1. Specify that you want to configure liveness detection.

   - For DHCP global configuration:

     ```
     [edit system services dhcp-local-server]
     user@host# edit liveness-detection
     ```

   - For DHCP group configuration:

     ```
     [edit system services dhcp-local-server group group-name]
     user@host# edit liveness-detection
     ```

   NOTE: Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the liveness-detection statement, and any subsequent configuration statements, at the **[edit system services dhcp-local-server dhcpv6]** or **[edit system services dhcp-local-server dhcpv6 group *group-name*]** hierarchy level.

2. Specify that you want to configure the liveness detection method.

   - For DHCP global configuration:

     ```
     [edit system services dhcp-local-server liveness-detection]
     user@host# edit method
     ```

   - For DHCP group configuration:

     ```
     [edit system services dhcp-local-server group group-name liveness-detection]
     user@host# edit method
     ```

3. Specify the liveness detection method that you want DHCP to use.

   NOTE: In releases earlier than Junos OS Release 17.4R1, the only method supported for liveness detection on all platforms is BFD.

   Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection. The two liveness detection methods are mutually exclusive. See DHCP Liveness Detection Using ARP and Neighbor Discovery Packets for information about configuring ARP and ND Layer 2 liveness detection.

   - For DHCP global configuration:

     ```
     [edit system services dhcp-local-server liveness-detection method]
     user@host# edit bfd
     ```

- For DHCP group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection method]
user@host# edit bfd
```

4. Configure the liveness detection method as desired.

   See "Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients" on page 682 for an example of how to configure DHCPv4 groups for DHCP local server liveness detection with BFD.

5. Configure the action the router takes when a liveness detection failure occurs.

   - For DHCP global configuration:

```
[edit system services dhcp-local-server liveness-detection]
user@host# edit failure-action action
```

   - For DHCP group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection]
user@host# edit failure-action action
```

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients

This example shows how to configure group liveness detection for DHCP local server subscribers or DHCP clients using Bidirectional Forwarding Detection (BFD) as the liveness detection method.

Requirements

This example uses the following hardware and software components:

- Juniper Networks MX Series routers
- Juniper Networks EX Series switches
- Junos OS Release 12.1 or later

Before you begin:

- Configure DHCP local server. See "Extended DHCP Local Server Overview" on page 562.

Overview

In this example, you configure group liveness detection for DHCP local server subscribers (clients) by completing the following operations:

1. Enable liveness detection for DHCP local server subscriber (or DHCP client) groups.
2. Specify BFD as the liveness detection method for all dynamically created DHCP local server subscribers (clients).
3. Configure BFD-specific statements to define how the protocol behaves.
4. Configure the action the router (switch) takes when a liveness detection failure occurs.

NOTE: This example explains how to configure liveness detection for a DHCPv4 network. Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the liveness-detection statement, and any subsequent configuration statements, at the **[edit system services dhcp-local-server dhcpv6]** or **[edit system services dhcp-local-server dhcpv6 group *group-name*]** hierarchy level.

Configuration

Step-by-Step Procedure

To configure group liveness detection for DHCP local server:

1. Specify that you want to configure liveness detection.

```
[edit system services dhcp-local-server ]
user@host# edit liveness-detection
```

2. Specify that you want to configure liveness detection for a specific DHCP local server group.

```
[edit system services dhcp-local-server liveness-detection]
user@host# edit group local_group_1
```

3. Specify that you want to configure the liveness detection method.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection]
user@host# edit method
```

4. Specify BFD as the liveness detection method that you want DHCP to use.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection
  method]
user@host# edit bfd
```

5. Configure the detection time threshold (in milliseconds) at which a trap is produced.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection
  method bfd]
user@host# set detection-time threshold 30000
```

6. Configure the time (in milliseconds) for which BFD holds a session up notification.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection
  method bfd]
user@host# set holddown-interval 50
```

7. Configure the BFD minimum transmit and receive interval (in milliseconds).

NOTE: You do not need to configure the BFD minimum transmit and receive interval if you configure the **minimum-interval** for the BFD **transmit-interval** statement and the **minimum-receive-interval**.

```
[edit system services dhcp-local-servergroup local_group_1 liveness-detection method
  bfd]
user@host# set minimum-interval 45000
```

8. Configure the minimum receive interval (in milliseconds).

NOTE: You do not need to configure the BFD minimum receive interval if you configure the BFD minimum transmit and receive interval.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection
  method bfd]
user@host# set minimum-receive-interval 60000
```

9. Configure a multiplier value for the detection time.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection
  method bfd]
user@host# set multiplier 100
```

10. Disable the ability for BFD interval timers to change or adapt to network situations.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection
   method bfd]
user@host# set no-adaptation
```

11. Configure the BFD session mode.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection
   method bfd]
user@host# set session-mode automatic
```

12. Configure the threshold and minimum interval for the BFD transmit interval.

NOTE: You do not need to configure the transmit interval values if you have already configured the minimum transmit and receive interval for BFD.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection
   method bfd]
user@host# set transmit-interval threshold 60000 minimum-interval 45000
```

13. Configure the BFD protocol version you want to detect.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection
   method bfd]
user@host# set version automatic
```

14. Configure the action the router (switch) takes when a liveness detection failure occurs. In this example, the failure action is to clear the client session only when a liveness detection failure occurs and the local interface is detected as being up.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection]
user@host# edit failure-action action
```

Results From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the instructions in this example to correct it.

```
[edit]
user@host# show system
services {
   dhcp-local-server {
      group local_group_1 {
         liveness-detection {
            failure-action clear-binding-if-interface-up;
```

```
            method {
              bfd {
                version automatic;
                minimum-interval 45000;
                minimum-receive-interval 60000;
                multiplier 100;
                no-adaptation;
                transmit-interval {
                  minimum-interval 45000;
                  threshold 60000;
                }
                detection-time {
                  threshold 30000;
                }
                session-mode automatic;
                holddown-interval 50;
              }
            }
          }
        }
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

DHCP Liveness Detection Using ARP and Neighbor Discovery Packets

- How DHCP Liveness Detection with ARP and Neighbor Discovery Packets Works on page 686
- Configuring BNG Detection of DHCP Local Server Client Connectivity with ARP and ND Packets on page 689
- Configuring BNG Detection of DHCP Relay Client Connectivity with ARP and ND Packets on page 691
- Configuring DHCP Host Detection of Client Connectivity with ARP and ND Packets on page 693

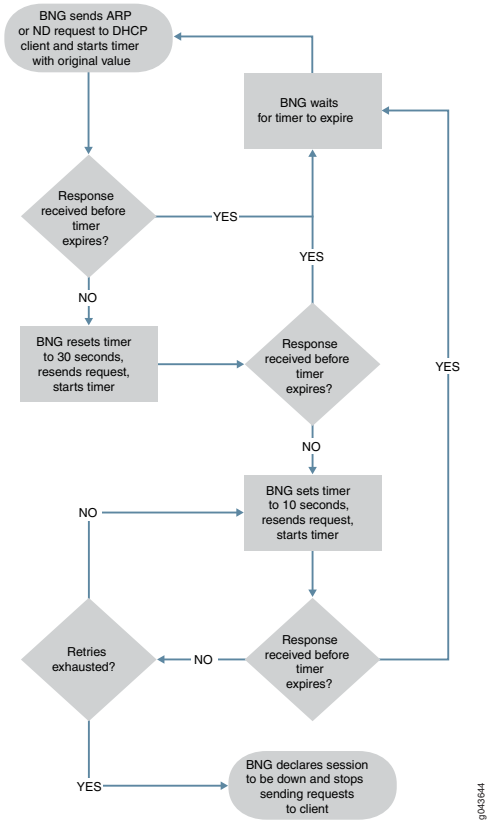
How DHCP Liveness Detection with ARP and Neighbor Discovery Packets Works

Starting in Junos OS Release 17.4R1, you can configure liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients. This Layer 2 liveness detection offers separate mechanisms for the DHCP client host and for the router acting as a broadband network gateway (BNG) to determine the validity and state of the DHCP client sessions. These mechanisms are referred to as the *send* functionality and the *receive* functionality. You can configure Layer 2 liveness detection for DHCP local server and DHCP relay clients.

Send Functionality

The BNG uses the send functionality to conduct a host connectivity check on its directly connected DHCPv4 and DHCPv6 clients to determine the validity and state of the DHCP client session, and to clean up inactive sessions. Figure 41 on page 687 illustrates the send functionality.

Figure 41: Layer 2 Liveness Detection Send Behavior Flow



1. The BNG sends request packets to the each DHCP client at a configurable interval, then waits for a response. The BNG retries the requests when it does not receive a timely response. It sends ARP requests for DHCPv4 clients and Neighbor Discovery (ND) requests for DHCPv6 clients.

2. If the BNG receives a response from the client before the interval times out, it waits for the timer to expire and then sends another request to that client.

3. If the BNG does not receive a response before the interval times out, it sets the timer to 30 seconds and sends another request. This is the first retry attempt; the timer is not configurable.

4. If the BNG receives a response from the client before the timer expires, then the BNG waits for the timer to run down, resets it to the original, configurable value, sends another request, and starts the timer.

5. If the 30-second timer expires before a response is received, the BNG sets the timer to 10 seconds and sends another request. This timer value is not configurable.

6. If the BNG receives a response from the client before the timer expires, then the BNG waits for the timer to run down, resets it to the original, configurable value, sends another request, and starts the timer.

7. If the BNG does not receive a response within the 10-second interval, it sends another request and starts the 10-second timer again. The BNG continues to send requests at 10-second intervals until it receives a response from the client before the interval times out or it exhausts the number of retry attempts.

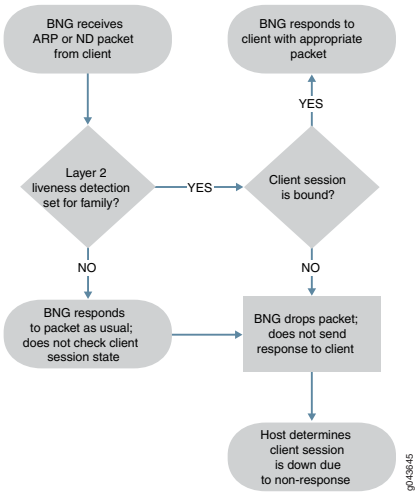
   The first retry attempt uses the 30-second interval. Subsequent retries occur at 10-second intervals. The number of possible 10-second retries is therefore the total number minus 1. For example, if you configure 5 retries, there is one 30-second retry and up to four 10-second retries.

8. If the BNG never sends a response from a client within the interval before the retries are exhausted, then the liveness detection check fails and the clear-binding failure action is implemented. The client session is cleared.

Receive Functionality

The receive functionality enables a DHCP client host to determine the state of the DHCPv4 or DHCPv6 client session from the perspective of a BNG. The BNG conducts a host connectivity check on its directly connected DHCPv4 and DHCPv6 clients when it receives ARP or ND packets. Figure 42 on page 688 illustrates the receive functionality.

Figure 42: Layer 2 Liveness Detection Receive Behavior Flow



When the BNG receives either of these packets, it does the following:

1. Checks whether Layer 2 liveness detection for subscriber management is enabled globally for the relevant address family, inet or inet6.

2. If Layer 2 liveness detection is not enabled, then the BNG responds as usual to the received packets without checking the state of the client session.

3. If liveness detection is enabled for the family, then the BNG checks whether the client session is still in the bound state.

4. If the client session is bound, the BNG responds to the client with the appropriate ARP or ND packet.

5. If the session is not bound, the BNG drops the received packet. It does not send an ARP or ND response packet to the host, enabling the host to determine that the BNG considers the session to be down.

The usefulness of the receive functionality depends on the ability of the DHCP client host to reclaim resources from the stale client based on the absence of a response packet from the BNG for an unbound client session. If this capability requires a change in the client implementation, you may want to use the send functionality.

Configuring BNG Detection of DHCP Local Server Client Connectivity with ARP and ND Packets

This procedure shows you how to configure the send functionality of Layer 2 liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients to check the connectivity of DHCP local server clients.

The send functionality enables the BNG to determine whether a client session is down based on a lack of response from the DHCP client to the ARP or ND request packets it sends to the client.

NOTE: **DHCP liveness detection can also be configured using Bidirectional Forwarding Detection (BFD). BFD liveness detection and ARP/ND liveness detection are mutually exclusive.**

To configure the send functionality for DHCPv4 local server liveness detection:

1. Specify that you want to configure the liveness detection method.
   - For DHCPv4 global configuration:

     ```
     [edit system services dhcp-local-server]
     user@host# edit liveness-detection method
     ```

   - For DHCPv4 group configuration:

     ```
     [edit system services dhcp-local-server]
     user@host# edit group group-name liveness-detection method
     ```

   - For DHCPv4 dual-stack-group configuration:

     ```
     [edit system services dhcp-local-server]
     ```

```
user@host# edit dual-stack-group dual-stack-group-name liveness-detection
  method
```

2. Specify the Layer 2 liveness detection method.

   - For DHCPv4 global configuration:

     ```
     [edit system services dhcp-local-server liveness-detection method]
     user@host# set layer2-liveness-detection
     ```

   - For DHCPv4 group configuration:

     ```
     [edit system services dhcp-local-server group group-name liveness-detection method]
     user@host# set layer2-liveness-detection
     ```

   - For DHCPv4 dual-stack-group configuration:

     ```
     [edit system services dhcp-local-server dual-stack-group dual-stack-group-name
       liveness-detection method]
     user@host# set layer2-liveness-detection
     ```

3. (Optional) Configure the number of retry attempts and the interval timer.

   - For DHCPv4 global configuration:

     ```
     [edit system services dhcp-local-server liveness-detection method]
     user@host# edit layer2-liveness-detection
     user@host# set max-consecutive-retries number
     user@host# set transmit-interval seconds
     ```

   - For DHCPv4 group configuration:

     ```
     [edit system services dhcp-local-server group group-name liveness-detection method]
     user@host# edit layer2-liveness-detection
     user@host# set max-consecutive-retries number
     user@host# set transmit-interval seconds
     ```

   - For DHCPv4 dual-stack-group configuration:

     ```
     [edit system services dhcp-local-server dual-stack-group dual-stack-group-name
       liveness-detection method]
     user@host# edit layer2-liveness-detection
     user@host# set max-consecutive-retries number
     user@host# set transmit-interval seconds
     ```

To configure the send functionality for DHCPv6 local server liveness detection:

1. Specify that you want to configure the liveness detection method.

   - For DHCPv6 global configuration:

     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit liveness-detection method
     ```

   - For DHCPv6 group configuration:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit group group-name liveness-detection method
```

2. Specify the Layer 2 liveness detection method.

   - For DHCPv6 global configuration:

     ```
     [edit system services dhcp-local-server dhcpv6 liveness-detection method]
     user@host# set layer2-liveness-detection
     ```

   - For DHCPv6 group configuration:

     ```
     [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection
       method]
     user@host# set layer2-liveness-detection
     ```

3. (Optional) Configure the number of retry attempts and the interval timer.

   - For DHCPv6 global configuration:

     ```
     [edit system services dhcp-local-server dhcpv6 liveness-detection method]
     user@host# edit layer2-liveness-detection
     user@host# set max-consecutive-retries number
     user@host# set transmit-interval seconds
     ```

   - For DHCPv6 group configuration:

     ```
     [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection
       method]
     user@host# edit layer2-liveness-detection
     user@host# set max-consecutive-retries number
     user@host# set transmit-interval seconds
     ```

Configuring BNG Detection of DHCP Relay Client Connectivity with ARP and ND Packets

This procedure shows you how to configure the send functionality of Layer 2 liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients to check the connectivity of DHCP relay clients.

The send functionality enables the BNG to determine whether a client session is down based on a lack of response from the DHCP client to the ARP or ND request packets it sends to the client.

NOTE: DHCP liveness detection can also be configured using Bidirectional Forwarding Detection (BFD). BFD liveness detection and ARP/ND liveness detection are mutually exclusive.

To configure the send functionality for DHCPv4 relay liveness detection:

1. Specify that you want to configure the liveness detection method.
   - For DHCPv4 global configuration:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit liveness-detection method
     ```

   - For DHCPv4 group configuration:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit group group-name liveness-detection method
     ```

   - For DHCPv4 dual-stack-group configuration:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit dual-stack-group dual-stack-group-name liveness-detection
       method
     ```

2. Specify the Layer 2 liveness detection method.
   - For DHCPv4 global configuration:

     ```
     [edit forwarding-options dhcp-relay liveness-detection method]
     user@host# set layer2-liveness-detection
     ```

   - For DHCPv4 group configuration:

     ```
     [edit forwarding-options dhcp-relay group group-name liveness-detection method]
     user@host# set layer2-liveness-detection
     ```

   - For DHCPv4 dual-stack-group configuration:

     ```
     [edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name
       liveness-detection method]
     user@host# set layer2-liveness-detection
     ```

3. (Optional) Configure the number of retry attempts and the interval timer.
   - For DHCPv4 global configuration:

     ```
     [edit forwarding-options dhcp-relay liveness-detection method]
     user@host# edit layer2-liveness-detection
     user@host# set max-consecutive-retries number
     user@host# set transmit-interval seconds
     ```

   - For DHCPv4 group configuration:

     ```
     [edit forwarding-options dhcp-relay group group-name liveness-detection method]
     user@host# edit layer2-liveness-detection
     user@host# set max-consecutive-retries number
     user@host# set transmit-interval seconds
     ```

   - For DHCPv4 dual-stack-group configuration:

```
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name
  liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

To configure the send functionality for DHCPv6 relay liveness detection:

1. Specify that you want to configure the liveness detection method.
   - For DHCPv6 global configuration:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit liveness-detection method
     ```

   - For DHCPv6 group configuration:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit group group-name liveness-detection method
     ```

2. Specify the Layer 2 liveness detection method.
   - For DHCPv6 global configuration:

     ```
     [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method]
     user@host# set layer2-liveness-detection
     ```

   - For DHCPv6 group configuration:

     ```
     [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection
       method]
     user@host# set layer2-liveness-detection
     ```

3. (Optional) Configure the number of retry attempts and the interval timer.
   - For DHCPv6 global configuration:

     ```
     [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method]
     user@host# edit layer2-liveness-detection
     user@host# set max-consecutive-retries number
     user@host# set transmit-interval seconds
     ```

   - For DHCPv6 group configuration:

     ```
     [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection
       method]
     user@host# edit layer2-liveness-detection
     user@host# set max-consecutive-retries number
     user@host# set transmit-interval seconds
     ```

Configuring DHCP Host Detection of Client Connectivity with ARP and ND Packets

This procedure shows you how to configure the receive functionality of Layer 2 liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6

Neighbor Unreachability Detection for DHCPv6 clients to check the connectivity of DHCP local server clients.

The receive functionality enables the DHCP client host to determine whether a client session is down based on a lack of response from the BNG to the ARP or ND packets it sends to the BNG. You configure the receive functionality globally for DHCP per address family as an override to the global subscriber management configuration.

1. Enable Layer 2 liveness detection globally per address family.
   - For DHCPv4:

     ```
     [edit system services subscriber-management overrides]
     user@host# set interfaces family inet layer2-liveness-detection
     ```

   - For DHCPv6:

     ```
     [edit system services subscriber-management overrides]
     user@host# set interfaces family inet6 layer2-liveness-detection
     ```

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, you can configure liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients.

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection.
17.4R1	Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection.
17.4R1	Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection.
17.4R1	Starting in Junos OS Release 17.4R1, you can configure liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients.

Related Documentation

- *DHCP Overview*

Securing DHCP Messages Sent Between DHCP Clients and Servers in Different VRFs

Junos OS allows you to use the DHCP relay agent to provide additional security when exchanging DHCP messages between different VRFs. To exchange DHCP messages between different VRFs, you must enable both the server side and the client side of the DHCP relay agent recognize and forward acceptable traffic based on DHCP option information in the packets. The DHCP relay agent can ensure that there is no direct routing between the client virtual routing and forwarding instance (VRF) and the DHCP server VRF, and that only acceptable DHCP packets are relayed across the two VRFs. For more information, read this topic.

- DHCP Message Exchange Between DHCP Clients and DHCP Server in Different VRFs on page 695
- Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances on page 696

DHCP Message Exchange Between DHCP Clients and DHCP Server in Different VRFs

In some service provider networks, the service network in which the DHCP server resides is isolated from the actual subscriber network. This separation of the service and subscriber networks can sometimes introduce potential security issues, such as route leaking. Starting in Junos OS Release 14.2, you can use the DHCP relay agent to provide additional security when exchanging DHCP messages between different VRFs. The DHCP relay agent can ensure that there is no direct routing between the client virtual routing and forwarding instance (VRF) and the DHCP server VRF, and that only acceptable DHCP packets are relayed across the two VRFs. Subscriber management supports the cross-VRF message exchange for both DHCP and DHCPv6 packets.

To exchange DHCP messages between different VRFs, you must enable both the server side and the client side of the DHCP relay agent to recognize and forward acceptable traffic based on DHCP option information in the packets. The message exchange uses the Agent Circuit ID (DHCP option 82 suboption 1) for DHCPv4 packets and the Relay Agent Interface-ID (DHCPv6 option 18) for DHCPv6 packets to identify traffic to be relayed.

Statistics for DHCP packets using the cross-VRF message exchange are counted in the client VRF.

The following list describe how DHCP relay agent exchanges messages between the DHCP clients and DHCP server in different VRFs:

- Packets from DHCP client to DHCP server—DHCP relay agent receives the DHCP packet from the client in the client VRF, and then inserts the appropriate DHCP option 82 suboption 1 or DHCPv6 option 18 attribute into the packet. The relay agent then forwards the packet to the DHCP server in the server's VRF.
- Packets from DHCP server to DHCP client—DHCP relay agent receives the DHCP reply message from the DHCP server in the server VRF. The relay agent derives the client's interface, including VRF, from the DHCP option 82 suboption 1 or DHCPv6 option 18

attribute in the packet in the DHCP server VRF. The relay agent then forwards the reply message to the DHCP client in the client's VRF.

Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances

Starting in Junos OS Release 14.2, you can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing and forwarding instances (VRFs).

You can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing instances. This type of configuration is for a *stateless* DHCP relay connection between a DHCP server and a DHCP client, when the DHCP server resides in a network that must be isolated from the client network.

A stateless DHCP relay agent does not maintain dynamic state information about the DHCP clients and does not maintain a static route for the traffic to flow between the client and server routing instances.

To enable the DHCP message exchange between the two VRFs, you configure each side of the DHCP relay to recognize and forward acceptable traffic based on the DHCP option information in the packets. The acceptable traffic is identified by either the Agent Circuit ID (DHCP option 82 suboption 1) for DHCPv4 packets or the Relay Agent Interface-ID (DHCPv6 option 18) for DHCPv6 packets.

The following list provides an overview of the tasks required to create the DHCP message exchange between the different VRFs:

- Client-side support—Configure the DHCP relay agent **forward-only** statement to specify the VRF location of the DHCP server, to which the DHCP relay agent forwards the client packets with the appropriate DHCP option information. The **forward-only** statement ensures that DHCP relay agent does not create a new session or perform any other subscriber management operations (such as creating dynamic interfaces or maintaining leases).

  You can optionally configure a specific logical system and routing instance for the server VRF. If you do not specify a logical system or routing instance, then DHCP uses the local logical system and routing instance from which the configuration is added.

- Server-side support—Configure the DHCP relay agent **forward-only-replies** statement so the DHCP relay agent forwards the reply packets that have the appropriate DHCP option information. This statement also ensures that DHCP relay agent does not create a new session or perform any other subscriber management operations.

NOTE: You do not need to configure the forward-only-replies statement if the DHCP client and DHCP server reside in the same logical system/routing instance.

- DHCP local server support—Configure the DHCP local server to support option 82 information in DHCP NAK and forcerenew messages. By default, the two message types do not support option 82.
- Additional support—Ensure that the following required support is configured:
  - Proxy ARP support must be enabled on the server-facing interface in the DHCP server VRF so that the DHCP relay agent can receive and respond to the ARP requests for clients and the client-facing interface in the DHCP server VRF.
  - Routes must be available to receive the DHCP packets from the DHCP server in the server VRF for the clients reachable in the client VRF.

The following procedures describe the configuration tasks for creating the DHCP message exchange between the DHCP server and clients in different VRFs.

- Client-Side Support on page 697
- Server-Side Support on page 698
- DHCP Local Server Support on page 698

Client-Side Support

To configure support on the client side of the DHCP relay agent:

1. Enable DHCP relay agent configuration.

```
[edit forwarding-options]
user@host# edit dhcp-relay
```

2. Specify the DHCP server VRF to which the DHCP relay agent forwards the packets from the DHCP client. DHCP relay agent forwards the acceptable packets that have the appropriate DHCP option information, but does not perform any additional subscriber management operations. You can configure the **forward-only** statement globally or for a named group of interfaces, and for DHCPv4 or DHCPv6. You can specify the current, default, or a specific logical system or routing instance for the server VRF.

   The following example configures the **forward-only** statement globally for DHCPv4, and specifies the default logical system and routing instance:

```
[edit forwarding-options dhcp-relay]
user@host# set forward-only logical-system default routing-instance default
```

NOTE: For local DHCPv4 clients, the DHCP relay agent adds the Agent Circuit ID option. However, if the Agent Circuit ID option is already present in the packet, you must ensure that the DHCP server supports the option 82 Vendor-Specific Information suboption (suboption 9).

If the **forward-only** statement is configured at the **[edit forwarding-options dhcp-relay relay-option]** hierarchy level, then that relay-option action takes precedence over the configuration of the **forward-only** statement for the DHCP cross-VRF message exchange.

Server-Side Support

To configure the cross-VRF message exchange support on the server side of the DHCP relay:

NOTE: You do not need to configure the **forward-only-replies** statement if the DHCP client and DHCP server reside in the same logical system/routing instance.

1. Enable DHCP relay agent configuration.

```
[edit forwarding-options]
user@host# edit dhcp-relay
```

2. Configure the DHCP relay agent to forward the DHCP packets from the DHCP server VRF to the client. DHCP relay agent only forwards the packets, and does not perform any additional subscriber management operations. You can configure the **forward-only-replies** statement globally for DHCPv4 and DHCPv6.

   The following example configures the **forward-only-replies** statement globally for DHCPv4.

```
[edit forwarding-options dhcp-relay]
user@host# set forward-only-replies
```

DHCP Local Server Support

To configure the DHCP local server to support option 82 information in NAK and forcerenew messages; the cross-VRF message exchange feature uses the option 82 or DHCPv6 option 18 information to determine the client VRF:

1. Enable DHCP local server configuration.

```
[edit system services]
user@host# edit dhcp-local-server
```

2. Specify that you want to configure an override option.

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

3. Configure DHCP local server to override the default behavior and support option 82 information in DHCP NAK and forcerenew messages. You can configure the override action globally, for a group of interfaces, or for a specific interface.

```
[edit system services dhcp-local-server overrides]
user@host# set include-option-82 forcerenew nak
```

Release History Table

Release	Description
14.2	Starting in Junos OS Release 14.2, you can use the DHCP relay agent to provide additional security when exchanging DHCP messages between different VRFs.
14.2	Starting in Junos OS Release 14.2, you can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing and forwarding instances (VRFs).

Related Documentation

- DHCP for Switches on page 581

Assigning IP Addresses for DHCP

Address pool is a set of Internet Protocol addresses available for allocation to users, such as in host configurations with the DHCP. An address-assignment pool can support either IPv4 address or IPv6 addresses. You can create centralized IPv4 and IPv6 address pools independently of the client applications that use the pools. For more information, read this topic.

- Address-Assignment Pools Overview on page 700
- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 701
- Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 702
- Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option on page 703
- Multiple Address Assignment for DHCPv6 Clients on page 704

Address-Assignment Pools Overview

The address-assignment pool feature supports subscriber management and DHCP management functionality by enabling you to create centralized IPv4 and IPv6 address pools independently of the client applications that use the pools. The authd process manages the pools and the address allocation, whether the addresses come from local pools or from a RADIUS server. For example, multiple client applications, such as DHCP, can use the same address-assignment pool to provide addresses for their particular clients. Client applications can acquire addresses for either authenticated or unauthenticated clients. The pool selected for a subscriber, based on the RADIUS server or network matching or other rule, is called the matching pool for the subscriber.

Address-assignment pools support both dynamic and static address assignment. In dynamic address assignment, a client is automatically assigned an address from the address-assignment pool. In static address assignment, which is supported for IPv4 pools only, you reserve an address that is then always used by a particular client. Addresses that are reserved for static assignment are removed from the dynamic address pool and cannot be assigned to other clients.

You can configure named address ranges within an address-assignment pool. A named range is a subset of the overall address range. A client application can use named ranges to manage address assignment based on client-specific criteria. For example, for IPv4 address-assignment pools, you might create a named range that is based on a specific DHCP option 82 value. Then, when a DHCP client request matches the specified option 82 value, an address from the specified range is assigned to the client.

Starting in Junos OS Release 18.1R1, you can exclude a specified address or range of consecutive addresses to prevent them from being allocated from an address pool. For example, you might want to reserve certain addresses or ranges to be used only for static subscribers. When you configure an address or range to be excluded, and the address or an address within the range, has already been allocated, that subscriber is logged out, the address is deallocated, and the address is marked for exclusion.

You can link address-assignment pools together to provide backup pools for address assignment. When no addresses are found to be available in the primary or matching address pool, the router or switch automatically proceeds to the linked (secondary) address pool to search for an available address to allocate.

Although the first pool in a chain of linked pools is generally considered the primary pool, a matching pool is not necessarily the first pool in the chain. For example, in a chain of three pools, A, B, and C, where A is the primary pool, pool B might be matched for certain subscribers based on information returned by the RADIUS server. The search for an available address for those subscribers begins in pool B.

Starting in Junos OS Release 18.1R1, the behavior changes for how the search for an available address proceeds through a chain of linked pools. By default, the matching pool is searched first, then the search moves to the first pool in the chain and proceeds through the chain until an available address is found and allocated, or until the search determines no addresses are free. In each pool, all address ranges are fully searched for an address. This behavior enables addresses to be assigned contiguously.

Alternatively, you can configure the **linked-pool-aggregation** statement to search first within a block of addresses in each range in the matching pool and then successively through the linked pools. The search then moves back to the first pool in the chain and searches all addresses in all ranges in each pool through the last pool in the chain.

The address-assignment pool hold-down feature enables you to specify that no additional address are allocated from an existing active address-assignment pool. This configuration gracefully transforms the active pool to an inactive state as the previously allocated addresses are returned to the pool. When the pool is inactive, you can safely perform maintenance on the pool without affecting any active subscribers.

You can also explicitly identify that an address-assignment pool is used for NDRA.

NOTE: This feature requires a license. To understand more about Subscriber Access Licensing , see Subscriber Access Licensing Overview. Please refer to the Juniper Licensing Guide for general information about License Management. Please refer to the product Data Sheets for details, or contact your Juniper Account Team or Juniper Partner.

Benefits of Address Assignment Pools

- You can create centralized pools of addresses independent of client applications.
- You can specify blocks of addresses, named ranges, so that a given address pool can be used to supply different addresses for different client applications or for subscribers that match different sets of criteria.
- You can link pools together to ensure that pools are searched for free addresses in a specific manner, contiguously or noncontiguously.
- You can gracefully transition an address pool from active to inactive by specifying that no further addresses are allocated from the pool.

Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use

You can specify the match order in which the extended DHCP local server uses the client data to determine the address-assignment pool that provides the IP address and configuration for a DHCP client. You use the **pool-match-order** statement to specify the match order. If you do not specify the **pool-match-order**, the router (or switch) uses the default **ip-address-first** matching to select the address pool. After DHCP local server determines the address assignment pool to use, the server performs the matching based on the criteria you specified in the pool configuration.

In the default **ip-address-first** matching, the server selects the address-assignment pool to use by matching the IP address in the client DHCP request with the network address of the address-assignment pool. If the client request contains the gateway IP address (giaddr), the local server matches the giaddr to the address-assignment pool's address. If there is no giaddr in the request, then the DHCP local server matches the IP address of the receiving interface to the address of the address-assignment pool.

In **external-authority** matching, the DHCP local server receives the address assignment from an external authority, such as RADIUS or Diameter. If RADIUS is the external authority, the DHCP local server uses the Framed-IPv6-Pool attribute (RADIUS attribute 100) to select the pool. If Diameter is the external authority, the server uses the Diameter counterpart of the Framed-IPv6-Pool attribute to determine the pool.

For IPv4 address-assignment pools, you can optionally configure the extended DHCP local server to match the DHCP relay agent information option (option 82) in the client DHCP packets to a named range in the address-assignment pool used for the client. Named ranges are subsets within the overall address-assignment pool address range, which you can configure when you create the address-assignment pool.

NOTE: To use the DHCP local server option 82 matching feature with an IPv4 address-assignment pool, you must ensure that the **option-82** statement is included in the **dhcp-attributes** statement for the address-assignment pool.

To configure the matching order the extended DHCP local server uses to determine the address-assignment pool used for a client:

1. Access the **pool-match-order** configuration.

```
[edit system services dhcp-local-server]
user@host# edit pool-match-order
```

2. Specify the pool matching methods in the order in which the router (switch) performs the methods. You can specify the methods in any order. All methods are optional—the router (switch) uses the **ip-address-first** method by default.

   - Configure the router (switch) to use an external addressing authority.

```
[edit system services dhcp-local-server pool-match-order]
user@host# set external-authority
```

   - Configure the router (switch) to use the ip-address-first method.

```
[edit system services dhcp-local-server pool-match-order]
user@host# set ip-address-first
```

   - (IPv4 address-assignment pools only) Specify the option 82 matching method.

```
[edit system services dhcp-local-server pool-match-order]
user@host# set option-82
```

Example: Extended DHCP Local Server Configuration with Optional Pool Matching

This example shows an extended DHCP local server configuration that includes optional IPv4 address-assignment pool matching and interface groups. For pool matching, this

configuration specifies that the DHCP local server first check the response from an external authentication authority (for example, RADIUS) and use the Framed-IPv6-Pool attribute to determine the address-assignment pool to use for the client address. If no external authority match is found, the DHCP local server then uses ip-address-first matching together with the option 82 information to match the named address range for client IPv4 address assignment. The option 82 matching must also be included in the address-assignment pool configuration.

```
[edit system services]
dhcp-local-server {
   group group_one {
      interface fe-0/0/2.0;
      interface fe-0/0/2.1;
   }
   group group_two {
      interface fe-0/0/3.0;
      interface fe-0/0/3.1;
   }
   pool-match-order {
      external-authority
      ip-address-first;
      option-82;
   }
}
```

NOTE: The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.

Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option

Subscriber management or DHCP management enables you to specify that DHCP local server assign a particular address to a client. For example, if a client is disconnected, you might use this capability to assign the same address that the client was using prior to being disconnected. If the requested address is available, DHCP assigns it to the client. If the address is unavailable, the DHCP local server offers another address, based on the address allocation process.

Both DHCP local server and DHCPv6 local server support the specific address request feature. DHCP local server uses DHCP option 50 in DHCP discover messages to request a particular address, while DHCPv6 local server uses the IA_NA option (Identity Association for Non-Temporary Addresses) in DHCPv6 solicit messages.

NOTE: Subscriber management (DHCP management) supports only one address for each of the DHCPv6 IA_NA or IA_PD address types. If the DHCPv6 client requests more than one address for a given type, the DHCPv6 local server uses only the first address and ignores the other addresses.

Multiple Address Assignment for DHCPv6 Clients

For a DHCPv6 local server, you can assign multiple addresses to a single DHCPv6 client. Multiple address support is enabled by default, and is activated when the DHCPv6 local server receives a DHCPv6 Solicit message from a DHCP client that contains multiple addresses.

For example, if you are implementing this feature on the routers, you might use the multiple address assignment feature when a customer premises equipment (CPE) device requires a host address and a delegated prefix.

You can use either local address pools or RADIUS when assigning multiple addresses to a DHCP client. When at least one address is successfully allocated, the switch creates a DHCP client entry and binds the entry to the assigned address. If both addresses are successfully allocated, the switch creates a single DHCP client entry and binds both addresses to that entry.

You can also configure a delegated address pool, which explicitly specifies the address pool that DHCP management uses to assign IPv6 prefixes for DHCP clients.

See Also

- *Specifying the Delegated Address-Assignment Pool to Be Used for DHCPv6 Prefix Delegation*

Release History Table

Release	Description
18.1R1	Starting in Junos OS Release 18.1R1, you can exclude a specified address or range of consecutive addresses to prevent them from being allocated from an address pool.
18.1R1	Starting in Junos OS Release 18.1R1, the behavior changes for how the search for an available address proceeds through a chain of linked pools.

Related Documentation

- DHCP for Switches on page 581

Suppressing DHCP Access

The DHCP process adds access-internal and destination routes for DHCPv4 sessions, and access-internal and access routes for DHCPv6 sessions during the DHCP client binding operation. However, you can override the default behavior and prevent DHCP from automatically installing the route information. For more information, read this topic.

- Suppressing DHCP Access, Access-Internal, and Destination Routes on page 705
- Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default on page 705

Suppressing DHCP Access, Access-Internal, and Destination Routes

During the DHCP client binding operation, the DHCP process adds route information for the DHCP sessions by default. The DHCP process adds access-internal and destination routes for DHCPv4 sessions, and access-internal and access routes for DHCPv6 sessions. In some scenarios, you might want to override the default behavior and prevent DHCP from automatically installing the route information. For example, DHCP relay installs destination (host) routes by default—this action is required in certain configurations to enable address renewals from the DHCP server to work properly. However, the default installation of destination routes might cause a conflict when you configure DHCP relay with static subscriber interfaces. To avoid such configuration conflicts you can override the default behavior and prevent DHCP relay from installing the routes.

NOTE: **You cannot suppress access-internal routes when the subscriber is configured with both IA_NA and IA_PD addresses over IP demux interfaces—the IA_PD route relies on the IA_NA route for next hop connectivity.**

You can configure both DHCP local server and DHCP relay agent to override the default route installation behavior, and you can specify the override for both DHCPv4 and DHCPv6 sessions. You can override the route installation globally or for named interface groups. For DHCPv4 you can override the installation of destination routes only or access-internal routes (the access-internal option prevents installation of both destination and access-internal routes). For DHCPv6 you can specify access routes, access-internal routes, or both.

Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default

You can configure both DHCP local server and DHCP relay agent to override the default installation of access, access-internal, and destination routes. For DHCPv4 you can override the installation of destination routes only or access-internal routes (the access-internal option prevents installation of both destination and access-internal routes). For DHCPv6 you can specify access routes, access-internal routes, or both. You can configure the override globally or for named interface groups.

NOTE: **You cannot suppress access-internal routes when the subscriber is configured with both IA_NA and IA_PD addresses over IP demux interfaces—the IA_PD route relies on the IA_NA route for next hop connectivity.**

NOTE: **The no-arp statement is deprecated and the function is replaced by the route-suppression statement.**

To configure route suppression and prevent DHCP from installing specific types of routes:

- For DHCP local server route suppression (for example, a global configuration):

```
[edit system services dhcp-local-server]
user@host# set route-suppression access-internal
```

- For DHCP relay (for example, a group-specific configuration):

```
[edit forwarding-options dhcp-relay group southeast]
user@host# set route-suppression destination
```

- For DHCPv6 local server (for example, a group-specific configuration):

```
[edit system services dhcp-local-server group southern3]
user@host# set dhcpv6 route-suppression access access-internal
```

- For DHCPv6 relay (for example, a global configuration):

```
[edit forwarding-options dhcp-relay]
user@host# set dhcpv6 route-suppression access
```

DHCP Snooping

DHCP snooping on Junos OS device validates DHCP messages and drops invalid traffic. You can configure how DHCP relay agent handles DHCP snooped packets. Depending on the configuration, DHCP relay agent either forwards or drops the snooped packets it receives.

- DHCP Snooping Support on page 706
- Example: Configuring DHCP Snooping Support for DHCP Relay Agent on page 708
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent on page 710

DHCP Snooping Support

DHCP snooping provides DHCP security by identifying incoming DHCP packets. In the default DHCP snooping configuration, all traffic is snooped. You can optionally use the **forward-snooped-clients** statement to evaluate the snooped traffic and to determine if the traffic is forwarded or dropped, based on whether or not the interface is configured as part of a group.

In Junos OS, DHCP snooping is enabled in a routing instance when you configure either the **dhcp-relay** statement at the **[edit forwarding-options]** hierarchy level, or the **dhcp-local-server** statement at the **[edit system services]** hierarchy level in that routing instance. The router discards snooped packets by default if there is no subscriber associated with the packet. To enable normal processing of snooped packets, you must explicitly configure the **allow-snooped-clients** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level.

You can configure DHCP snooping support for a specific routing instance for the following:

- DHCPv4 relay agent—Override the router's (or switch's) default snooping configuration and specify that DHCP snooping is enabled or disabled globally, for a named group of interfaces, or for a specific interface within a named group.

  In a separate procedure, you can set a global configuration to specify whether the DHCPv4 relay agent forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces. The router also uses the global DHCP relay agent snooping configuration to determine whether to forward or drop snooped BOOTREPLY packets. A renew request may be unicast directly to the DHCP server. This is a BOOTPREQUEST packet and is snooped.

- DHCPv6 relay agent—As you can with snooping support for the DHCPv4 relay agent, you can override the default DHCPv6 relay agent snooping configuration on the router to explicitly enable or disable snooping support globally, for a named group of interfaces, or for a specific interface with a named group of interfaces.

  In multi-relay topologies where more than one DHCPv6 relay agent is between the DHCPv6 client and the DHCPv6 server, snooping enables intervening DHCPv6 relay agents between the client and the server to correctly receive and process the unicast traffic from the client and forward it to the server. The DHCPv6 relay agent snoops incoming unicast DHCPv6 packets by setting up a filter with UDP port 547 (the DHCPv6 UDP server port) on a per-forwarding table basis. The DHCPv6 relay agent then processes the packets intercepted by the filter and forwards the packets to the DHCPv6 server.

  Unlike the DHCPv4 relay agent, the DHCPv6 relay agent does not support global configuration of forwarding support for DHCPv6 snooped packets.

- DHCP local server—Configure whether DHCP local server forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces.

- You can also disable snooping filters. In the preceding configurations, all DHCP traffic is forwarded to the slower routing plane of the routing instance before it is either forwarded or dropped. Disabling snooping filters causes DHCP traffic that can be forwarded directly from the faster hardware control plane to bypass the routing control plane.

See Also

- *Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server*
- *Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent*
- *Disabling DHCP Snooping Filters*
- *Example: Enabling DHCP Snooping Support for DHCPv6 Relay Agent*

Example: Configuring DHCP Snooping Support for DHCP Relay Agent

This example shows how to configure DHCP snooping support for DHCP relay agent.

Requirements

- Configure DHCP relay agent. See "Extended DHCP Relay Agent Overview" on page 618.

Overview

In this example, you configure DHCP snooping support for DHCP relay agent by completing the following operations:

- Override the default DHCP snooping configuration and enable DHCP snooping support for the interfaces in group **frankfurt**.
- Configure DHCP relay agent to forward snooped packets to only configured interfaces.

NOTE: **By default, DHCP snooping is disabled globally.**

Configuration

Step-by-Step Procedure

To configure DHCP relay support for DHCP snooping:

1. Specify that you want to configure DHCP relay agent.

```
[edit]
user@host# edit forwarding-options dhcp-relay
```

2. Specify the named group of interfaces on which DHCP snooping is supported.

```
[edit forwarding-options dhcp-relay]
user@host# edit group frankfurt
```

3. Specify the interfaces that you want to include in the group. DHCP relay agent considers these as the configured interfaces when determining whether to forward or drop traffic.

```
[edit forwarding-options dhcp-relay group frankfurt]
user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9
```

4. Specify that you want to override the default configuration for the group.

```
[edit forwarding-options dhcp-relay group frankfurt]
user@host# edit overrides
```

5. Enable DHCP snooping support for the group.

```
[edit forwarding-options dhcp-relay group frankfurt overrides]
user@host# set allow-snooped-clients
```

6. Return to the **[edit forwarding-options dhcp-relay]** hierarchy level to configure the forwarding action and specify that DHCP relay agent forward snooped packets on only configured interfaces:

```
[edit forwarding-options dhcp-relay group frankfurt overrides]
user@host# up 2
```

7. Enable DHCP snooped packet forwarding for DHCP relay agent.

```
[edit forwarding-options dhcp-relay]
user@host# edit forward-snooped-clients
```

8. Specify that snooped packets are forwarded on only configured interfaces (the interfaces in group **frankfurt**).

```
[edit forwarding-options dhcp-relay forward-snooped-clients]
user@host# set configured-interfaces
```

Results From configuration mode, confirm your configuration by entering the **show forwarding-options** command. If the output does not display the intended configuration, repeat the instructions in this example to correct it. The following output also shows a range of configured interfaces in group frankfurt.

```
[edit]
user@host# show forwarding-options
dhcp-relay {
   forward-snooped-clients configured-interfaces;
   group frankfurt {
      overrides {
         allow-snooped-clients;
      }
      interface fe-1/0/1.3 {
         upto fe-1/0/1.9;
      }
   }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

See Also
- *Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent*

Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent

You can configure how DHCP relay agent handles DHCP snooped packets. Depending on the configuration, DHCP relay agent either forwards or drops the snooped packets it receives.

DHCP relay uses a two-part configuration to determine how to handle DHCP snooped packets. This topic describes how you use the **forward-snooped-clients** statement to manage whether DHCP relay agent forwards or drops snooped packets, depending on the type of interface on which the packets are snooped. In the other part of the DHCP relay agent snooping configuration, which is described in *Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent*, you enable or disable the DHCP relay snooping feature.

Table 53 on page 710 shows the action the router or switch takes on snooped packets when DHCP snooping is enabled by the **allow-snooped-clients** statement.
Table 54 on page 711 shows the action the router (or switch) takes on snooped packets when DHCP snooping is disabled by the **no-allow-snooped-clients** statement.

The router or switch also uses the configuration of the DHCP relay agent forwarding support to determine how to handle snooped BOOTREPLY packets. Table 55 on page 711 shows the action the router (or switch) takes for the snooped BOOTREPLY packets.

NOTE: Configured interfaces have been configured with the **group** statement in the **[edit forwarding-options dhcp-relay]** hierarchy. Non-configured interfaces are in the logical system/routing instance but have not been configured by the **group** statement.

Table 53: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Enabled

forward-snooped-clients Configuration	Action on Configured Interfaces	Action on Non-Configured Interfaces
forward-snooped-clients not configured	snooped packets result in subscriber (DHCP client) creation	dropped
all-interfaces	forwarded	forwarded
configured-interfaces	forwarded	dropped
non-configured-interfaces	snooped packets result in subscriber (DHCP client) creation	forwarded

Table 54: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Disabled

forward-snooped-clients Configuration	Action on Configured Interfaces	Action on Non-Configured Interfaces
forward-snooped-clients not configured	dropped	dropped
all-interfaces	dropped	forwarded
configured-interfaces	dropped	dropped
non-configured-interfaces	dropped	forwarded

Table 55: Actions for Snooped BOOTREPLY Packets

forward-snooped-clients Configuration	Action
forward-snooped-clients not configured	snooped **BOOTREPLY** packets dropped if client is not found
forward-snooped-clients all configurations	snooped **BOOTREPLY** packets forwarded if client is not found

To configure DHCP snooped packet forwarding and BOOTREPLY snooped packet forwarding for DHCP relay agent:

1. Specify that you want to configure DHCP relay agent.

```
[edit]
user@host# edit forwarding-options dhcp-relay
```

2. Enable DHCP snooped packet forwarding.

```
[edit forwarding-options dhcp-relay]
user@host# edit forward-snooped-clients
```

3. Specify the interfaces that are supported for snooped packet forwarding.

```
[edit forwarding-options dhcp-relay forward-snooped-clients]
user@host# set (all-interfaces | configured-interfaces | non-configured-interfaces)
```

For example, to configure DHCP relay agent to forward DHCP snooped packets on only configured interfaces:

```
[edit]
forwarding-options {
   dhcp-relay {
```

```
    forward-snooped-clients configured-interfaces;
  }
}
```

See Also

- *Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent*

CHAPTER 13

DHCP for Security Devices

DHCP Overview

The Dynamic Host Configuration Protocol (DHCP) can serve as a DHCP local server, a DHCP client, or a DHCP relay agent.

DHCP Overview

A Dynamic Host Configuration Protocol (DHCP) server can automatically allocate IP addresses and also deliver configuration settings to client hosts on a subnet. DHCP lets network administrators centrally manage a pool of IP addresses among hosts and automate the assignment of IP addresses in a network. An IP address can be leased to a host for a limited period of time, allowing the DHCP server to share a limited number of IP addresses among a group of hosts that do not need permanent IP addresses.

The Juniper Networks device acts as the DHCP server, providing IP addresses and settings to hosts, such as PCs, that are connected to device interfaces. The DHCP server is compatible with the DHCP servers of other vendors on the network.

The device can also operate as a DHCP client and DHCP relay agent.

DHCP is based on BOOTP, a bootstrap protocol that allows a client to discover its own IP address, the IP address of a server host, and the name of a bootstrap file. DHCP servers can handle requests from BOOTP clients, but provide additional capabilities beyond

BOOTP, such as the automatic allocation of reusable IP addresses and additional configuration options.

NOTE: Although a Juniper Networks device can act as a DHCP server, a DHCP client, or DHCP relay agent at the same time, you cannot configure more than one DHCP role on a single interface.

DHCP provides two primary functions:

- Allocate temporary or permanent IP addresses to clients.
- Store, manage, and provide client configuration parameters.

NOTE: On all SRX Series devices, DHCPv4 is supported only in Layer 3 mode; the DHCP server and DHCP client are not supported in Layer 2 transparent mode.

DHCP Local Server

You can enable an SRX Series device to function as a DHCP local server, and then configure its options on the device. The DHCP local server provides an IP address and other configuration information in response to a client request.

To configure the DHCP local server on the device, include the **dhcp-local-server** statement at the **[edit system services]** hierarchy level.

NOTE: You cannot configure the DHCP local server and the DHCP relay agent on the same interface.

DHCP Client, DHCP Local Server, and Address-Assignment Pool Interaction

In a typical branch network configuration, the DHCP client is on the subscriber's computer, and the DHCP local server is configured on the device. The following steps provide a high-level description of the interaction among the DHCP client, DHCP local server, and address-assignment pools.

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber.

2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.

3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server selected to grant the address and configuration information.

4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server and client installs the host route and ARP entry, and then monitors the lease state.

DHCP Local Server and Address-Assignment Pools

In a DHCP local server operation, the client address and configuration information reside in centralized address-assignment pools, that are managed independently from the DHCP local server and they can be shared by different client applications.

Configuring a DHCP environment that includes a DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the DHCP local server on the device and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients.

NOTE: **The DHCP local server and the address-assignment pools used by the server must be configured in the same routing instance.**

DHCP Client

DHCP configuration consists of configuring DHCP clients and a DHCP local server. A client configuration determines how clients send a message requesting an IP address, while a server configuration enables the server to send an IP address back to the client.

For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP local server in the network. You set the vendor class ID, lease time, DHCP server address, retransmission attempts, and retry interval.

DHCP Relay Agent

You can configure DHCP relay options on the device and enable the device to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP local server.

To configure the DHCP relay agent on the router, include the **dhcp-relay** statement at the **[edit forwarding-options]** hierarchy level.

You can also include the **dhcp-relay** statement at the following hierarchy level:

[edit routing-instances routing-instance-name forwarding-options]

DHCP Client, DHCP Relay Agent, and DHCP Local Servers

In a typical branch network configuration, the DHCP client is on the subscriber's computer, and the DHCP relay agent is configured on the device between the DHCP client and one or more DHCP local servers.

The following steps describe, at a high level, how the DHCP client, DHCP relay agent, and DHCP local server interact in a configuration that includes two DHCP local servers.

1. The DHCP client sends a discover packet to find a DHCP local server in the network from which to obtain configuration parameters for the subscriber, including an IP address.

2. The DHCP relay agent receives the discover packet and forwards copies to each of the two DHCP local servers. The DHCP relay agent then creates an entry in its internal client table to keep track of the client's state.

3. In response to receiving the discover packet, each DHCP local server sends an offer packet to the client. The DHCP relay agent receives the offer packets and forwards them to the DHCP client.

4. On receipt of the offer packets, the DHCP client selects the DHCP local server from which to obtain configuration information. Typically, the client selects the server that offers the longest lease time on the IP address.

5. The DHCP client sends a request packet that specifies the DHCP local server from which to obtain configuration information.

6. The DHCP local server requested by the client sends an acknowledgement (ACK) packet that contains the client's configuration parameters.

7. The DHCP relay agent receives the ACK packet and forwards it to the client.

8. The DHCP client receives the ACK packet and stores the configuration information.

9. If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.

10. After establishing the initial lease on the IP address, the DHCP client and the DHCP local server use unicast transmission to negotiate lease renewal or release.

Considerations

The following considerations apply when you enable a DHCP local server, DHCP relay agent, or DHCP client in a routing instance:

- The DHCP local server, DHCP relay agent, and DHCP client can be configured in one routing instance, but the functionality is mutually exclusive on one interface. If the DHCP client is enabled on one interface, the DHCP local server or the DHCP relay agent cannot be enabled on that interface.
- The DHCP client, DHCP relay agent and DHCP local server services act independently in their respective routing instance. The following features can function simultaneously on a device:
  - DHCP client and DHCP local server
  - DHCP client and DHCP relay agent
  - Multiple routing instances. Each instance can have a DHCP local server, DHCP relay agent, or DHCP client, or each routing instance can have a DHCP client and DHCP local server or a DHCP client and DHCP relay agent.
- In Junos Release 12.1X46, autoinstallation is not compatible with jDHCPd:

```
version 12.1X46-D40.2;
system {
    /* not compatible with jDHCPd */   <<<<<<
    autoinstallation {
        usb {
            disable;
        }
    }
```

NOTE: Before you enable DHCP services in a routing instance, you must remove all the configuration related to DHCP services that does not include routing instance support. If you do not do this, the old default routing instance configuration will override the new routing instance configuration.

NOTE: On all SRX Series devices, logical systems and routing instances are not supported for a DHCP client in chassis cluster mode.

DHCP Settings and Restrictions Overview

Propagation of TCP/IP Settings for DHCP

The Juniper Networks device can operate simultaneously as a client of the DHCP server in the untrust zone and a DHCP server to the clients in the trust zone. The device takes the TCP/IP settings that it receives as a DHCP client and forwards them as a DHCP server to the clients in the trust zone. The device interface in the untrust zone operates as the DHCP client, receiving IP addresses dynamically from an Internet service provider (ISP) on the external network.

During the DHCP protocol exchange, the device receives TCP/IP settings from the external network on its DHCP client interface. Settings include the address of the ISP's DHCP

name server and other server addresses. These settings are propagated to the DHCP server pools configured on the device to fulfill host requests for IP addresses on the device's internal network.

DHCP Conflict Detection and Resolution

A client that receives an IP address from the device operating as a DHCP server performs a series of Address Resolution Protocol (ARP) tests to verify that the address is available and no conflicts exist. If the client detects an address conflict, it informs the DHCP server about the conflict and can request another IP address from the DHCP server.

The device maintains a log of all client-detected conflicts and removes addresses with conflicts from the DHCP address pool. To display the conflicts list, you use the **show system services dhcp conflict** command. The addresses in the conflicts list remain excluded until you use the **clear system services dhcp conflict** command to manually clear the list.

DHCP Interface Restrictions

The device supports DHCP client requests received on any Ethernet interface. DHCP requests received from a relay agent are supported on all interface types.

DHCP is not supported on interfaces that are part of a virtual private network (VPN).

Related Documentation

- Understanding DHCP Server Operation on page 718
- Understanding DHCP Client Operation on page 733
- Understanding DHCP Relay Agent Operation on page 742
- Example - Configuring DHCPv6 Prefix Delegation (PD) over Point-to-Point Protocol over Ethernet (PPPoE) on page 765

DHCP Server

A Dynamic Host Configuration Protocol (DHCP) server provides a framework to pass configuration information to client hosts on a TCP/IP network. A device acting as a DHCP server can dynamically allocate IP addresses and other configuration parameters, minimizing the overhead that is required to add clients to the network. Read this topic for more information.

- Understanding DHCP Server Operation on page 718
- DHCP Server Configuration Overview on page 719
- Minimum DHCP Local Server Configuration on page 721
- Enabling TCP/IP Propagation on a DHCP Local Server on page 722
- Example: Configuring the Device as a DHCP Server on page 722
- Verifying and Managing DHCP Local Server Configuration on page 728

Understanding DHCP Server Operation

As a DHCP server, a Juniper Networks device can provide temporary IP addresses from an IP address pool to all clients on a specified subnet, a process known as dynamic

binding. Juniper Networks devices can also perform static binding, assigning permanent IP addresses to specific clients based on their media access control (MAC) addresses. Static bindings take precedence over dynamic bindings.

This section contains the following topics:

DHCP Options

In addition to its primary DHCP server functions, you can also configure the device to send configuration settings like the following to clients through DHCP:

- IP address of the DHCP server (Juniper Networks device)
- List of Domain Name System (DNS) and NetBIOS servers
- List of gateway routers
- IP address of the boot server and the filename of the boot file to use
- DHCP options defined in RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

Compatibility with Autoinstallation

The functions of a Juniper Networks device acting as a DHCP server are compatible with the autoinstallation feature. The DHCP server automatically checks any autoinstallation settings for conflicts and gives the autoinstallation settings priority over corresponding DHCP settings. For example, an IP address set by autoinstallation takes precedence over an IP address set by the DHCP server.

Chassis Cluster Support

DHCP server operations are supported on all SRX Series devices in chassis cluster mode.

See Also

- *DHCP Server, Client, and Relay Agent Overview*
- Understanding DHCP Client Operation on page 733
- Understanding DHCP Relay Agent Operation on page 742

DHCP Server Configuration Overview

A typical DHCP server configuration provides the following configuration settings for a particular subnet on a device interface:

- An IP address pool, with one address excluded from the pool.
- Default and maximum lease times.
- Domain search suffixes. These suffixes specify the domain search list used by a client when resolving hostnames with DNS.

- A DNS name server.
- Device solicitation address option (option 32). The IP address excluded from the IP address pool is reserved for this option.

In addition, the DHCP server might assign a static address to at least one client on the subnet. Table 56 on page 720 provides the settings and values for the sample DHCP server configuration.

Table 56: Sample DHCP Server Configuration Settings

Setting	Sample Value
DHCP Subnet Configuration	
Address pool subnet address	**192.168.2.0/24**
High address in the pool range	**192.168.2.254**
Low address in the pool range	**192.168.2.2**
Address pool default lease time, in seconds	**1,209,600** (14 days)
Address pool maximum lease time, in seconds	**2,419,200** (28 days)
Domain search suffixes	**mycompany.net** **mylab.net**
Address to exclude from the pool	**192.168.2.33**
DNS server address	**192.168.10.2**
Identifier code for router solicitation address option	**32**
Type choice for router solicitation address option	**Ip address**
IP address for router solicitation address option	**192.168.2.33**
DHCP MAC Address Configuration	
Static binding MAC address	**01:03:05:07:09:0B**
Fixed address	**192.168.2.50**

See Also

- *DHCP Server, Client, and Relay Agent Overview*
- Understanding DHCP Client Operation on page 733
- Understanding DHCP Relay Agent Operation on page 742
- RFC 3397, *Dynamic Host Configuration Protocol (DHCP) Domain Search Option*

Minimum DHCP Local Server Configuration

The following sample output shows the minimum configuration you must use to configure an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DHCP local server. In this output, the server group is named mobileusers, and the DHCP local server is enabled on interface ge-1/0/1.0 within the group. The address pool is named acmenetwork from low range of 192.168.1.10/24 to a high range of 192.168.1.20/24.

```
[edit access]
address-assignment {
   pool acmenetwork {
      family inet {
         network 192.168.1.0/24;
         range r1 {
            low 192.168.1.10;
            high 192.168.1.20;
         }
      }
   }
}
```

```
edit system services
dhcp-local-server {
   group mobileusers {
      interface ge-1/0/1.0
   }
}
```

```
edit interfaces ge-1/0/1 unit 0
family {
   inet {
      address 192.168.1.1/24
   }
}
```

NOTE: You can configure the DHCP local server in a routing instance by using the **dhcp-local server**, **interface**, and **address-assignment** statements in the **[edit routing-instances]** hierarchy level.

See Also

- Configuring Address-Assignment Pools on page 730

Enabling TCP/IP Propagation on a DHCP Local Server

This topic describes how to configure TCP/IP settings on a DHCP local server, which includes a DHCP client and a DHCP local server.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

To enable TCP/IP setting propagation on a DHCP local server:

1. Configure the **update-server** option on the DHCP client.

```
[edit interfaces ge-0/0/1 unit 0 family inet]
dhcp-client {
  update-server;
}
```

2. Configure the address pool to specify the interface (where **update-server** is configured) from which TCP/IP settings can be propagated.

```
[edit access]
address-assignment {
  pool sprint family inet {
    network 192.168.2.0/24;
      dhcp-attributes {
        propagate-settings ge-0/0/1.0;
    }
  }
}
```

3. Configure the DHCP local server.

```
edit system services
dhcp-local-server {
  group bob {
    interface ge-1/0/1.0
  }
}
```

See Also

- Minimum DHCP Local Server Configuration on page 721

Example: Configuring the Device as a DHCP Server

This example shows how to configure the device as a DHCP server.

For information on how to configure JDHCP in a routing instance, see How to configure JDHCP in a routing instance.

Requirements

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices. See the *Understanding Management Predefined Policy Applications*.
- Determine the DHCP options required by the subnets and clients in your network.

Overview

In this example, you configure the device as a DHCP server. You specify the IP address pool as 192.168.2.0/24 and from a low range of 192.168.2.2 to a high range of 192.168.2.254. You set the maximum-lease-time to 2,419,200. Then you specify the DNS server IP address as 192.168.10.2.

WARNING: **Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated. and only the new JDHCP CLI is supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:**

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **set access** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/2 unit 0 family inet address 192.168.2.1/24
```

```
set system services dhcp-local-server group g1 interface ge-0/0/2.0
set access address-assignment pool p1 family inet network 192.168.2.0/24
set access address-assignment pool p1 family inet range r1 low 192.168.2.2
set access address-assignment pool p1 family inet range r1 high 192.168.2.254
set access address-assignment pool p1 family inet dhcp-attributes maximum-lease-time
  2419200
set access address-assignment pool p1 family inet dhcp-attributes name-server
  192.168.10.2
```

GUI Step-by-Step Procedure

To configure the device as a DHCP server, specify the DHCP pool information, server information, lease time, and option information:

1. In the J-Web interface, select **Configure** > **DHCP** > **DHCP Services**.
2. Select DHCP Pools. Click **Add**.
3. Specify the IP address that is used as the source address the DHCP server includes in IP packets when communicating with clients. The address is included in the DHCP packet in option 54.
4. Specify the subnet information for the IPv4 address-assignment pool. Type **192.168.2.0/24**.
5. In the Address Range Low, type **192.168.2.2**.
6. In the Address Range High, type **192.168.2.254**.
7. In the Exclude Addresses box, type the addresses you want excluded from a DHCP address pool. Type **192.168.2.0/24**
8. Specify the server identifier to assign to any DHCP clients in this address pool. The identifier can be used to identify a DHCP server in a DHCP message.
9. Specify the domain name to assign to any DHCP clients in this address pool.
10. Specify the next server that DHCP clients need to contact. Type **192.168.10.2**
11. Define the maximum amount of time (in seconds) that DHCP should lease an address. Type **2419200**.
12. Define DHCP option 32, the device solicitation address option. You must enter a numeric value for option code. Select the option type from the list that corresponds to the option code.

13. Click **OK**.

14. If you are done configuring the device, click **Commit** > **Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the device as a DHCP server:

1. Configure an interface with an IP address on which the DHCP server will be reachable.

```
[edit]
user@host# set interfaces ge-0/0/2 unit 0 family inet address 192.168.2.1/24
```

2. Configure the DHCP server.

```
[edit]
user@host#  set system services dhcp-local-server group g1 interface ge-0/0/2.0
```

3. Create an address pool for IPv4 addresses that can be assigned to clients. The addresses in the pool must be on the subnet in which the DHCP clients reside. Do not include addresses that are already in use on the network.

```
[edit]]
user@host# set access address-assignment pool p1 family inet network
   192.168.2.0/24
```

4. (Optional) Specify the IP address pool range. Define a range of addresses in the address-assignment pool. The range is a subset of addresses within the pool that can be assigned to clients. If no range is specified, then all addresses within the pool are available for assignment. Configure the name of the range and the lower and upper boundaries of the addresses in the range.

```
[edit]]
user@host# set access address-assignment pool p1 192.168.2.0/24 address-range
   low 192.168.2.2 high 192.168.2.254
```

5. (Optional) Configure one or more routers as the default gateway on the client's subnet.

```
[edit]
user@host# set access address-assignment pool p1 family inet dhcp-attributes
   router 192.168.10.3
```

6. (Optional) Configure the IP address that is used as the source address for the DHCP server in messages exchanged with the client. Clients use this information to distinguish between lease offers.

```
[edit]
user@host# set access address-assignment pool pool1 family inet dhcp-attributes
   server-identifier 192.168.10.1
```

7. (Optional) Specify the maximum time period, in seconds, that a client holds the lease for an assigned IP address if the client does not renew the lease.

```
[edit]
user@host# set access address-assignment pool pool1 family inet dhcp-attributes
   maximum-lease-time 2419200
```

8. (Optional) Specify user-defined options to be included in DHCP packets

```
[edit]
user@host# set access address-assignment pool pool1 family inet dhcp-attributes
   option 98 string test98
```

9. Assign a fixed IP address with the MAC address of the client.

```
[edit]
user@host# set access address-assignment pool pool1 family inet host host1
   ip-address 192.168.2.100 hardware-address 2c:56:dc:72:99:f3
```

Results

- From configuration mode, confirm your configuration by entering the **show access address-assignment** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show access address-assignment
pool p1 {
   family inet {
   network 192.168.2.0/24;
   range r1 {
   low 192.168.2.2;
      high 192.168.2.254;
   }
   dhcp-attributes {
      maximum-lease-time 2419200;
      name-server {
      192.168.10.2;
            }
        }
      }
   }
```

```
}
```

- From configuration mode, confirm your configuration by entering the **show system services dhcp-local-server** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system services dhcp-local-server
group g1 {
interface ge-0/0/2.0;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying the DHCP Binding Database on page 727
- Verifying DHCP Server Operation on page 728

Verifying the DHCP Binding Database

Purpose Verify that the DHCP binding database reflects the DHCP server configuration.

Action From operational mode, enter these commands:

- **show dhcp server binding** command to display all active bindings in the database.
- **show dhcp server binding *address* detail** command (where *address* is the IP address of the client) to display more information about a client.

These commands produce following sample output:

```
user@host> show dhcp server binding
```

```
IP Address   Hardware Address   Type          Lease expires at
30.1.1.20  00:12:1e:a9:7b:81  dynamic       2007-05-11 11:14:43 PDT
```

```
user@host> show dhcp server binding address detail
```

```
    IP address           192.0.2.2
    Hardware address     00:a0:12:00:13:02
    Pool                 192.0.2.0/24
    Interface  fe-0/0/0, relayed by 192.0.2.200

Lease information:
    Type                 DHCP
    Obtained at          2004-05-02 13:01:42 PDT
    Expires at           2004-05-03 13:01:42 PDT
    State                active

DHCP options:
     Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
```

```
Name: domain-name, Value: mydomain.tld
  Code: 32, Type: ip-address, Value: 192.0.2.33
```

Verifying DHCP Server Operation

Purpose Verify that the DHCP server operation has been configured.

Action From operational mode, enter the following command:

- **show dhcp server statistics** command to verify the DHCP server statistics.

```
user@host> show dhcp server statistics
Packets dropped:
    Total                       0

Messages received:
    BOOTREQUEST                 45
    DHCPDECLINE                 0
    DHCPDISCOVER                1
    DHCPINFORM                  39
    DHCPRELEASE                 0
    DHCPREQUEST                 5
    DHCPLEASEQUERY              0
    DHCPBULKLEASEQUERY          0

Messages sent:
    BOOTREPLY                   6
    DHCPOFFER                   1
    DHCPACK                     3
    DHCPNAK                     2
    DHCPFORCERENEW              0
    DHCPLEASEUNASSIGNED         0
    DHCPLEASEUNKNOWN            0
    DHCPLEASEACTIVE             0
    DHCPLEASEQUERYDONE          0
```

See Also

- *DHCP Server, Client, and Relay Agent Overview*
- Understanding DHCP Relay Agent Operation on page 742
- *DHCP Settings and Restrictions Overview*

Verifying and Managing DHCP Local Server Configuration

Purpose View or clear information about client address bindings and statistics for the extended DHCP local server.

NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the **clear dhcp server binding** command before you delete the DHCP server configuration.

Action

- To display the address bindings in the client table on the extended DHCP local server:

  user@host> **show dhcp server binding routing-instance *customer routing instance***

- To display extended DHCP local server statistics:

  user@host> **show dhcp server statistics routing-instance *customer routing instance***

- To clear the binding state of a DHCP client from the client table on the extended DHCP local server:

  user@host> **clear dhcp server binding routing-instance *customer routing instance***

- To clear all extended DHCP local server statistics:

  user@host> **clear dhcp server statistics routing-instance *customer routing instance***

Release History Table

Release	Description
15.1X49-D60	Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated. and only the new JDHCP CLI is supported.

Related Documentation

- DHCP Address-Assignment Pools on page 729
- DHCP Client on page 733
- DHCP Relay Agent on page 742
- DHCPv6 Server on page 758

DHCP Address-Assignment Pools

Address pool is a set of Internet Protocol addresses available for allocation to users, such as in host configurations with the DHCP. An address-assignment pool can support either IPv4 address or IPv6 addresses. You cannot use the same pool for both types of address. For more information, read this topic.

- Configuring Address-Assignment Pools on page 730
- Configuring an Address-Assignment Pool Name and Addresses on page 730
- Configuring a Named Address Range for Dynamic Address Assignment on page 731

Configuring Address-Assignment Pools

The address-assignment pool feature for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices enables you to create address pools that can be shared by different client applications such as DHCPv4 or DHCPv6.

To configure an address-assignment pool:

1. Configure the address-assignment pool name and specify the addresses for the pool.

   See "Configuring an Address-Assignment Pool Name and Addresses" on page 730.

2. (Optional) Configure named ranges (subsets) of addresses.

   See "Configuring a Named Address Range for Dynamic Address Assignment" on page 731.

3. (Optional;IPv4 only) Create static address bindings.

   See "Configuring Static Address Assignments" on page 732.

4. (Optional) Configure attributes for DHCP clients.

   See "Configuring DHCP Client-Specific Attributes for Address-Assignment Pools" on page 734.

Configuring an Address-Assignment Pool Name and Addresses

When configuring an address-assignment pool on SRX300, SRX320, SRX340, SRX345, SRX1500, and SRX550M devices, you must specify the name of the pool and its addresses.

To configure an IPv4 address-assignment pool:

1. Configure the name of the pool and specify the IPv4 family.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Configure the network address and the prefix length of the addresses in the pool.

```
[edit access address-assignment pool blr-pool family inet]
user@host# set network 192.168.0.0/16
```

NOTE: You can configure an IPv4 address-assignment pool in a routing instance by configuring the address-assignment statements at the**[edit routing-instance** ***routing-instance-name***] hierarchy level. For example **[edit routing-instances routing-instances name access address-assignment pool blr-pool family inet]**. The above steps shows only the **[edit access]** configuration.

Configuring a Named Address Range for Dynamic Address Assignment

You can optionally configure multiple named ranges, or subsets, of addresses within an address-assignment pool. During a dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, you specify a name for the range and define the address range.

NOTE: Supported only on SRX300, SRX320, SRX340, SRX345, SRX1500, and SRX550M devices.

To create a named range within an IPv4 address-assignment pool:

1. Specify the name of the address-assignment pool.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Configure the name of the range and the lower and upper boundaries of the addresses in the range.

```
[edit access address-assignment pool isp_1 family inet]
user@host# set range southeast low 192.168.102.2 high 192.168.102.254
```

NOTE: To configure named address ranges in a routing instance, configure the **address-assignment** statements in the **[edit routing-instances]** hierarchy level.

Configuring Static Address Assignments

You can optionally create a static IPv4 address binding by reserving a specific address for a particular client. The address is removed from the address-assignment pool so that it is not assigned to another client. When you reserve an address, you identify the client host and create a binding between the client MAC address and the assigned IP address.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

To configure a static IPv4 address binding:

1. Specify the name of the IPv4 address-assignment pool containing the IP address you want to reserve for the client.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Specify the name of the client for the static binding, the client MAC address, and the IP address to reserve for the client. This configuration specifies that the client with MAC address 01:03:05:07:09:0b is always assigned IP address 192.168.10.2.

```
[edit access address-assignment pool blr-pool family inet]
user@host# set host svale6_boston_net hardware-address 01:03:05:07:09:0b
   ip-address 192.168.10.2
```

NOTE: To configure static binding for an IPv4 address in a routing instance, configure the address-assignment statements in the [edit routing-instances] hierarchy.

Configuring Address-Assignment Pool Linking

Address-assignment pool linking enables you to specify a secondary address pool for the device to use when the primary address-assignment pool is fully allocated. When the primary pool has no available addresses remaining, the device automatically switches over to the linked secondary pool and begins allocating addresses from that pool. The device uses a secondary pool only when the primary address-assignment pool is fully allocated.

You can create a chain of multiple linked pools. For example, you can link pool A to pool B, and link pool B to pool C. When pool A has no available addresses, the device switches to pool B for addresses. When pool B is exhausted, the device switches to pool C. There is no limit to the number of linked pools in a chain. However, you cannot create multiple links to or from the same pool—a pool can be linked to only one secondary pool, and a secondary pool can be linked from only one primary pool.

To link a primary address-assignment pool named pool1 to a secondary pool named pool2 on SRX1500, SRX5400, SRX5600, or SRX5800 devices:

```
[edit access address-assignment]
user@host# set pool pool1 link pool2
```

Related Documentation

- DHCP Overview on page 713
- DHCP Server on page 718
- DHCP Client on page 733
- DHCP Relay Agent on page 742

DHCP Client

SRX Series device can act as a DHCP client, receiving its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. The device can also act as a DHCP server, providing TCP/IP settings and IP addresses to clients in any zone. For more information, read this topic.

- Understanding DHCP Client Operation on page 733
- Minimum DHCP Client Configuration on page 734
- Configuring DHCP Client-Specific Attributes for Address-Assignment Pools on page 734
- Configuring Optional DHCP Client Attributes on page 735
- Verifying and Managing DHCP Client Configuration on page 736
- Example: Configuring the Device as a DHCP Client on page 737

Understanding DHCP Client Operation

A Juniper Networks device can act as a DHCP client, receiving its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. The device can also act as a DHCP server, providing TCP/IP settings and IP addresses to clients in any zone. When the device operates as a DHCP client and a DHCP server simultaneously, it can transfer the TCP/IP settings learned through its DHCP client module to its default DHCP server module. For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP server in the network. You set the vendor class ID, lease time, DHCP server address, retransmission attempts, and retry interval. You can renew DHCP client releases.

DHCP client operations are supported on all SRX Series devices in chassis cluster mode.

See Also

- *DHCP Server, Client, and Relay Agent Overview*
- Understanding DHCP Relay Agent Operation on page 742
- *DHCP Settings and Restrictions Overview*

Minimum DHCP Client Configuration

The following sample output shows the minimum configuration you must use to configure an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DHCP client. In this output, the interface is ge-0/0/0 and the logical unit is 0.

```
[edit interfaces]
   ge-0/0/0 {
      unit 0 {
         family inet {
            dhcp-client
      }
   }
}
```

NOTE: To configure a DHCP client in a routing instance, add the interface in a routing instance using the **[edit routing-instances]** hierarchy.

Configuring DHCP Client-Specific Attributes for Address-Assignment Pools

You use the address-assignment pool feature to include application-specific attributes when clients obtain an address. The client application, such as DHCP, uses the attributes to determine how addresses are assigned and to provide optional application-specific characteristics to the client. For example, the DHCP application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCP specifies additional DHCP attributes such as the boot file that the client uses, the DNS server, and the maximum lease time.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

You use the **dhcp-attributes** statement to configure DHCP client-specific attributes for address-assignment pools.

To configure address-assignment pool attributes for DHCP clients:

1. Specify the name of the address-assignment pool.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Configure optional DHCP client attributes.

```
[edit access address-assignment pool blr-pool family inet]
user@host# set dhcp-attributes maximum-lease-time 2419200
user@host# set dhcp-attributes name-server 192.168.10.2
```

```
user@host# set dhcp-attributes boot-file boot-file.txt
user@host# set dhcp-attributes boot-file boot-server example.com
```

NOTE: To configure DHCP client-specific attributes in a routing instance, configure the dhcp-attributes statements in the [edit routing-instances] hierarchy.

Configuring Optional DHCP Client Attributes

For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP local server in the network. You can then set the client-identifier, options no-hostname, lease time, retransmission attempts, retry interval, preferred DHCP local server address, and vendor class ID.

To configure optional DHCP client attributes on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Configure the DHCP client identifier prefix as the routing instance name.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set client-identifier prefix host
```

2. Configure the DHCP options no-hostname if you do not want the client to send hostname (RFC option code 12) in the packets.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```

3. Set the DHCP lease time.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

4. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```

5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```

6. Set the IPv4 address of the preferred DHCP local server.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set server-address 10.1.1.1
```

7. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```

NOTE: To configure the DHCP client in a routing instance, configure the interface in the **[edit routing-instances]** hierarchy.

Verifying and Managing DHCP Client Configuration

Purpose View or clear information about client address bindings and statistics for the DHCP client on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

Action

- To display the address bindings in the client table on the DHCP client:

```
user@host> show dhcp client binding
```

- To display DHCP client statistics:

```
user@host> show dhcp client statistics
```

- To clear the binding state of a DHCP client from the client table on the DHCP client:

```
user@host> clear dhcp client binding
```

- To clear all DHCP client statistics:

```
user@host> clear dhcp client statistics
```

NOTE: To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- **show dhcp client binding routing instance** *<routing-instance name>*
- **show dhcp client statistics routing instance** *<routing-instance name>*
- **clear dhcp client binding routing instance** *<routing-instance name>*
- **clear dhcp client statistics routing instance** *<routing-instance name>*

Example: Configuring the Device as a DHCP Client

This example shows how to configure the device as a DHCP client.

Requirements

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet. You can use the **show system services dhcp pool** CLI command to view information on DHCP address pools.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices. See the *Understanding Management Predefined Policy Applications*.
- Determine the DHCP options required by the subnets and clients in your network. See "Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server" on page 553

Overview

In this example, you configure the device as a DHCP client. You specify the interface as ge-0/0/2, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as 00:0a:12:00:12:12 in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the options no-hostname if you do not want the DHCP client to send the hostname with the packets. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds.

Then you set the number of retransmission attempts to 6. The range is from 0 through 50,000, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Set the force-discover option if you want to force the DHCP client to send a DHCP discover packet after one to three failed dhcp-request attempts. The force-discover option ensures that the DHCP server will assign the same or a new IP address to the client. Finally, you set the IPv4 address of the preferred DHCP server to 10.1.1.1 and the vendor class ID to ether.

WARNING: Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI is supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on

a device that already has the DHCPD configuration, the following warning messages are displayed:

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.

NOTE: Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option **dhcp-client** at **[edit interfaces interface-name unit logical-unit-number family inet]** hierarchy is changed to **dhcp** to align with other Junos platforms. There is no change in the functionality.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/2 unit 0 family inet dhcp-client client-identifier prefix host-name
set interfaces ge-0/0/2 unit 0 family inet dhcp-client lease-time 86400
set interfaces ge-0/0/2 unit 0 family inet dhcp-client retransmission-attempt 6
set interfaces ge-0/0/2 unit 0 family inet dhcp-client retransmission-interval 5
set interfaces ge-0/0/2 unit 0 family inet dhcp-client force-discover
set interfaces ge-0/0/2 unit 0 family inet dhcp-client server-address 192.168.2.1
set interfaces ge-0/0/2 unit 0 family inet dhcp-client vendor-id ether
set interfaces ge-0/0/2 unit 0 family inet dhcp-client options no-hostname
```

GUI Step-by-Step Procedure

To configure the device as a DHCP client:

1. In the J-Web interface, select **Configure** > **Services** > **DHCP** > **DHCP Client**.
2. Under Interfaces, add **ge-0/0/2.0**.
3. Configure the DHCP client identifier as either an ASCII or hexadecimal value.
4. From the Client identifier choice list, select **hexadecimal**.
5. In the Hexadecimal box, type the client identifier—**00:0a:12:00:12:12**.
6. Set the DHCP lease time in seconds. This is the lease time in seconds requested in a DHCP client protocol packet; the range is 60 through 2,147,483,647. Type **86400**.

7. Set the retransmission number of attempts to 6. This is the number of attempts to retransmit the DHCP client protocol packet. The range is 0 through 6.

8. Set the retransmission interval in seconds to 5. This is the number of seconds between successive transmissions. The range is 4 through 64. The default is 4 seconds.

9. Configure the force-discover option to force the DHCP client to send a DHCP discover packet after one to three failed **dhcp-request** attempts.

10. Set the IPv4 address of the preferred DHCP server. Type **192.168.2.1**.

11. Set the vendor class ID. This is the vendor class identification for the DHCP client. Type **ether**.

12. Configure options no-hostname if you do not want the client to send hostname in the packets (RFC option code 12).

13. Click **OK**.

14. If you are done configuring the device, click **Commit** >.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the device as a DHCP client:

1. Specify the DHCP client interface.

```
[edit]
user@host# edit interfaces ge-0/0/2 unit 0 family inet dhcp-client
```

2. Configure the DHCP client identifier as a hexadecimal value.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set client-identifier prefix host
```

3. Set the DHCP lease time.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

4. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```

5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```

6. Configure the force-discover option.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set force-discover.
```

7. Set the IPv4 address of the preferred DHCP server.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set server-address 192.168.2.1
```

8. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```

9. Configure options no-hostname if you do not want the client to send the hostname in packets.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```

Results From configuration mode, confirm your configuration by entering the **show interfaces ge-0/0/2 unit 0 family inet** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces ge-0/0/2 unit 0 family inet
dhcp-client {
   client-identifier hexadecimal 00:0a:12:00:12:12;
   options no-hostname;
   lease-time 86400;
   retransmission-attempt 6;
   retransmission-interval 5;
   force-discover;
   server-address 192.168.2.1;
   update-server;
   vendor-id ether;
```

```
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying the DHCP Client on page 741

Verifying the DHCP Client

Purpose Verify that the DHCP client information has been configured.

Action From operational mode, enter these commands:

- **show dhcp client binding** command to display the binding state of a Dynamic Host Configuration Protocol (DHCP) client.
- **show dhcp client statistics** command to display client statistics.

These commands produce the following sample output:

```
user@host> show dhcp client binding
```

```
IP address        Hardware address   Expires     State      Interface
192.168.2.2       88:a2:5e:0a:d6:03  2419093     BOUND      ge-0/0/2.0
```

```
user@host> show dhcp client statistics
```

```
Packets dropped:
    Total                     2
    Send error                2

Messages received:
    BOOTREPLY                 6
    DHCPOFFER                 4
    DHCPACK                   2
    DHCPNAK                   0
    DHCPFORCERENEW            0

Messages sent:
    BOOTREQUEST               39
    DHCPDECLINE               0
    DHCPDISCOVER              23
    DHCPREQUEST               16
    DHCPINFORM                0
    DHCPRELEASE               0
    DHCPRENEW                 0
    DHCPREBIND                0
```

See Also

- *DHCP Server, Client, and Relay Agent Overview*
- Understanding DHCP Server Operation on page 718
- *DHCP Settings and Restrictions Overview*

Release History Table

Release	Description
17.3R1	Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option **dhcp-client** at **[edit interfaces interface-name unit logical-unit-number family inet]** hierarchy is changed to **dhcp** to align with other Junos platforms.
15.1X49-D60	Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI is supported.

Related Documentation

- DHCP Overview on page 713
- DHCP Server on page 718
- DHCP Address-Assignment Pools on page 729
- DHCP Relay Agent on page 742
- DHCPv6 Server on page 758

DHCP Relay Agent

The DHCP relay agent operates as the interface between DHCP clients and the server. The DHCP Relay Agent relays DHCP messages between DHCP clients and DHCP servers on different IP networks. For more information, read this topic.

- Understanding DHCP Relay Agent Operation on page 742
- Example: Minimum JDHCP Relay Agent Configuration on page 743
- Example: Configuring JDHCP Relay Configuration on page 743
- Example: Configuring the Device as a BOOTP or DHCP Relay Agent using Legacy DHCP Deamon Command on page 753

Understanding DHCP Relay Agent Operation

A Juniper Networks device operating as a DHCP relay agent forwards incoming requests from BOOTP and DHCP clients to a specified BOOTP or DHCP server. Client requests can pass through virtual private network (VPN) tunnels.

You cannot configure a single device interface to operate as both a DHCP client and a DHCP relay.

NOTE: The DHCP requests received on an interface are associated to a DHCP pool that is in the same subnet as the primary IP address/subnet on an interface. If an interface is associated with multiple IP addresses/subnets, the device uses the lowest numerically assigned IP address as the primary IP address/subnet for the interface. To change the IP address/subnet that is listed as the primary address on an interface, use the **set interfaces < interface name > unit 0 family inet xxx.xxx.xxx.xxx/yy primary** command and commit the change.

See Also

- *DHCP Server, Client, and Relay Agent Overview*
- Understanding DHCP Server Operation on page 718
- *DHCP Settings and Restrictions Overview*

Example: Minimum JDHCP Relay Agent Configuration

This example shows the minimum configuration you need to use the extended DHCP relay agent on the router or switch:

```
[edit forwarding-options]
dhcp-relay {
   server-group {
      test 203.0.113.21;
   }
   active-server-group test;
   group all {
      interface fe-0/0/2.0;
   }
}
```

NOTE: The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.

This example creates a server group and an active server group named **test** with IP address 203.0.113.21. The DHCP relay agent configuration is applied to a group named **all**. Within this group, the DHCP relay agent is enabled on interface fe-0/0/2.0.

Example: Configuring JDHCP Relay Configuration

The DHCP relay agent operates as the interface between DHCP clients and the server. The DHCP Relay Agent relays DHCP messages between DHCP clients and DHCP servers on different IP networks.

This example describes how to configure the DHCP relay agent on the SRX Series device. SRX series device acting as DHCP relay agent is responsible for forwarding the requests

and responses between the DHCP clients and the server which are part of different routing instances.

Requirements

This example uses the following hardware and software components:

- SRX Series devices with Junos OS 15.1X49-D10 or later.

Overview

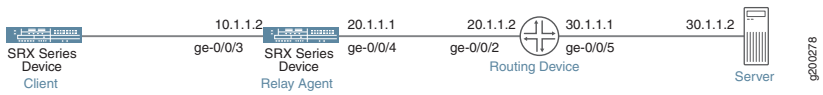
You can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing instances. This type of configuration is for DHCP relay connection between a DHCP server and a DHCP client, when the DCHP server resides in a network that is isolated from the client network.

Topology

To exchange DHCP messages between different routing instances, you must enable both the server-facing interface and the client-facing interface of the DHCP relay agent to recognize and forward DHCP packets.

The following Figure 43 on page 744 shows DHCP performance as DHCP local server, DHCP client, and DHCP relay agent

Figure 43: Understanding DHCP Services in a Routing Instance



The following list provides an overview of the tasks required to create the DHCP message exchange between the different routing instances:

- Configure the client-facing side of the DHCP relay agent.
- Configure the server-facing side of the DHCP relay agent.
- Configure the Security Zone to Allow the DHCP protocol.

Table1: DHCP Relay Parameters:

Parameters	Cleint-Side-Details	Server-Side-Details
interface	ge-0/0/3.0	ge-0/0/3.0

Parameters	Cleint-Side-Details	Server-Side-Details
routing interface	trust-vr	untrust-vr
ip address	10.1.1.2/24	20.1.1.1/24

NOTE: In order to make this setup work, the DHCP server connecting route and relay agent interface route must be in both routing-instances. For example, in the above topology, the server route 30.1.1.0/24 needs to be shared with the dhcp-relay VR, and the dhcp-relay interface route 10.1.1.0/24 exact needs to be shared with the default routing instance.

Also, a dummy dhcp-relay config must be added in the routing instance with the DHCP server. If this is not configured, dhcp-relay will not be able to receive packets from the DHCP server.

Configuration

CLI Quick Configuration

The following procedures describe the configuration tasks for creating the DHCP message exchange between the DHCP server and clients in different routing instances. To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

Quick configuration for Client-Facing Support:

```
set routing-instances trust-vr instance-type virtual-router
set routing-instances trust-vr interface ge-0/0/3.0
set interfaces ge-0/0/3 unit 0 family inet address 10.1.1.2/24
set routing-instances trust-vr routing-options instance-import routing-policy-VR1
set routing-instances trust-vr forwarding-options dhcp-relay forward-only-replies
```

Quick configuration for Server-Facing Support:

```
set routing-instances untrust-vr instance-type virtual-router
set routing-instances untrust-vr interface ge-0/0/4.0
set interfaces ge-0/0/4 unit 0 family inet address 20.1.1.1/24
```

Quick configuration for DHCP Relay Support:

```
set routing-instances trust-vr forwarding-options dhcp-relay server-group server-1 30.1.1.2
set routing-instances trust-vr forwarding-options dhcp-relay active-server-group server-1
set routing-instances untrust-vr forwarding-options dhcp-relay server-group
    dummy-config
set routing-instances trust-vr forwarding-options dhcp-relay group relay-in-vr interface
    ge-0/0/3.0
set routing-instances trust-vr routing-options interface-routes rib-group inet untrust-trust
```

```
set routing-instances trust-vr routing-options static route 30.1.1.2/32 next-hop 20.1.1.2
set routing-instances trust-vr routing-options instance-import export_dhcp_server_route
set routing-instances untrust-vr routing-options interface-routes rib-group inet
    untrust-trust
set routing-instances untrust-vr routing-options instance-import
    import_relay_route_to_server_vr
set policy-options policy-statement export_dhcp_server_route term 1 from instance
    untrust-vr
set policy-options policy-statement export_dhcp_server_route term 1 from route-filter
    30.1.1.0/24 exact
set policy-options policy-statement export_dhcp_server_route term 1 then accept
set policy-options policy-statement export_dhcp_server_route term 2 then reject
set policy-options policy-statement import_relay_route_to_server_vr term 1 from instance
    trust-vr
set policy-options policy-statement import_relay_route_to_server_vr term 1 from route-filter
    10.1.1.0/24 exact
set policy-options policy-statement import_relay_route_to_server_vr term 1 then accept
set policy-options policy-statement import_relay_route_to_server_vr term 2 then reject
set routing-options static route 30.1.1.2/32 next-table untrust-vr.inet.0
set routing-options rib-groups untrust-trust import-rib untrust-vr.inet.0
set routing-options rib-groups untrust-trust import-rib trust-vr.inet.0
```

Quick configuration for Security Zone to Allow the DHCP Protocol:

```
set security policies default-policy permit-all
set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-traffic
    system-services all
set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-traffic
    protocols all
set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic
    system-services all
set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic protocols
    all
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure support on the client-facing side of the DHCP relay agent:

1. Set a routing instance type as virtual router.

   ```
   [edit]
   user@host# set routing-instances trust-vr instance-type virtual-router
   ```

2. Set an interface to the virtual router

   ```
   [edit]
   user@host# set routing-instances trust-vr interface ge-0/0/3.0
   ```

3. Set the IP address to the interface.

```
[edit]
user@host# set interfaces ge-0/0/3 unit 0 family inet address 10.1.1.2/24
```

4. Set the routing-policy VR1.

```
[edit]
user@host# set routing-instances trust-vr routing-options instance-import
  routing-policy-VR1
```

5. Set the forward-only-replies option.

```
[edit]
user@host# set routing-instances trust-vr forwarding-options dhcp-relay
  forward-only-replies
```

Step-by-Step Procedure

To configure support on the server-facing side of the DHCP relay agent:

1. Set a virtual router.

```
[edit]
user@host# set routing-instances untrust-vr instance-type virtual-router
```

2. Set an interface to the virtual router.

```
[edit]
user@host# set routing-instances untrust-vr interface ge-0/0/4.0
```

3. Set the IP address to the interface.

```
[edit]
user@host# set interfaces ge-0/0/4 unit 0 family inet address 20.1.1.1/24
```

Step-by-Step Procedure

To configure the DHCP local server to support:

1. Set the server group by specifying the name of the group and DHCP server addresses for the use by the extended DHCP relay agent.

```
[edit ]
user@host# set routing-instances trust-vr forwarding-options dhcp-relay
  server-group server-1 30.1.1.2
```

2. Set an active server group to apply a common DHCP relay agent configuration to a named group of DHCP server addresses.

```
[edit ]
```

```
user@host# set routing-instances trust-vr forwarding-options dhcp-relay
  active-server-group server-1
```

3. Set a dummy dhcp-relay in DHCP server routing instance.

```
[edit ]
user@host# set routing-instances untrust-vr forwarding-options dhcp-relay
  server-group dummy-config
user@host# set routing-instances trust-vr forwarding-options dhcp-relay group
  relay-in-vr interface ge-0/0/3.0
```

4. Set the configuration in dhcp-relay routing instance.

```
[edit ]
user@host# set routing-instances trust-vr routing-options interface-routes rib-group
  inet untrust-trust
user@host# set routing-instances trust-vr routing-options static route 30.1.1.2/32
  next-hop 20.1.1.2
user@host# set routing-instances trust-vr routing-options instance-import
  export_dhcp_server_route
user@host# set routing-instances untrust-vr routing-options interface-routes
  rib-group inet untrust-trust
user@host# set routing-instances untrust-vr routing-options instance-import
  import_relay_route_to_server_vr
```

5. Set the configuration to share routes between routing instances.

```
[edit ]
user@host# set policy-options policy-statement export_dhcp_server_route term 1
  from instance untrust-vr
user@host# set policy-options policy-statement export_dhcp_server_route term 1
  from route-filter 30.1.1.0/24 exact
user@host# set policy-options policy-statement export_dhcp_server_route term 1
  then accept
user@host# set policy-options policy-statement export_dhcp_server_route term 2
  then reject
user@host# set policy-options policy-statement import_relay_route_to_server_vr
  term 1 from instance trust-vr
user@host# set policy-options policy-statement import_relay_route_to_server_vr
  term 1 from route-filter 10.1.1.0/24 exact
user@host# set policy-options policy-statement import_relay_route_to_server_vr
  term 1 then accept
user@host# set policy-options policy-statement import_relay_route_to_server_vr
  term 2 then reject
user@host# set routing-options static route 30.1.1.2/32 next-table untrust-vr.inet.0
user@host# set routing-options rib-groups untrust-trust import-rib untrust-vr.inet.0
```

NOTE: You can enable an SRX Series device to function as a DHCP local server. The DHCP local server provides an IP address and other configuration information in response to a client request.

Step-by-Step Procedure

To configure the security zone to allow the DHCP Protocol:

1. Set the default security policy to permit all traffic.

```
[edit ]
user@host# set security policies default-policy permit-all
```

2. Set all system services and protocols on interface ge-0/0/4.0.

```
[edit ]
user@host# set security zones security-zone untrust interfaces ge-0/0/4.0
   host-inbound-traffic system-services all
user@host# set security zones security-zone untrust interfaces ge-0/0/4.0
   host-inbound-traffic protocols all
```

3. Set all system services and protocols on interface ge-0/0/3.0.

```
[edit ]
user@host# set security zones security-zone trust interfaces ge-0/0/3.0
   host-inbound-traffic system-services all
user@host# set security zones security-zone trust interfaces ge-0/0/3.0
   host-inbound-traffic protocols all
```

Results

- Result for Client-facing Support:

From configuration mode, confirm your configuration by entering the **show routing-instances** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show routing-instances
trust-vr {
   instance-type virtual-router;
   routing-options {
      instance-import routing-policy-VR1;
   }
   interface ge-0/0/3.0;
   forwarding-options {
      dhcp-relay {
         forward-only-replies;
      }
   }
}
```

- Result for Server-Facing Support:

  From configuration mode, confirm your configuration by entering the **show routing-instances** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show routing-instances
untrust-vr {
  instance-type virtual-router;
    interface ge-0/0/4.0;
  }
```

- Result for DHCP Local Server Support:

  From configuration mode, confirm your configuration by entering the **show routing-instances**, **show policy-options** and **show routing-options** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show routing-instances
trust-vr {
  instance-type virtual-router;
  routing-options {
    static {
      route 30.1.1.2/32 next-hop 20.1.1.2;
    }
    interface-routes {
      rib-group inet untrust-trust;
    }
    instance-import export_dhcp_server_route;
  }
  interface ge-0/0/3.0;
  forwarding-options {
    dhcp-relay {
      server-group {
        server-1 {
          30.1.1.2;
        }
      }
      active-server-group server-1;
      group relay-in-vr {
        interface ge-0/0/3.0;
      }
    }
  }
}
untrust-vr {
  instance-type virtual-router;
  routing-options {
    interface-routes {
      rib-group inet untrust-trust;
    }
```

```
      instance-import import_relay_route_to_server_vr;
    }
    interface ge-0/0/4.0;
    forwarding-options {
      dhcp-relay {
        server-group {
          dummy-config;
        }
      }
    }
}
[edit]
user@host# show policy-options
policy-statement export_dhcp_server_route {
    term 1 {
      from {
        instance untrust-vr;
        route-filter 30.1.1.0/24 exact;
      }
      then accept;
    }
    term 2 {
      then reject;
    }
}
policy-statement import_relay_route_to_server_vr {
    term 1 {
      from {
        instance trust-vr;
        route-filter 10.1.1.0/24 exact;
      }
      then accept;
    }
    term 2 {
      then reject;
    }
}
[edit]
user@host#  show routing-options
    static {
      route 30.1.1.2/32 next-table untrust-vr.inet.0;
    }
    rib-groups {
      untrust-trust {
        import-rib [ untrust-vr.inet.0 trust-vr.inet.0 ];
      }
    }
```

- Result for Security Zone to Allow the DHCP Protocol:

  From configuration mode, confirm your configuration by entering the **show security policies** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
default-policy {
   permit-all;
}
[edit]
user@host# show security zones
   security-zone HOST {
      interfaces {
         all;
      }
   }
   security-zone untrust {
      interfaces {
         ge-0/0/4.0 {
            host-inbound-traffic {
               system-services {
                  all;
               }
               protocols {
                  all;
               }
            }
         }
      }
   }
   security-zone trust {
      interfaces {
         ge-0/0/3.0 {
            host-inbound-traffic {
               system-services {
                  all;
               }
               protocols {
                  all;
               }
            }
         }
      }
   }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the DHCP Relay Statistics Configuration:

Purpose Verify that the DHCP Relay Statistics has been configured.

Action

- From operational mode, enter the **show dhcp relay statistics routing-instance dhcp-relay** command.

```
Packets dropped:
Total 0

Messages received:
BOOTREQUEST 1
DHCPDECLINE 0
DHCPDISCOVER 0
DHCPINFORM 0
DHCPRELEASE 0
DHCPREQUEST 1

Messages sent:
BOOTREPLY 1
DHCPOFFER 0
DHCPACK 1
DHCPNAK 0
DHCPFORCERENEW 0
```

Verifying DHCP client bindings in the routing instance.

Purpose Verify that the DHCP client bindings in the routing instances has been configured.

Action

- From operational mode, enter the **show dhcp relay binding routing-instance dhcp-relay** command.

```
IP address   Session Id  Hardware address   Expires   State     Interface
10.10.10.2   14          00:0c:29:e9:6d:00  86381     BOUND     ge-0/0/1.0
```

Example: Configuring the Device as a BOOTP or DHCP Relay Agent using Legacy DHCP Deamon Command

This example shows how to configure the device as a BOOTP or DHCP relay agent.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you enable the DHCP relay agent to relay BOOTP or DHCP messages to a BOOTP server. You specify the IP time-to-live value to be set in responses to the client as 20. The range is from 1 through 255. You then set the maximum number of hops allowed per packet to 10. The range is from 1 through 16.

Then you specify the minimum number of seconds before requests are forwarded as 300. The range is from 0 through 30,000 seconds.

You then specify the IP time-to-live value to be set in responses to the client as 30. The range is from 1 through 255. You set the description of the server as text and the DHCP option as 82. You set the maximum number of hops allowed per packet to 16 and specify the minimum number of seconds as 400 before requests are forwarded.

WARNING: Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI is supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set forwarding-options helpers bootp client-response-ttl 20
set forwarding-options helpers bootp maximum-hop-count 10
set forwarding-options helpers bootp minimum-wait-time 300
set forwarding-options helpers bootp description text
set forwarding-options helpers bootp interface ge-0/0/0 client-response-ttl 30
set forwarding-options helpers bootp interface ge-0/0/0 description text
set forwarding-options helpers bootp interface ge-0/0/0 dhcp-option82
set forwarding-options helpers bootp interface ge-0/0/0 maximum-hop-count 16
set forwarding-options helpers bootp interface ge-0/0/0 minimum-wait-time 400
```

GUI Step-by-Step Procedure

To configure the device as a BOOTP/DHCP relay agent:

1. In the Client response TTL box, type **20**.
2. In the Maximum hop count box, type **10**.
3. In the Minimum wait time box, type **300**.
4. In the Description box, type the description of the server.
5. In the Client response TTL box, type **30**.
6. In the Description box, type the description of the server.
7. Select the **Dhcp option 82** check box.
8. In the Maximum hop count box, type **16**.
9. In the Minimum wait time box, type **400**.
10. Click **OK** until you return to the Configuration page.
11. Click **OK** to check your configuration and save it as a candidate configuration.
12. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the device as a BOOTP or DHCP relay agent:

1. Specify the IP time-to-live value in BOOTP response messages sent to a BOOTP client.

```
[edit forwarding-options helpers bootp]
user@host# set client-response-ttl 20
```

2. Specify the maximum number of hops allowed per packet.

```
[edit forwarding-options helpers bootp]
user@host# set maximum-hop-count 10
```

3. Specify the minimum wait time in seconds.

```
[edit forwarding-options helpers bootp]
user@host# set minimum-wait-time 300
```

4. Specify the description of the server.

```
[edit forwarding-options helpers bootp]
user@host# set description text
```

5. Define the incoming BootP request forwarding interface.

```
[edit forwarding-options helpers bootp]
user@host# set interface ge-0/0/0
```

6. Define the IP time-to-live value.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set client-response-ttl 30
```

7. Specify the description of the server.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set description text
```

8. Set the DHCP option 82.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set dhcp-option82
```

9. Specify the maximum number of hops allowed per packet.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set forwarding-options helpers bootp interface ge-0/0/0
  maximum-hop-count 16
```

10. Specify the minimum wait time.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set minimum-wait-time 400
```

Results From configuration mode, confirm your configuration by entering the **show forwarding-options** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
```

```
user@host# show forwarding-options
  helpers {
    bootp {
      description text;
      maximum-hop-count 10;
      minimum-wait-time 300;
      client-response-ttl 20;
      interface {
        ge-0/0/0 {
          description text;
          maximum-hop-count 16;
          minimum-wait-time 400;
          client-response-ttl 30;
          dhcp-option82;
        }
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying DHCP Relay Statistics

Purpose Verify that the DHCP Relay statistics have been configured.

Action From operational mode, enter the **show system services dhcp relay-statistics** command.

```
user@host> show system services dhcp relay-statistics
```

```
Received Packets:    4 Forwarded Packets              4 Dropped Packets
         4     Due to missing interface in relay database: 4     Due to missing
matching routing instance: 0     Due to an error during packet read: 0     Due
to an error during packet send: 0     Due to invalid server address: 0     Due
to missing valid local address: 0     Due to missing route to server/client: 0
```

See Also

- *DHCP Server, Client, and Relay Agent Overview*
- *DHCP Settings and Restrictions Overview*

Release History Table

Release	Description
15.1X49-D60	Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI is supported.

Related Documentation

- DHCP Server on page 718
- DHCP Address-Assignment Pools on page 729
- DHCP Client on page 733

DHCPv6 Server

SRX Series device can act as a DHCPv6 server and allocates IP addresses to IPv6 clients. DHCPv6 server also delivers configuration settings to client hosts on a subnet or to the requesting devices that need an IPv6 prefix. For the DHCPv6 server to allow DHCPv6 requests, you must create a security policy to enable DHCPv6 traffic. For more information, read this topic.

- DHCPv6 Server Overview on page 758
- Creating a Security Policy to Enable DHCPv6 Traffic on page 759
- Example: Configuring DHCPv6 Server Options on page 760
- Understanding Cascaded DHCPv6 Prefix Delegating on page 764
- Example - Configuring DHCPv6 Prefix Delegation (PD) over Point-to-Point Protocol over Ethernet (PPPoE) on page 765

DHCPv6 Server Overview

A Dynamic Host Configuration Protocol version 6 (DHCPv6) server can automatically allocate IP addresses to IPv6 clients and deliver configuration settings to client hosts on a subnet or to the requesting devices that need an IPv6 prefix. A DHCPv6 server allows network administrators to manage pool of IP addresses centrally among hosts and to automate the assignment of IP addresses in a network.

NOTE: SRX Series devices do not support DHCP client authentication. In a DHCPv6 deployment, security policies control access through the device for any DHCP client that has received an address and other attributes from the DHCPv6 server.

Some features include:

- Configuration for a specific interface or a group of interfaces
- Stateless address autoconfiguration (SLAAC)

- Prefix delegation, including access-internal route installation
- DHCPv6 server groups

The DHCPv6 server configuration usually consists of DHCPv6 options for clients, an IPv6 prefix, an address pool that contains IPv6 address ranges and options, and a security policy to allow DHCPv6 traffic. In a typical setup the provider Juniper Networks device is configured as an IPv6 prefix delegation server that assigns addresses to the customer edge device. The customer's edge router then provides addresses to internal devices.

To configure DHCPv6 local server on a device, you include the DHCPv6 statement at the **[edit system services dhcp-local-server]** hierarchy level. You then create an address assignment pool for DHCPv6 that is configured in the **[edit access address-assignment pool]** hierarchy level using the **family inet6** statement.

You can also include the **dhcpv6** statement at the **[edit routing-instances *routing-instance-name* system services dhcp-local-server]** hierarchy.

NOTE: Existing DHCPv4 configurations in the **[edit system services dhcp]** hierarchy are not affected when you upgrade to Junos OS Release 10.4 from an earlier version or enable DHCPv6 server.

See Also
- Example: Configuring an Address-Assignment Pool for IPv6 Addresses on page 794
- Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment on page 797

Creating a Security Policy to Enable DHCPv6 Traffic

For the DHCPv6 server to allow DHCPv6 requests, you must create a security policy to enable DHCPv6 traffic. In this example, the zone my-zone allows DHCPv6 traffic from the zone untrust, and the ge-0/0/3.0 interface is configured with the IPv6 address 2001:db8:3001::1.

To create a security zone policy to allow DHCPv6 on SRX1500, SRX5400, SRX5600, and SRX5800 devices:

1. Create the zone and add an interface to that zone.

```
[edit security zones]
user@host# edit security-zone my-zone interfaces ge-0/0/3.0
```

2. Configure host inbound traffic system services to allow DCHPv6.

```
[edit security zones security-zone my-zone interfaces ge-0/0/3.0]
user@host# set host-inbound-traffic system-services dhcpv6
```

3. If you are done configuring the device, enter **commit** from configuration mode.

See Also
- Example: Configuring an Address-Assignment Pool for IPv6 Addresses on page 794

Example: Configuring DHCPv6 Server Options

This example shows how to configure DHCPv6 server options on SRX1500, SRX5400, SRX5600, and SRX5800 devices.

Requirements

Before you begin:

- Determine the IPv6 address pool range.
- Determine the IPv6 prefix. See the *Understanding Address Books*.
- Determine the grace period, maximum lease time, or any custom options that should be applied to clients.
- List the IP addresses that are available for the devices on your network; for example, DNS and SIP servers.

Overview

In this example, you set a default client limit as 100 for all DHCPv6 groups. You then create a group called my-group that contains at least one interface. In this case, the interface is ge-0/0/3.0. You set a range of interfaces using the upto command and set a custom client limit as 200 for group my-group that overrides the default limit. Finally, you configure interface ge-0/0/3.0 with IPv6 address 2001:db8:3001::1/64 and set router advertisement for interface ge-0/0/3.0. Starting with Junos OS Release 15.X49-D70 and Junos OS Release 17.3R1, you can add the option **dynamic-server** to dynamically support prefix and attributes that are updated by the WAN server.

NOTE: A DHCPv6 group must contain at least one interface.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system services dhcp-local-server dhcpv6 overrides interface-client-limit 100
set system services dhcp-local-server dhcpv6 group my-group interface ge-0/0/3.0
```

```
set system services dhcp-local-server dhcpv6 group my-group interface ge-0/0/3.0 upto
  ge-0/0/6.0
set system services dhcp-local-server dhcpv6 group my-group overrides
  interface-client-limit 200
set interfaces ge-0/0/3 unit 0 family inet6 address 2001:db8:3000::1/64
set protocols router-advertisement interface ge-0/0/3.0 prefix 2001:db8:3000::/64
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure DHCPv6 server options:

1. Configure a DHCP local server.

```
[edit]
user@host# edit system services dhcp-local-server dhcpv6
```

2. Set a default limit for all DHCPv6 groups.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set overrides interface-client-limit 100
```

3. Specify a group name and interface.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group interface ge-0/0/3.0
```

4. Set a range of interfaces.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group interface ge-0/0/3.0 upto ge-0/0/6.0
```

5. Set a custom client limit for the group.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group overrides interface-client-limit 200
```

6. Configure an interface with an IPv6 address.

```
[edit interfaces]
user@host# set ge-0/0/3 unit 0 family inet6 address 2001:db8:3000::1/64
```

7. Set router advertisement for the interface.

```
[edit protocols]
```

```
user@host# set router-advertisement interface ge-0/0/3.0 prefix
  2001:db8:3000::/64
```

Results From configuration mode, confirm your configuration by entering the **show system services dhcp-local-server**, **show interfaces ge-0/0/3**, and **show protocols** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system services dhcp-local-server
dhcpv6 {
  overrides {
  interface-client-limit 100;
  ]
    group my-group {
    overrides {
    interface-client-limit 200;
    }
    interface ge-0/0/3.0 {
      upto ge-0/0/6.0;
    }
  }
}
    [edit]
      user@host# show interfaces ge-0/0/3
    unit 0 {
    family inet6 {
      address 2001:db8:3000::1/64;
    }
  }
    [edit]
      user@host# show protocols
      router-advertisement {
      interface ge-0/0/3.0 {
      prefix 2001:db8:3000::1/64;
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying DHCPv6 Local Server Configuration

Purpose Verify that the client address bindings and statistics for the DHCPv6 local server have been configured

Action From operational mode, enter the **show dhcpv6 server binding** command to display the address bindings in the client table on the DHCPv6 local server.

```
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:bd8:1111:2222::/64 6           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:01
2001:bd8:1111:2222::/64 7           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
2001:bd8:1111:2222::/64 8           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
2001:bd8:1111:2222::/64 9           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:04
2001:bd8:1111:2222::/64 10          86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:05
```

From operational mode, enter the **show dhcpv6 server statistics** command to display the DHCPv6 local server statistics.

```
Dhcpv6 Packets dropped:
    Total               0

Messages received:
    DHCPV6_DECLINE             0
    DHCPV6_SOLICIT             9
    DHCPV6_INFORMATION_REQUEST 0
    DHCPV6_RELEASE             0
    DHCPV6_REQUEST             5
    DHCPV6_CONFIRM             0
    DHCPV6_RENEW               0
    DHCPV6_REBIND              0
    DHCPV6_RELAY_FORW          0
Messages sent:
    DHCPV6_ADVERTISE           9
    DHCPV6_REPLY               5
    DHCPV6_RECONFIGURE         0
    DHCPV6_RELAY_REPL          0
```

- **clear dhcpv6 server bindings all** command to clear all DHCPv6 local server bindings. You can clear all bindings or clear a specific interface, or routing instance.
- **clear dhcpv6 server statistics** command to clear all DHCPv6 local server statistics.

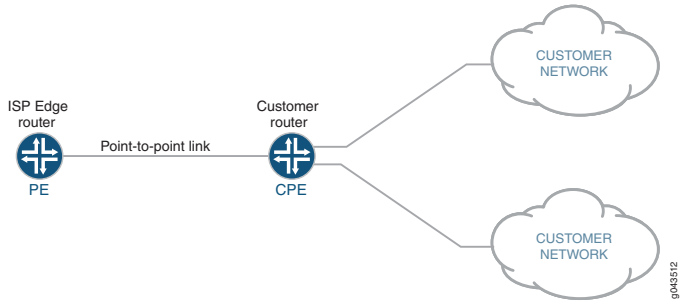
See Also
- Example: Configuring an Address-Assignment Pool for IPv6 Addresses on page 794
- Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment on page 797

Understanding Cascaded DHCPv6 Prefix Delegating

You can use DHCPv6 client prefix delegation to automate the delegation of IPv6 prefixes to the customer premises equipment (CPE). With prefix delegation, a delegating device delegates IPv6 prefixes to a requesting device. The requesting device then uses the prefixes to assign global IPv6 addresses to the devices on the subscriber LAN. The requesting device can also assign subnet addresses to subnets on the LAN.

With cascaded prefix delegation, the IPv6 address block is delegated to a DHCPv6 client that is running on the WAN interface of a customer edge device. The identity association (IA) for the client is used for the identity association for prefix delegation (IA_PD). The CE device requests, through DHCPv6, an IPv6 address with the IA type of nontemporary addresses (IA_NA). Both IA_PD and IA_NA are requesting in the same DHCPv6 exchange.

Figure 44: IPv6 Prefix Delegation

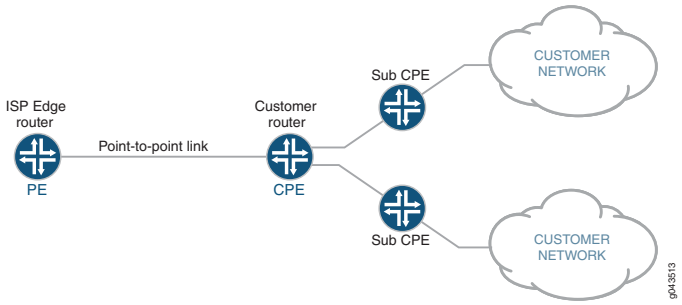


The topology in Figure 44 on page 764shows an SRX Series device acting as the CPE. The WAN interface links to the provider edge (PE) device and the LAN interfaces link to the customer networks. The service provider delegates a prefix (delegated-prefix) and an IPv6 address (cpe-wan-ipv6-address) to a DHCPv6 client. When a requesting device receives that IPv6 address through the DHCPv6 client, the device must install the IPv6 address on its WAN interface. The DHCPv6 client then divides the delegated prefix into sub-prefixes and subsequently assigns them to the connected LAN interfaces of the CPE device, making some subset of the remaining space available for sub-prefix delegation.

A CPE assigns sub-prefixes to its LAN interfaces and broadcasts the sub-prefixes through device advertisement. In this scenario, the CPE acts as a sub-PE and delegates sub-prefixes and assigns them to sub-CPEs.

NOTE: The requirements of sub-prefix delegation are the same as for the prefix delegation defined in RFC 3769.

Figure 45: Sub-prefix Delegation



There can be multi-level sub prefix delegations, see Figure 45 on page 765. The top level CPE gets a delegated prefix from the PE and delegates the sub prefixes to second level sub-CPEs, then to the third level sub-CPEs, and finally to the end levels. The end level sub-CPEs assign the IPv6 address to end hosts through SLAAC, stateless DHCPv6 or stateful DHCPv6. This is called cascaded prefix delegating.

Example - Configuring DHCPv6 Prefix Delegation (PD) over Point-to-Point Protocol over Ethernet (PPPoE)

This example shows how to configure DHCPv6 PD over PPPoE on SRX Series devices.

Requirements

No special configuration beyond the device initialization is required before configuring this feature.

Overview

The example uses SRX550M devices for configuring DHCPv6 PD over PPPoE. Before you begin, configure DHCPv6 server to permit in host-inbound traffic and receive DHCPv6 packet. Provide a host-name to establish PPPoE session. To enable IPv6, chassis reboot is required.

Configuring DHCPv6 PD over PPPoE involves the following configurations:

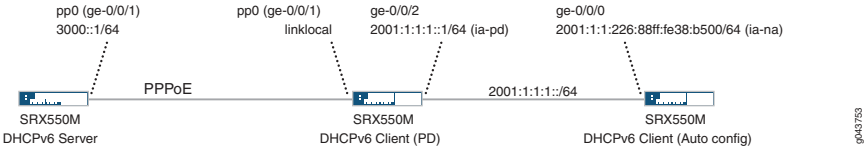
- Configuring DHCPv6 Server
- DHCPv6 Client (PD)
- DHCPv6 Client (Auto)

Topology

The following illustration describes DHCPv6 PD over PPPoE topology which provide a configuration suite using SRX Series devices.

Figure 46 on page 766 shows the topology used in this example.

Figure 46: Configuring SRX Series Devices for DHCPv6 PD over PPPoE



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

Quick configuration for DHCPv6 Server:

- DHCPv6 server configuration

```
set interfaces ge-0/0/2 unit 0 family inet6
set system services dhcp-local-server dhcpv6 overrides interface-client-limit 100
set system services dhcp-local-server dhcpv6 group my-group overrides
  interface-client-limit 200
set system services dhcp-local-server dhcpv6 group my-group overrides delegated-pool
  v6-pd-pool
set system services dhcp-local-server dhcpv6 group my-group interface pp0.0
```

- PPPoE configuration

```
set system host-name SRX550M
set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
set interfaces pp0 unit 0 ppp-options chap access-profile prof-ge001
set interfaces pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
set interfaces pp0 unit 0 pppoe-options server
set interfaces pp0 unit 0 family inet6 address 3000::1/64
```

- Router advertisement configuration

```
set protocols router-advertisement interface pp0.0 max-advertisement-interval 20
set protocols router-advertisement interface pp0.0 min-advertisement-interval 10
set protocols router-advertisement interface pp0.0 managed-configuration
set protocols router-advertisement interface pp0.0 other-stateful-configuration
set protocols router-advertisement interface pp0.0 prefix 3000::1/64
```

- Enable IPv6

```
set security forwarding-options family inet6 mode flow-based
```

- PPPoE profile configuration

```
set access profile prof-ge001 client test_user chap-secret test
```

- PD address pool configuration

```
set access address-assignment pool v6-pd-pool family inet6 prefix 2001:1:1::/48
set access address-assignment pool v6-pd-pool family inet6 range vp-pd prefix-length
  48
set access address-assignment pool v6-pd-pool family inet6 dhcp-attributes dns-server
  3000::1
```

- Security zone configuration

```
set security zones security-zone trust interface pp0.0 host-inbound-traffic
  system-services dhcpv6
```

Quick configuration for DHCPv6 Client (PD):

- DHCPv6 server configuration for autoconfig device

```
set interfaces ge-0/0/2 unit 0 family inet6
set system services dhcp-local-server dhcpv6 overrides interface-client-limit 10
set system services dhcp-local-server dhcpv6 overrides process-inform pool p1
set system services dhcp-local-server dhcpv6 group ipv6 interface ge-0/0/2.0
```

- PPPoE configuration

```
set system host-name SRX550M
set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
set interfaces pp0 unit 0 ppp-options chap default-chap-secret test
set interfaces pp0 unit 0 ppp-options chap local-name test_user
set interfaces pp0 unit 0 ppp-options chap passive
set interfaces pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
set interfaces pp0 unit 0 pppoe-options client
```

- DHCPv6 client configuration

```
set interfaces pp0 unit 0 family inet6 dhcpv6-client client-type statefull
set interfaces pp0 unit 0 family inet6 dhcpv6-client client-ia-type ia-pd
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement
  interface ge-0/0/2.0 other-stateful-configuration
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement
  interface ge-0/0/2.0 max-advertisement-interval 10
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement
  interface ge-0/0/2.0 min-advertisement-interval 5
set interfaces pp0 unit 0 family inet6 dhcpv6-client client-identifier duid-type duid-ll
set interfaces pp0 unit 0 family inet6 dhcpv6-client req-option dns-server
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-server
set protocols router-advertisement interface pp0.0
```

- Enable IPv6

```
set security forwarding-options family inet6 mode flow-based
```

- DHCPv6 server propagate configuration

```
set access address-assignment pool p1 family inet6 prefix 2001::/16
```

```
set access address-assignment pool p1 family inet6 dhcp-attributes propagate-settings
    pp0.0
```

- Security zone configuration

```
set security zones security-zone untrust interface pp0.0 host-inbound-traffic
    system-services dhcpv6
set security zones security-zone trust interface ge-0/0/2.0 host-inbound-traffic
    system-services dhcpv6
```

Quick configuration for DHCPv6 Client (Auto):

- DHCPv6 client configuration

```
set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-type autoconfig
set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-ia-type ia-na
set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-identifier duid-type
    duid-ll
set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client req-option dns-server
```

- Router advertisement configuration

```
set protocols router-advertisement interface fe-0/0/0.0
```

- Enable IPv6

```
set security forwarding-options family inet6 mode flow-based
```

- Security zone configuration

```
set security zones security-zone trust interface fe-0/0/0.0 host-inbound-traffic
    system-services dhcpv6
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. To configure DHCPv6 server on SRX550M device:

   a. Set the interface.

   ```
   [edit]
   user@host# set interfaces ge-0/0/2 unit 0 family inet6
   ```

   b. Configure a DHCP local server.

   ```
   [edit ]
   user@host# set system services dhcp-local-server dhcpv6
   ```

   c. Set a default limit for all DHCPv6 groups.

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# set overrides interface-client-limit 100
   ```

   d. Set a custom client limit for the group.

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# set group my-group overrides interface-client-limit 200
   ```

   e. Specify delegated pool name.

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# set group my-group overrides delegated-pool v6-pd-pool
   ```

   f. Create a group called my-group that contains pp0 interface.

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# set group my-group interface pp0.0
   ```

2. Configuring PPPoE:

   a. Set interface to encapsulate PPPoE.

   ```
   [edit]
   user@host# set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
   ```

   b. Set chap access profile value.

   ```
   [edit system interface]
   user@host# set interface pp0 unit 0 ppp-options chap access-profile prof-ge001
   ```

   c. Set underlying interface name.

   ```
   [edit system interface]
   user@host# set interface pp0 unit 0 pppoe-options underlying-interface
     ge-0/0/1.0
   ```

   d. Set PPPoE-options server.

```
[edit system interface]
user@host# set interface pp0 unit 0 pppoe-options server
```

e. Set family name and address.

```
[edit system interface]
user@host# set interface pp0 unit 0 family inet6 address 3000::1/64
```

3. Configuring Router advertisement:

a. Set max advertisement interval limit.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0
  max-advertisement-interval 20
```

b. Set minimum advertisement interval limit.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0
  min-advertisement-interval 10
```

c. Set the configuration state to managed configuration.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0
  managed-configuration
```

d. Set the configuration state to other stateful configuration.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0
  other-stateful-configuration
```

e. Set the prefix value.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 prefix 3000::1/64
```

4. Enable IPv6:

a. Set the family name and mode to enable IPv6.

```
[edit]
user@host# set security forwarding-options family inet6 mode flow-based
```

5. Configuring PPPoE profile:

a. Set access profile name, client name and chap secret.

```
[edit]
user@host# set access profile prof-ge001 client test_user chap-secret test
```

6. Configuring PD address pool:

a. Set address-assignment pool name, family name and prefix.

```
[edit]
user@host# set access address-assignment pool v6-pd-pool family inet6 prefix
  2001:1:1::/48
```

b. Set range and prefix length.

```
[edit]
user@host# set access address-assignment pool v6-pd-pool family inet6 range
  vp-pd prefix-length 48
```

c. Set dhcp attributes with dns server value.

```
[edit]
user@host# set access address-assignment pool v6-pd-pool family inet6
  dhcp-attributes dns-server 3000::1
```

7. Configuring Security zone:

a. Set the zone name, interface and host-inbound-traffic system-services.

```
[edit]
user@host# set security zones security-zone trust interface pp0.0
  host-inbound-traffic system-services dhcpv6
```

Step-by-Step Procedure

1. To configure DHCPv6 client (PD) on SRX550M device:

a. Set the interface.

```
[edit]
user@host# set interfaces ge-0/0/2 unit 0 family inet6
```

b. Set DHCPv6 local server to override the interface client limit.

```
[edit]
user@host# set system services dhcp-local-server dhcpv6 overrides
  interface-client-limit 10
```

c. Set the process-inform pool name.

```
[edit]
user@host# set system services dhcp-local-server dhcpv6 overrides
  process-inform pool p1
```

d. Set group name and interface.

```
[edit]
user@host# set system services dhcp-local-server dhcpv6 group ipv6 interface
  ge-0/0/2.0
```

2. Configuring PPPoE:

a. Set the interface to encapsulate ppp over ethernet.

```
[edit system interface]
user@host# set interface ge-0/0/1 unit 0 encapsulation ppp-over-ether
```

b. Set default chap secret.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 ppp-options chap default-chap-secret
  test
```

c. Set chap local name.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 ppp-options chap local-name test_user
```

d. Set PPP options chap state.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 ppp-options chap passive
```

e. Set underlying-interface.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 pppoe-options underlying-interface
  ge-0/0/1.0
```

f. Set pppoe-options.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 pppoe-options client
```

3. Configuring DHCPv6 client:

a. Set the family name and dhcpv6 client type.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client client-type
  statefull
```

b. Set the dhcpv6 client identity association type.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client client-ia-type
  ia-pd
```

c. Set update-router-advertisement interface and other stateful-configuration.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client
  update-router-advertisement interface ge-0/0/2.0 other-stateful-configuration
```

d. Set maximum advertisement interval value.

```
[edit]
```

```
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client
  update-router-advertisement interface ge-0/0/2.0 max-advertisement-interval
  10
```

e. Set minimum advertisement interval value.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client
  update-router-advertisement interface ge-0/0/2.0 min-advertisement-interval
  5
```

f. Set client-identifier duid type.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client client-identifier
  duid-type duid-11
```

g. Set requested option for DHCPv6 client.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client req-option
  dns-server
```

h. Update the server.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client update-server
```

i. Set the protocols and the interface.

```
[edit]
user@host# set protocols router-advertisement interface pp0.0
```

4. Enable IPv6

a. Set the family name and mode to enable IPv6.

```
[edit]
user@host# set security forwarding-options family inet6 mode flow-based
```

5. Configuring DHCPv6 server to propagate DNS server information to end device:

a. Set address assignment pool name, family name and prefix.

```
[edit]
user@host# set access address-assignment pool p1 family inet6 prefix 2001::/16
```

b. Set the interface name for propagating TCP/IP settings to pool.

```
[edit]
user@host# set access address-assignment pool p1 family inet6 dhcp-attributes
  propagate-settings pp0.0
```

6. Configuring security zone:

a. Set the zone name, untrust interface and system services.

```
[edit]
user@host# set security zones security-zone trust interface pp0.0
  host-inbound-traffic system-services dhcpv6
```

b. Set the trust interface.

```
[edit]
user@host# set security zones security-zone trust interface ge-0/0/2.0
  host-inbound-traffic system-services dhcpv6
```

Step-by-Step Procedure

1. To configure DHCPv6 client (Auto) on SRX550M device:

   a. Set the interface, unit value, family name and DHCPv6 client type.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client client-type
     autoconfig
   ```

   b. Set Dhcpv6 client identity association type.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client
     client-ia-type ia-na
   ```

   c. Set client-identifier type.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client
     client-identifier duid-type duid-11
   ```

   d. Set DHCPV6 client requested option.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client req-option
     dns-server
   ```

2. Configuring router advertisement:

   a. Set the protocol and interface.

   ```
   [edit]
   user@host# set protocols router-advertisement interface fe-0/0/0.0
   ```

3. Enable IPv6.

   a. Set family name and mode.

   ```
   [edit]
   user@host# set security forwarding-options family inet6 mode flow-based
   ```

4. Configuring security zone:

5. Set the zone name, trust interface and system services.

```
[edit]
user@host# set security zones security-zone trust interface pp0.0
   host-inbound-traffic system-services dhcpv6
```

Results

- Result for DHCPv6 Server:

From configuration mode, confirm your configuration by entering the **show system services dhcp-local-server**, **show interfaces**, **show protocols**, **show security forwarding-options**, **show access profile prof-ge001**, **show access address-assignment pool**, and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system services dhcp-local-server
dhcpv6 {
   overrides {
      interface-client-limit 100;
   }
   group my-group {
      overrides {
         interface-client-limit 200;
         delegated-pool v6-pd-pool;
      }
      interface pp0.0set;
      interface pp0.0;
   }
   }
...
[edit]
user@host# show interfaces
ge-0/0/1 {
   unit 0 {
      encapsulation ppp-over-ether;
   }
}
pt-1/0/0 {
   vdsl-options {
      vdsl-profile auto;
   }
}
pp0 {
   unit 0 {
      ppp-options {
         chap {
            default-chap-secret "$ABC123"; ## SECRET-DATA
         }
      }
   }
```

```
}
ge-0/0/1 {
   unit 0 {
      encapsulation ppp-over-ether;
   }
}
pt-1/0/0 {
   vdsl-options {
      vdsl-profile auto;
   }
}
pp0 {
   unit 0 {
      ppp-options {
         chap {
            default-chap-secret "$ABC123"; ## SECRET-DATA
         }
      }
   }
}
...
[edit]
user@host# show protocols
interface pp0.0 {
   max-advertisement-interval 20;
   min-advertisement-interval 10;
   managed-configuration;
   other-stateful-configuration;
   prefix 3000::1/64;
}
...
[edit]
user@host# show security forwarding-options
family {
   inet6 {
      mode flow-based;
   }
}
...
[edit]
user@host#  show access address-assignment
pool v6-pd-pool {
   family inet6 {
      prefix 2001:1:1::/48;
      range vp-pd prefix-length 48;
      dhcp-attributes {
         dns-server {
            3000::1;
         }
      }
   }
}
...
[edit]
user@host# show security zones
```

```
security-zone Host {
   host-inbound-traffic {
      system-services {
         all;
      }
   }
   interfaces {
      ge-0/0/0.0;
   }
}
security-zone trust {
   interfaces {
      pp0.0 {
         host-inbound-traffic {
            system-services {
               dhcpv6;
            }
         }
      }
   }
}
```

- Result for DHCPv6 Client (PD):

```
[edit]
user@host# show system services dhcp-local-server
dhcpv6 {
   overrides {
      interface-client-limit 10;
      process-inform {
         pool p1;
      }
   }
   group my-group {
      overrides {
         interface-client-limit 200;
         delegated-pool v6-pd-pool;
      }
      interface pp0.0;
   }
   group ipv6 {
      interface ge-0/0/2.0;
   }
}
...
[edit]
user@host# show interfaces
ge-0/0/1 {
   unit 0 {
      encapsulation ppp-over-ether;
   }
}
pt-1/0/0 {
   vdsl-options {
```

```
      vdsl-profile auto;
    }
  }
  pp0 {
    unit 0 {
      ppp-options {
        chap {
          default-chap-secret "$ABC123"; ## SECRET-DATA
          local-name test_user;
          passive;
        }
      }
      pppoe-options {
        underlying-interface ge-0/0/1.0;
        client;
      }
    }
  }
  ...
  [edit]
  user@host# show interfaces pp0
  unit 0 {
    ppp-options {
      chap {
        default-chap-secret "$ABC123"; ## SECRET-DATA
        local-name test_user;
        passive;
      }
    }
    pppoe-options {
      underlying-interface ge-0/0/1.0;
      client;
    }
    family inet6 {
      dhcpv6-client {
        client-type statefull;
        client-ia-type ia-pd;
        update-router-advertisement {
          interface ge-0/0/2.0 {
            other-stateful-configuration;
            max-advertisement-interval 10;
            min-advertisement-interval 5;
          }
        }
        client-identifier duid-type duid-ll;
        req-option dns-server;
      }
    }
  }
  ...
  [edit]
  user@host# show security forwarding-options
    family {
      inet6 {
        mode flow-based;
```

```
      }
    }
...
[edit]
user@host# show access address-assignment
pool v6-pd-pool {
  family inet6 {
    prefix 2001:1:1::/48;
    range vp-pd prefix-length 48;
    dhcp-attributes {
      dns-server {
        3000::1;
      }
    }
  }
}
pool p1 {
  family inet6 {
    prefix 2001::/16;
    dhcp-attributes {
      propagate-settings pp0.0;
    }
  }
}
...
[edit]
user@host# show access address-assignment
security-zone Host {
  host-inbound-traffic {
    system-services {
      all;
    }
  }
  interfaces {
    ge-0/0/0.0;
  }
}
security-zone trust {
  interfaces {
    pp0.0 {
      host-inbound-traffic {
        system-services {
          dhcpv6;
        }
      }
    }
    ge-0/0/2.0 {
      host-inbound-traffic {
        system-services {
          dhcpv6;
        }
      }
    }
  }
}
```

```
security-zone untrust {
   interfaces {
      pp0.0 {
         host-inbound-traffic {
            system-services {
               dhcpv6;
            }
         }
      }
   }
}
```

- Result for DHCPv6 Client (Auto):

```
[edit]
user@host# show interfaces ge-0/0/0
unit 0 {
   family inet6 {
      dhcpv6-client {
         client-type autoconfig;
         client-ia-type ia-na;
         req-option dns-server;
      }
   }
}
...
[edit]
user@host# show protocols
router-advertisement {
   interface pp0.0 {
      max-advertisement-interval 20;
      min-advertisement-interval 10;
      managed-configuration;
      other-stateful-configuration;
      prefix 3000::1/64;
   }
   interface fe-0/0/0.0;
}
...
[edit]
user@host#  show security forwarding-options
   family {
      inet6 {
         mode flow-based;
      }
   }
...
[edit]
user@host# show security zones
security-zone Host {
   host-inbound-traffic {
      system-services {
         all;
      }
```

```
    }
    interfaces {
      ge-0/0/0.0;
    }
  }
  security-zone trust {
    interfaces {
      pp0.0 {
        host-inbound-traffic {
          system-services {
            dhcpv6;
          }
        }
      }
      ge-0/0/2.0 {
        host-inbound-traffic {
          system-services {
            dhcpv6;
          }
        }
      }
      fe-0/0/0.0 {
        host-inbound-traffic {
          system-services {
            dhcpv6;
          }
        }
      }
    }
  }
  security-zone untrust {
    interfaces {
      pp0.0 {
        host-inbound-traffic {
          system-services {
            dhcpv6;
          }
        }
      }
    }
  }
```

Verification

Confirm that the configuration is working properly.

Verifying DHCPv6 Server Configuration

Purpose Verify that the DHCPv6 Server has been configured.

Action

- From operational mode, enter the **show dhcpv6 server binding** command.

  The following output shows the options for the **show dhcpv6 server binding** command.

```
[edit]
user@host>show dhcpv6 server binding detail
  Session Id:  75
       Client IPv6 Prefix:                    2001:1:1::/48
       Client DUID:                           LL0x1-3c:94:d5:98:90:01
       State:
  BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)
       Lease Expires:                         2016-03-26 10:12:37 JST
       Lease Expires in:                      86213 seconds
       Lease Start:                           2016-03-25 10:12:37 JST
       Last Packet Received:                  2016-03-25 10:12:50 JST
       Incoming Client Interface:             pp0.0
       Server Ip Address:                     0.0.0.0
       Client Prefix Pool Name:               v6-pd-pool
       Client Id Length:                      10
       Client Id:                             /0x00030001/0x3c94d598/0x9001
```

- From operational mode, enter the **show route table inet6.0** command.

  The following output shows the options for the **show route table inet6.0** command.

```
[edit]
user@host>show route table inet6.0
  inet6.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
  + = Active Route, - = Last Active, * = Both

  2001:1:1::/48      *[Access/13] 00:03:45     <<<<<< Route for end device
  will be automatically generated
                      > to fe80::3e94:d50f:fc98:8600 via pp0.0
  3000::/64          *[Direct/0] 00:04:04
                      > via pp0.0
  3000::1/128        *[Local/0] 19:53:18
                        Local via pp0.0
  fe80::b2c6:9a0f:fc7d:6900/128
                     *[Local/0] 19:53:18
                        Local via pp0.0
```

- From operational mode, enter the **show interfaces pp0.0 terse** command.

  The following output shows the options for the **show interfaces pp0.0 terse** command.

```
[edit]
user@host>show interfaces pp0.0 terse
  Interface               Admin Link Proto    Local                 Remote
  pp0.0                   up    up   inet6    3000::1/64
                                              fe80::b2c6:9a0f:fc7d:6900/64
```

Verifying DHCPv6 Client (PD) Configuration

Purpose Verify that the DHCPv6 Client (PD) has been configured.

Action

- From operational mode, enter the **show dhcpv6 client binding detail** command.

  The following output shows the options for the **show dhcpv6 client binding detail** command.

```
[edit]
user@host>show dhcpv6 client binding detail
  Client Interface: pp0.0
       Hardware Address:             3c:94:d5:98:86:01
       State:                        BOUND(DHCPV6_CLIENT_STATE_BOUND) <<<<<
  SRX is bound to prefix via pp0.0
       ClientType:                   STATEFUL
       Lease Expires:                2016-03-26 10:12:50 JST
       Lease Expires in:             86232 seconds
       Lease Start:                  2016-03-25 10:12:50 JST
       Bind Type:                    IA_PD
       Client DUID:                  LL0x29-3c:94:d5:98:86:01
       Rapid Commit:                 Off
       Server Ip Address:            fe80::b2c6:9a0f:fc7d:6900
       Update Server                 Yes
       Client IP Prefix:             2001:1:1::/48
  DHCP options:
      Name: server-identifier, Value: VENDOR0x00000583-0x41453530
      Name: dns-recursive-server, Value: 3000::1
```

- From operational mode, enter the **show dhcpv6 server binding detail** command.

  The following output shows the options for the **show dhcpv6 server binding detail** command.

```
[edit]
user@host>show dhcpv6 server binding detail
  Session Id:  75
       Client IPv6 Prefix:                   2001:1:1::/48
       Client DUID:                          LL0x1-3c:94:d5:98:90:01
       State:
  BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)
       Lease Expires:                        2016-03-26 10:12:37 JST
       Lease Expires in:                     86213 seconds
       Lease Start:                          2016-03-25 10:12:37 JST
       Last Packet Received:                 2016-03-25 10:12:50 JST
       Incoming Client Interface:            pp0.0
       Server Ip Address:                    0.0.0.0
       Client Prefix Pool Name:              v6-pd-pool
       Client Id Length:                     10
       Client Id:                            /0x00030001/0x3c94d598/0x9001
```

- From operational mode, enter the **show route table inet6.0** command.

  The following output shows the options for the **show route table inet6.0** command.

```
[edit]
user@host>show route table inet6.0
  inet6.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
  + = Active Route, - = Last Active, * = Both

  ::/0               *[Access-internal/12] 00:03:35
                      > to fe80::b2c6:9a0f:fc7d:6900 via pp0.0
  2001:1:1:1::/64    *[Direct/0] 00:03:48
                      > via ge-0/0/2.0
  2001:1:1:1::1/128  *[Local/0] 00:03:48      <<<<<< IPv6 address allocated
  by Prefix delegation
                         Local via ge-0/0/2.0
  3000::/64          *[Access-internal/12] 00:03:35
```

```
                     > to fe80::b2c6:9a0f:fc7d:6900 via pp0.0
fe80::/64          *[Direct/0] 00:03:48
                     > via ge-0/0/2.0
fe80::3e94:d50f:fc98:8600/128
                   *[Local/0] 19:05:19
                      Local via pp0.0
fe80::3e94:d5ff:fe98:8602/128
                   *[Local/0] 00:03:48
                      Local via ge-0/0/2.0
```

- From operational mode, enter the **show interfaces pp0.0 terse** command.

  The following output shows the options for the **show interfaces pp0.0 terse** command.

```
[edit]
user@host>show interfaces pp0.0 terse
  Interface               Admin Link Proto    Local                 Remote
  pp0.0                   up    up   inet6    fe80::3e94:d50f:fc98:8600/64
```

- From operational mode, enter the **show interfaces ge-0/0/2.0 terse** command.

  The following output shows the options for the **show interfaces ge-0/0/2.0 terse** command.

```
[edit]
user@host>show interfaces ge-0/0/2.0 terse
  Interface               Admin Link Proto    Local                 Remote
  ge-0/0/2.0              up    up   inet6    2000:1:1:1::1/64
                                              fe80::3e94:d5ff:fe98:8602/64
```

- From operational mode, enter the **show ipv6 router-advertisement** command.

  The following output shows the options for the **show ipv6 router-advertisement** command.

```
[edit]
user@host>show ipv6 router-advertisement
  Interface: pp0.0
    Advertisements sent: 3, last sent 00:01:56 ago
    Solicits received: 0
    Advertisements received: 10
    Advertisement from fe80::b2c6:9a0f:fc7d:6900, heard 00:00:08 ago
      Managed: 1 [0]
      Other configuration: 1 [0]
      Reachable time: 0 ms
      Default lifetime: 60 sec [1800 sec]
      Retransmit timer: 0 ms
      Current hop limit: 64
      Prefix: 3000::/64
        Valid lifetime: 2592000 sec
        Preferred lifetime: 604800 sec
        On link: 1
        Autonomous: 1
  Interface: ge-0/0/2.0
    Advertisements sent: 24, last sent 00:00:03 ago
    Solicits received: 0
    Advertisements received: 0
```

Verifying DHCPv6 client (Auto) Configuration

Purpose Verify that the DHCPv6 client (Auto) has been configured.

Action

- From operational mode, enter the **show dhcpv6 client binding detail** command.

  The following output shows the options for the **show dhcpv6 client binding detail** command.

```
[edit]
user@host>show dhcpv6 client binding detail
  Client Interface: fe-0/0/0.0
       Hardware Address:             00:26:88:38:b5:00
       State:                        BOUND(DHCPV6_CLIENT_STATE_BOUND)
       ClientType:                   AUTO
       Lease Expires:                2016-03-26 10:15:35 JST
       Lease Expires in:             86395 seconds
       Lease Start:                  2016-03-25 10:15:35 JST
       Bind Type:                    IA_NA
       Client DUID:                  LL0x3-00:26:88:38:b5:00
       Rapid Commit:                 Off
       Server Ip Address:            fe80::3e94:d5ff:fe98:8602
       Client IP Address:            2001:1:1:1:226:88ff:fe38:b500/128
       Client IP Prefix:             2001:1:1:1::/64

  DHCP options:
      Name: server-identifier, Value: VENDOR0x00000583-0x414c3131
```

- From operational mode, enter the **show route table inet6.0** command.

  The following output shows the options for the **show route table inet6.0** command.

```
[edit]
user@host>show route table inet6.0
  inet6.0: 5 destinations, 6 routes (5 active, 0 holddown, 0 hidden)
  + = Active Route, - = Last Active, * = Both

  ::/0               *[Access-internal/12] 00:02:36
                      > to fe80::3e94:d5ff:fe98:8602 via fe-0/0/0.0
  2001:1:1:1::/64    *[Access-internal/12] 00:02:36
                      > to fe80::3e94:d5ff:fe98:8602 via fe-0/0/0.0
  2001:1:1:1:226:88ff:fe38:b500/128
                     *[Direct/0] 00:02:36
                      > via fe-0/0/0.0
                      [Local/0] 00:02:36
                        Local via fe-0/0/0.0
  fe80::/64          *[Direct/0] 1w3d 15:51:19
                      > via fe-0/0/0.0
  fe80::226:88ff:fe38:b500/128
                     *[Local/0] 1w3d 15:51:19
                        Local via fe-0/0/0.0
```

- From operational mode, enter the **show ipv6 router-advertisement** command.

  The following output shows the options for the **show ipv6 router-advertisement** command.

```
[edit]
user@host>show ipv6 router-advertisement
  Interface: fe-0/0/0.0
    Advertisements sent: 1, last sent 00:02:45 ago
    Solicits received: 0
    Advertisements received: 8
    Advertisement from fe80::3e94:d5ff:fe98:8602, heard 00:00:02 ago
      Managed: 0
      Other configuration: 1 [0]
      Reachable time: 0 ms
      Default lifetime: 30 sec [1800 sec]
      Retransmit timer: 0 ms
      Current hop limit: 64
      Prefix: 2001:1:1:1::/64
        Valid lifetime: 86400 sec
        Preferred lifetime: 86400 sec
        On link: 1
        Autonomous: 1
```

Release History Table

Release	Description
15.1X49-D70	Starting with Junos OS Release 15.X49-D70 and Junos OS Release 17.3R1, you can add the option **dynamic-server** to dynamically support prefix and attributes that are updated by the WAN server.

Related Documentation

- DHCPv6 Client on page 786
- Understanding DHCPv6 Client and Server Identification on page 793
- DHCPv6 Address-Assignment Pools on page 794

DHCPv6 Client

SRX Series device can act as a DHCPv6 client, receiving its TCP/IP settings and the IPv6 address for any physical interface in any security zone from an external DHCPv6 server. To enable a device to operate as a DHCPv6 client, you must configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 local server in the network. For more information, read this topic.

- DHCPv6 Client Overview on page 787
- Minimum DHCPv6 Client Configuration on page 787
- Configuring DHCP Client-Specific Attributes on page 789
- Configuring Optional DHCPv6 Client Attributes on page 790
- Configuring the DHCPv6 Client Rapid Commit Option on page 791
- Configuring a DHCPv6 Client in Autoconfig Mode on page 792
- Configuring TCP/IP Propagation on a DHCPv6 Client on page 793

DHCPv6 Client Overview

A Juniper Networks device can act as a Dynamic Host Configuration Protocol version 6 (DHCPv6) client, receiving its TCP/IP settings and the IPv6 address for any physical interface in any security zone from an external DHCPv6 server. When the device operates as a DHCPv6 client and a DHCPv6 server simultaneously, it can transfer the TCP/IP settings learned through its DHCPv6 client module to its default DHCPv6 server module. For the device to operate as a DHCPv6 client, you configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 server in the network.

DHCPv6 client support for Juniper Networks devices includes the following features:

- Identity association for nontemporary addresses (IA_NA)
- Identity association for prefix delegation (IA_PD)
- Rapid commit
- TCP/IP propagation
- Auto-prefix delegation
- Autoconfig mode (stateful and stateless)

To configure the DHCPv6 client on the device, include the **dhcpv6-client** statement at the [**edit interfaces**] hierarchy level.

NOTE: To configure a DHCPv6 client in a routing instance, add the interface in a routing instance using the [edit routing-instances] hierarchy.

NOTE: On all SRX Series devices, DHCPv6 client authentication is not supported.

NOTE: On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, DHCPv6 client does not support:

- Temporary addresses
- Reconfigure messages
- Multiple identity association for nontemporary addresses (IA_NA)
- Multiple prefixes in a single identity association for prefix delegation (IA_PD)
- Multiple prefixes in a single router advertisement

Minimum DHCPv6 Client Configuration

This topic describes the minimum configuration you must use to configure an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DHCPv6 client.

To configure the device as a DHCPv6 client:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the DHCPv6 client type. The client type can be autoconfig or statefull.

   - To enable DHCPv6 auto configuration mode, configure the client type as **autoconfig**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type autoconfig
```

   - For stateful address assignment, configure the client type as **statefull**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

3. Specify the identity association type.

   - To configure identity association for nontemporary address (IA_NA) assignment, specify the **client-ia type** as **ia-na**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

   - To configure identity association for prefix delegation (IA_PD), specify the **client-ia-type** as **ia-pd**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

4. Configure the DHCPv6 client identifier by specifying the DHCP unique identifier (DUID) type. The following DUID types are supported:

   - Link Layer address (duid-ll)
   - Link Layer address plus time (duid-llt)
   - Vendor-assigned unique ID based on enterprise number (vendor)

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-identifier duid-type duid-ll
```

NOTE: To configure a DHCPv6 client in a routing instance, add the interface to a routing instance using the **[edit routing-instances]** hierarchy.

Configuring DHCP Client-Specific Attributes

You use the address-assignment pool feature to include application-specific attributes when clients obtain an address. A client application, such as DHCPv6, uses the attributes to determine how addresses are assigned and to provide optional application-specific characteristics to the client. For example, the DHCPv6 application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCPv6 specifies additional DHCPv6 attributes such as the DNS server or the maximum lease time for clients.

NOTE: For SRX1500, SRX5400, SRX5600, and SRX5800 devices only.

You use the **dhcp-attributes** statement to configure DHCPv6 client-specific attributes for address-assignment pools at the **[edit access address-assignment pool *pool-name* family inet6] hierarchy**.

Table 57 on page 789 describes the DHCPv6 client attributes for configuring IPv6 address-assignment pools.

Table 57: DHCPv6 Attributes

Attribute	Description	DHCPv6 Option
dns-server	IPv6 address of DNS server to which clients can send DNS queries	23
grace-period	Grace period offered with the lease	–
maximum-lease-time	Maximum lease time allowed by the DHCPv6 server	–
option	User-defined options	–
sip-server-address	IPv6 address of SIP outbound proxy server	22
sip-server-domain-name	Domain name of the SIP outbound proxy server	21

See Also

- Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment on page 797

Configuring Optional DHCPv6 Client Attributes

To enable a device to operate as a DHCPv6 client, you configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 local server in the network. You can then specify the retransmission attempts, client requested configuration options, interface used to delegate prefixes, rapid commit, and update server options.

To configure optional DHCPv6 client attributes:

1. Specify one of the following DHCPv6 client requested configuration options:
   - dns-server
   - domain
   - ntp-server
   - sip-domain
   - sip-server

   For example, to specify the DHCPv6 client requested option as **dns-server**:

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set req-option dns-server
   ```

2. Set the number of attempts allowed to retransmit a DHCPv6 client protocol packet.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set retransmission-attempt 6
   ```

3. Configure the **update-server** option on the DHCPv6 client.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set update-server
   ```

4. Specify the interface used to delegate prefixes.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set update-router-advertisement interface ge-0/0/0
   ```

5. Configure the two-message (rapid commit) exchange option for address assignment.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set rapid-commit
   ```

NOTE: To configure a DHCPv6 client in a routing instance, add the interface to a routing instance using the **[edit routing-instances]** hierarchy.

NOTE: On all SRX Series devices, DHCPv6 client authentication is not supported.

NOTE: On SRX300, SRX320, SRX340, and SRX345, and SRX550M devices, DHCPv6 client does not support:

- Temporary addresses
- Reconfigure messages
- Multiple identity association for nontemporary addresses (IA_NA)
- Multiple prefixes in a single identity association for prefix delegation (IA_PD)
- Multiple prefixes in a single router advertisement

Configuring the DHCPv6 Client Rapid Commit Option

The DHCPv6 client can obtain configuration parameters from a DHCPv6 server through a rapid two-message exchange (solicit and reply). When the rapid commit option is enabled by both the DHCPv6 client and the DHCPv6 server, the two-message exchange is used, rather than the default four-method exchange (solicit, advertise, request, and reply). The two-message exchange provides faster client configuration and is beneficial in environments in which networks are under a heavy load.

To configure the DHCPv6 client to support the DHCPv6 rapid commit option on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the two-message exchange option for address assignment.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set rapid-commit
```

Configuring a DHCPv6 Client in Autoconfig Mode

A DHCPv6 client configured in autoconfig mode acts as a stateful client, a stateless client (DHCPv6 server is required for TCP/IP configuration), and stateless–no DHCP client, based on the managed (M) and other configuration (O) bits in the received router advertisement messages.

If the managed bit is 1 and the other configuration bit is 0, the DHCPv6 client acts as a stateful client. In stateful mode, the client receives IPv6 addresses from the DHCPv6 server, based on the identity association for nontemporary addresses (IA_NA) assignment.

If the managed bit is 0 and the other configuration bit is 1, the DHCPv6 client acts as a stateless client. In stateless mode, the addresses are automatically configured, based on the prefixes in the router advertisement messages received from the router. The stateless client receives configuration parameters from the DHCPv6 server.

If the managed bit is 0 and the other configuration bit is also 0, the DHCPv6 client acts as a stateless–no DHCP client. In the stateless–no DHCP mode, the client receives IPv6 addresses from the router advertisement messages.

To configure DHCPv6 client in autoconfig mode on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Configure the DHCPv6 client type as **autoconfig**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type autoconfig
```

2. Specify the identity association type as **ia-na** for nontemporary addresses.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

3. Specify the interface on which to configure router advertisement.

```
[edit protocols router-advertisement]
user@host# set interface ge-0/0/0
```

Configuring TCP/IP Propagation on a DHCPv6 Client

You can enable or disable the propagation of TCP/IP settings received on the device acting as a DHCPv6 client. The settings can be propagated to the server pool running on the device. This topic describes how to configure TCP/IP settings on a DHCPv6 client, where both the DHCPv6 client and DHCPv6 server are on the same device.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

To configure TCP/IP setting propagation on a DHCPv6 client:

1. Configure the **update-server** option on the DHCPv6 client.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-server
```

2. Configure the address pool to specify the interface (where **update-server** is configured) from which TCP/IP settings can be propagated.

```
[edit access]
user@host# set address-assignment pool 2 family inet6 dhcp-attributes
   propagate-settings ge-0/0/0
```

Related Documentation

- DHCP Client on page 733
- DHCPv6 Client on page 786
- Understanding DHCPv6 Client and Server Identification on page 793

Understanding DHCPv6 Client and Server Identification

Each DHCPv6 client and server is identified by a DHCP unique identifier (DUID). The DUID is unique across all DHCPv6 clients and servers, and it is stable for any specific client or server. DHCPv6 clients use DUIDs to identify a server in messages where a server needs to be identified. DHCPv6 servers use DUIDs to determine the configuration parameters to be used for clients and in the association of addresses with clients.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

The DUID is a 2-octet type code represented in network byte order, followed by a variable number of octets that make up the actual identifier; for example, 00:02:00:01:02:03:04:05:07:a0. A DUID can be up to 128 octets in length (excluding the type code). The following types are currently defined for the DUID parameter:

- Type 1—Link Layer address plus time (duid-llt)
- Type 2—Vendor-assigned unique ID based on enterprise number (vendor)
- Type 3—Link Llayer address (duid-ll)

The duid-llt DUID consists of a 2-octet type field that contains the value 1, a 2-octet hardware type code, 4 octets that signify a time value, followed by the Link Layer address of any one network interface that is connected to the DHCP device at the time that the DUID is generated.

The vendor DUID is assigned by the vendor to the device and contains the vendor's registered private enterprise number as maintained by the identity association for nontemporary addresses (IA_NA) assignment, followed by a unique identifier assigned by the vendor.

The duid-ll DUID contains a 2-octet type field that stores the value 3, and a 2-octet network hardware type code, followed by the Link Layer address of any one network interface that is permanently connected to the client or server device.

Related Documentation

- DHCPv6 Client Overview on page 787

DHCPv6 Address-Assignment Pools

Address pool is a set of Internet Protocol addresses available for allocation to users, such as in host configurations with the DHCP. An address-assignment pool can support either IPv4 address or IPv6 addresses. You cannot use the same pool for both types of address. For more information, read this topic.

- Example: Configuring an Address-Assignment Pool for IPv6 Addresses on page 794
- Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment on page 797
- Configuring an Address-Assignment Pool for Router Advertisement on page 798
- Configuring Nontemporary Address Assignment on page 798
- Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation on page 799
- Configuring Auto-Prefix Delegation on page 800

Example: Configuring an Address-Assignment Pool for IPv6 Addresses

This example shows how to configure an address-assignment pool on SRX1500, SRX5400, SRX5600, and SRX5800 devices.

- Requirements on page 795
- Overview on page 795
- Configuration on page 795
- Verification on page 796

Requirements

Before you begin:

- Specify the name of the address-assignment pool and configure addresses for the pool.
- Set DHCPv6 attributes for the address-assignment pool.

Overview

In this example, you configure an address-pool called my-pool and specify the IPv6 family as inet6. You configure the IPv6 prefix as 2001:db8:3000:1::/64, the range name as range1, and the IPv6 range for DHCPv6 clients from a low of 2001:db8:3000:1::/64 to a high of 2001:db8:3000:200::/64. You can define the range based on the lower and upper boundaries of the prefixes in the range or based on the length of the prefixes in the range. Finally, you specify the DHCPv6 attribute for the DNS server as 2001:db8:3001::1, the grace period as 3600, and the maximum lease time as 120.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set access address-assignment pool my-pool family inet6 prefix 2001:db8:3000:1::/64
set access address-assignment pool my-pool family inet6 range range1 low
  2001:db8:3000:1::/64 high 2001:db8:3000:200::/64
set access address-assignment pool my-pool family inet6 dhcp-attributes dns-server
  2001:db8:3001::1
set access address-assignment pool my-pool family inet6 dhcp-attributes grace-period
  3600
set access address-assignment pool my-pool family inet6 dhcp-attributes
  maximum-lease-time 120
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure an IPv6 address-assignment pool:

1. Configure an address-pool and specify the IPv6 family.

```
[edit access]
user@host# edit address-assignment pool my-pool family inet6
```

2. Configure the IPv6 prefix, the range name, and IPv6 range for DHCPv6 clients.

```
[edit access address-assignment pool my-pool family inet6]
```

```
user@host# set prefix 2001:db8:3000:1::/64
user@host# set range range1 low 2001:db8:3000:1::/64 high
  2001:db8:3000:200::/64
```

3. Configure the DHCPv6 attribute for the DNS server for the address pool.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes dns-server 2001:db8:3001::1
```

4. Configure the DHCPv6 attribute for the grace period.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes grace-period 3600
```

5. Configure the DHCPv6 attribute for the maximum lease time.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes maximum-lease-time 120
```

Results From configuration mode, confirm your configuration by entering the **show access address-assignment** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
  user@host# show access address-assignment
  pool my-pool {
  family inet6 {
  prefix 2001:db8:3000:1::/64;
    range range1 {
    low 2001:db8:3000:1::/64 ;
  high 2001:db8:3000:200::/64;
  }
  dhcp-attributes {
    maximum-lease-time 120;
    grace-period 3600;
    dns-server {
      2001:db8:3001::1;
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Configuration

Purpose Verify that the address-assignment pool has been configured.

Action From operational mode, enter the **show access address-assignment** command.

See Also
- DHCPv6 Server Overview on page 758
- Example: Configuring DHCPv6 Server Options on page 760
- Creating a Security Policy to Enable DHCPv6 Traffic on page 759

Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment

You can optionally configure multiple named ranges, or subsets of addresses, within an address-assignment pool. During dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, you specify a name for the range and define the address range and DHCPv6 attributes.

NOTE: Supported only on SRX1500, SRX5400, SRX5600, and SRX5800 devices.

To configure a named address range for dynamic address assignment:

1. Specify the name of the address-assignment pool and the IPv6 family.

```
[edit access]
user@host# edit address-assignment pool my-pool2 family inet6
```

2. Configure the IPv6 prefix and then define the range name and IPv6 range for DHCPv6 clients. You can define the range based on the lower and upper boundaries of the prefixes in the range, or based on the length of the prefixes in the range.

```
[edit access address-assignment pool my-pool2 family inet6]
user@host# set prefix 2001:db8:3000:5::/64
user@host# set range range2 low 2001:db8:3000:2::/64 high 2001:db8:3000:300::/64
```

3. Configure DHCPv6 attributes for the address pool.

```
[edit access address-assignment pool my-pool2 family inet6]
user@host# set dhcp-attributes dns-server 2001:db8:18:: grace-period 3600
  maximum-lease-time 120
```

4. If you are done configuring the device, enter **commit** from configuration mode.

See Also • Configuring Address-Assignment Pool Linking on page 732

Configuring an Address-Assignment Pool for Router Advertisement

For SRX1500, SRX5400, SRX5600, and SRX5800 devices, you can create an address-assignment pool that is explicitly used for router advertisement address assignment. You populate the address-assignment pool using the standard procedure, but you additionally specify that the pool is used for router advertisement.

To configure an address-assignment pool that is used for router advertisement:

1. Create the IPv6 address-assignment pool. See "Example: Configuring an Address-Assignment Pool for IPv6 Addresses" on page 794.

2. Specify that the address-assignment pool is used for router advertisement.

```
[edit access address-assignment]
user@host# set neighbor-discovery-router-advertisement router1
```

3. If you are done configuring the device, enter **commit** from configuration mode.

Configuring Nontemporary Address Assignment

Nontemporary address assignment is also known as stateful address assignment. In the stateful address assignment mode, the DHCPv6 client requests global addresses from the DHCPv6 server. Based on the DHCPv6 server's response, the DHCPv6 client assigns the global addresses to interfaces and sets a lease time for all valid responses. When the lease time expires, the DHCPv6 client renews the lease from the DHCPv6 server.

NOTE: **This feature is supported on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.**

To configure nontemporary (stateful) address assignment:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the client type as **statefull**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

3. Specify the IA_NA assignment.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

See Also
- Minimum DHCPv6 Client Configuration on page 787

Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation

The DHCPv6 client requests IPv6 addresses and prefixes from the DHCPv6 server. Based on the DHCPv6 server's response, the DHCPv6 client assigns the IPv6 addresses to interfaces and sets a lease time for all valid responses. When the lease time expires, the DHCPv6 client renews the lease from the DHCPv6 server.

To configure identity association for nontemporary addresses (IA_NA) and identity association for prefix delegation (IA_PD) on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the client type as **statefull**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

3. Specify the IA_NA.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

4. Specify the IA_PD.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

See Also
- Minimum DHCPv6 Client Configuration on page 787

Configuring Auto-Prefix Delegation

You can use DHCPv6 client prefix delegation to automate the delegation of IPv6 prefixes to the customer premises equipment (CPE). With prefix delegation, a delegating router delegates IPv6 prefixes to a requesting router. The requesting router then uses the prefixes to assign global IPv6 addresses to the devices on the subscriber LAN. The requesting router can also assign subnet addresses to subnets on the LAN.

To configure auto-prefix delegation for SRX300, SRX320. SRX340, SRX345, SRX550M, and SRX1500 devices:

1. Configure the DHCPv6 client type as **statefull**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

2. Specify the identity association type as **ia-na** for nontemporary addresses.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

3. Specify the identity association type as **ia-pd** for prefix delegation.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

4. Configure the DHCPv6 client identifier by specifying the DUID type.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-identifier duid-type duid-ll
```

5. Specify the interface used to delegate prefixes.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-router-advertisement interface ge-0/0/0
```

See Also

- Minimum DHCPv6 Client Configuration on page 787
- Configuring Optional DHCPv6 Client Attributes on page 790

Related Documentation

- DHCP Address-Assignment Pools on page 729
- DHCPv6 Server on page 758
- DHCPv6 Client on page 786
- Understanding DHCPv6 Client and Server Identification on page 793

DHCP In Chassis Cluster Mode

Junos OS allows you to configure two SRX Series devices as DHCP clients and a third SRX Series device as a DHCP server and setup high availability between the two DHCP clients in chassis cluster mode.

Similarly, you can also configure two SRX Series devices as DHCP servers in chassis cluster mode and a third SRX Series device as a DHCP client. for more information, read this topic.

Example: Configuring the Device as a DHCP Server in Chassis Cluster Mode

This example shows how to configure a DHCP server in chassis cluster mode.

Requirements

This example uses the following hardware and software components:

- Two SRX Series devices as DHCP servers
- One SRX Series device as DHCP client
- Junos OS Release 12.1X47-D10 or later for SRX Series Services Gateways

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices.
- Determine the DHCP options required by the subnets and clients in your network.

Overview

In this example, you configure two SRX Series devices as DHCP servers and a third SRX Series device as a DHCP client. Configure the two DHCP servers in chassis cluster mode.

For the DHCP server, configure the SRX Series device as a DHCP local server with minimum DHCP local server configurations. You specify the server group as g1 and enable the DHCP local server on interface reth1.

For the DHCP client, you specify the interface as ge-0/0/1, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as 00:0a:12:00:12:12 in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds.

You set the number of retransmission attempts to 6. The range is from 0 through 6, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Finally, you set the IPv4 address of the preferred DHCP server to 10.1.1.1 and the vendor class ID to ether.

WARNING: Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices has been deprecated and only the new DHCP CLI is supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

Configure DHCP Server 1 and Server 2:

```
set system services dhcp-local-server group g1 interface reth1
set access address-assignment pool p1 family inet network 203.0.113.1/10
set access address-assignment pool p1 family inet range r1 low 203.0.113.5
set access address-assignment pool p1 family inet range r1 high 203.0.113.20
```

Configure chassis cluster on DHCP Server 1 and DHCP Server 2:

```
set chassis cluster reth-count 4
set chassis cluster control-link-recovery
set chassis cluster heartbeat-interval 2000
set chassis cluster redundancy-group 0 node 0 priority 200
set chassis cluster redundancy-group 0 node 1 priority 1
set interfaces ge-0/0/1 gigether-options redundant-parent reth1
set interfaces ge-6/0/1 gigether-options redundant-parent reth1
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 0 family inet address 10.1.1.1/24
```

Configure the DHCP client:

```
set interfaces ge-0/0/1 unit 0 family inet dhcp-client
set interfaces ge-0/0/1 unit 0 family inet dhcp-client client-identifier user-id ascii
   00:0a:12:00:12:12
set interfaces ge-0/0/1 unit 0 family inet dhcp-client lease-time 86400
set interfaces ge-0/0/1 unit 0 family inet dhcp-client retransmission-attempt 6
set interfaces ge-0/0/1 unit 0 family inet dhcp-client retransmission-interval 5
set interfaces ge-0/0/1 unit 0 family inet dhcp-client server-address 10.1.1.1
set interfaces ge-0/0/1 unit 0 family inet dhcp-client vendor-id ether
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the devices as DHCP servers:

1. Configure the DHCP local server.

```
[edit system services]
user@host# set dhcp-local-server group g1 interface reth1
```

2. Configure an address pool.

```
[edit access]
user@host# set address-assignment pool p1 family inet network 203.0.113.1/10
user@host# set address-assignment pool p1 family inet range r1 low 203.0.113.5
user@host# set address-assignment pool p1 family inet range r1 high 203.0.113.20
```

Step-by-Step Procedure

To configure the DHCP servers in chassis cluster mode:

1. Specify the number of redundant Ethernet interfaces for the chassis cluster.

```
{primary:node0}[edit]
user@host# set chassis cluster reth-count 4
```

2. Enable control link recovery.

```
{primary:node0}[edit]
user@host# set chassis cluster control-link-recovery
```

3. Configure heartbeat settings.

```
{primary:node0}[edit]
user@host# set chassis cluster heartbeat-interval 2000
```

4. Configure the redundancy groups.

```
{primary:node0}[edit]
```

```
user@host# set chassis cluster redundancy-group 0 node 0 priority 200
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
```

5. Configure redundant Ethernet interfaces.

```
{primary:node0}[edit]
user@host# set interfaces ge-0/0/1 gigether-options redundant-parent reth1
user@host# set interfaces ge-6/0/1 gigether-options redundant-parent reth1
user@host# set interfaces reth1 redundant-ether-options redundancy-group 1
user@host# set interfaces reth1 unit 0 family inet address 10.1.1.1/24
```

Step-by-Step Procedure

To configure the device as DHCP client:

1. Specify the DHCP client interface.

```
[edit]
user@host# edit interfaces ge-0/0/1 unit 0 family inet dhcp-client
```

2. Configure the DHCP client identifier as a hexadecimal value.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set client-identifier user-id ascii 00:0a:12:00:12:12
```

3. Set the DHCP lease time.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

4. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```

5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```

6. Set the IPv4 address of the preferred DHCP server.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set server-address 10.1.1.1
```

7. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```

Results From configuration mode, confirm your configuration by entering the **show** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system services
dhcp-local-server {
   group g1 {
      interface reth1.0;
   }
}
```

```
[edit]
user@host# show access address-assignment
pool p1 {
   family inet {
      network 203.0.113.1/10;
      range r1 {
         low 203.0.113.5;
         high 203.0.113.20;
      }
   }
}
```

```
[edit]
user@host# show chassis cluster
control-link-recovery;
reth-count 4;
heartbeat-interval 2000;
redundancy-group 0 {
   node 0 priority 200;
   node 1 priority 1;
}
```

```
[edit]
user@host# show interfaces reth1
redundant-ether-options {
   redundancy-group 1;
}
unit 0 {
   family inet {
      address 10.1.1.1.24;
   }
}
```

```
[edit]
user@host# show interfaces ge-0/0/1 unit 0 family inet
```

```
dhcp-client {
   client-identifier user-id ascii 00:0a:12:00:12:12;
   lease-time 86400;
   retransmission-attempt 6;
   retransmission-interval 5;
   server-address 10.1.1.1;
   vendor-id ether;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying the DHCP Server in Chassis Cluster Mode

Purpose Verify that the DHCP server is working in chassis cluster mode.

Action From operational mode, enter the **show dhcp server binding** and **show dhcp server statistics** commands.

```
user@host> show dhcp server binding
```

```
IP address     Session Id  Hardware address      Expires    State   Interface
 10.1.1.1     1         64:87:88:79:a3:81     81855      BOUND    reth1
```

```
user@host> show dhcp server statistics
```

```
Packets dropped:
    Total                     0
    dhcp-service total        0

Messages received:
    BOOTREQUEST               2
    DHCPDECLINE               0
    DHCPDISCOVER              1
    DHCPINFORM                0
    DHCPRELEASE               0
    DHCPREQUEST               1

Messages sent:
    BOOTREPLY                 2
    DHCPOFFER                 1
    DHCPACK                   0
    DHCPNAK                   0
    DHCPFORCERENEW            0
```

Meaning The sample output shows that DHCP servers configured in the example work in a chassis cluster.

See Also
- Understanding DHCP Server Operation on page 718

Example: Configuring the Device as a DHCP Client in Chassis Cluster Mode

This example shows how to configure the device as a DHCP client in chassis cluster mode.

Requirements

This example uses the following hardware and software components:

- Two SRX Series devices as DHCP client
- One SRX Series device as DHCP server
- Junos OS Release 12.1X47-D10 or later for SRX Series Services Gateways

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices.
- Determine the DHCP options required by the subnets and clients in your network.

Overview

In this example, you configure two SRX Series devices as DHCP clients and a third SRX Series device as a DHCP server. Configure the two DHCP clients in chassis cluster mode.

For DHCP clients, you specify the interface as reth1, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as 00:0a:12:00:12:12 in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the options no-hostname if you do not want the DHCP client to send the hostname with the packets. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds. You set the number of retransmission attempts to 6. The range is from 0 through 6, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Finally, you set the IPv4 address of the preferred DHCP server to 203.0.113.1 and the vendor class ID to ether.

For the DHCP server, configure the SRX Series device as a DHCP local server with minimum DHCP local server configurations. You specify the server group as g1 and enable the DHCP local server on interface ge-0/0/2.0.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

Configure DHCP Client 1 and Client 2:

```
set interfaces reth1 unit 0 family inet dhcp-client
set interfaces reth1 unit 0 family inet dhcp-client client-identifier user-id ascii
    00:0a:12:00:12:12
set interfaces reth1 unit 0 family inet dhcp-client options no-hostname
set interfaces reth1 unit 0 family inet dhcp-client lease-time 86400
set interfaces reth1 unit 0 family inet dhcp-client retransmission-attempt 6
set interfaces reth1 unit 0 family inet dhcp-client retransmission-interval 5
set interfaces reth1 unit 0 family inet dhcp-client server-address 203.0.113.1
set interfaces reth1 unit 0 family inet dhcp-client vendor-id ether
```

Configure chassis cluster on Client 1 and Client 2:

```
set chassis cluster reth-count 2
set chassis cluster control-link-recovery
set chassis cluster heartbeat-interval 1000
set chassis cluster redundancy-group 1 node 0 priority 100
set chassis cluster redundancy-group 1 node 1 priority 1
set chassis cluster redundancy-group 0 node 0 priority 100
set chassis cluster redundancy-group 0 node 1 priority 1
set interfaces ge-0/0/1 gigether-options redundant-parent reth1
set interfaces ge-4/0/1 gigether-options redundant-parent reth1
set interfaces reth1 redundant-ether-options redundancy-group 1
```

Configure the DHCP server:

```
set system service dhcp-local-server group g1 interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family inet address 203.0.113.1/24
set access address-assignment pool p1 family inet network 203.0.113.0/24
set access address-assignment pool p1 family inet range r1 low 203.0.113.5
set access address-assignment pool p1 family inet range r1 high 203.0.113.20
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the devices as DHCP clients:

1. Specify the DHCP client interface.

```
[edit]
user@host# edit interfaces reth1 unit 0 family inet dhcp-client
```

2. Configure the DHCP client identifier as a hexadecimal value.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set client-identifier user-id ascii 00:0a:12:00:12:12
```

3. Set the hostname if you do not want the DHCP client to send hostname in the packets (RFC option code 12).

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```

4. Set the DHCP lease time.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

5. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```

6. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```

7. Set the IPv4 address of the preferred DHCP server.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set server-address 203.0.113.1
```

8. Set the vendor class ID for the DHCP client.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```

Step-by-Step Procedure

To configure the DHCP clients in chassis cluster mode:

1. Specify the number of redundant Ethernet interfaces for the chassis cluster.

```
{primary:node0}[edit]
user@host# set chassis cluster reth-count 2
```

2. Enable control link recovery.

```
{primary:node0}[edit]
user@host# set chassis cluster control-link-recovery
```

3. Configure heartbeat settings.

```
{primary:node0}[edit]
user@host# set chassis cluster heartbeat-interval 1000
```

4. Configure the redundancy groups.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 node 0 priority 100
user@host# set chassis cluster redundancy-group 1 node 1 priority 1
user@host# set chassis cluster redundancy-group 0 node 0 priority 100
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
```

5. Configure redundant Ethernet interfaces.

```
{primary:node0}[edit]
user@host# set interfaces ge-0/0/1 gigether-options redundant-parent reth1
user@host# set interfaces reth1 redundant-ether-options redundancy-group 1
```

Step-by-Step Procedure

To configure the device as DHCP server:

1. Configure the DHCP local server.

```
[edit system services]
user@host# set dhcp-local-server group g1 interface ge-0/0/2.0
```

2. Configure IP address of the server.

```
[edit interfaces]
user@host# set interfaces ge-0/0/2 unit 0 family inet address 203.0.113.1/24
```

3. Configure an address pool.

```
[edit access]
user@host# set address-assignment pool p1 family inet network 203.0.113.0/24
user@host# set address-assignment pool p1 family inet range r1 low 203.0.113.5
user@host# set address-assignment pool p1 family inet range r1 high 203.0.113.20
```

Results

From configuration mode, confirm your configuration by entering the **show** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces reth1 unit 0 family inet
dhcp-client {
   client-identifier user-id ascii 00:0a:12:00:12:12;
   options no-hostname;
   lease-time 86400;
   retransmission-attempt 6;
   retransmission-interval 5;
   server-address 203.0.113.1;
   vendor-id ether;
}
```

```
[edit]
user@host# show chassis cluster
control-link-recovery;
reth-count 2;
heartbeat-interval 1000;
redundancy-group 0 {
   node 0 priority 100;
   node 1 priority 1;
}
redundancy-group 1{
   node 0 priority 100;
   node 1 priority 1;
}
```

```
[edit]
user@host# show interfaces reth1
redundant-ether-options {
   redundancy-group 1;
}
```

```
[edit]
user@host# show access address-assignment
pool p1 {
   family inet {
      network 203.0.113.0/24;
      range r1 {
         low 203.0.113.5;
         high 203.0.113.20;
      }
   }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the DHCP Client in Chassis Cluster Mode

Purpose Verify that the DHCP client is working in chassis cluster mode.

Action From operational mode, enter the **show dhcp client binding**, **show dhcp client statistics** and **show dhcp client binding interface reth1 detail** commands.

```
user@host> show dhcp client binding
```

```
IP address     Hardware address   Expires     State      Interface
 203.0.113.14      00:1f:12:e3:34:01  84587       BOUND      reth1.0
```

```
user@host> show dhcp client statistics
```

```
Packets dropped:
    Total                     4
    Send error                4

Messages received:
    BOOTREPLY                 3
    DHCPOFFER                 1
    DHCPACK                   2
    DHCPNAK                   0
    DHCPFORCERENEW            0

Messages sent:
    BOOTREQUEST               0
    DHCPDECLINE               0
    DHCPDISCOVER              5
    DHCPREQUEST               8
    DHCPINFORM                0
    DHCPRELEASE               1
    DHCPRENEW                 0
    DHCPREBIND                0
```

```
user@host> show dhcp client binding interface reth1 detail
```

```
Client Interface: reth1.0
     Hardware Address:             00:10:db:ff:10:01
     State:                        BOUND(LOCAL_CLIENT_STATE_BOUND)
     Lease Expires:                2013-12-18 10:15:36 CST
     Lease Expires in:             30 seconds
     Lease Start:                  2013-12-17 10:15:36 CST
     Server Identifier:            203.0.113.1
     Client IP Address:            10.1.1.14
     Update Server                 No

DHCP options:
    Name: dhcp-lease-time, Value: 1 day
    Name: server-identifier, Value: 10.1.1.1
    Name: subnet-mask, Value: 255.255.255.0
```

Meaning The sample output shows that DHCP clients configured in the example work in a chassis cluster.

See Also

- Understanding DHCP Client Operation on page 733
-

Release History Table

Release	Description
15.1X49-D60	Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices has been deprecated and only the new DHCP CLI is supported.

Related Documentation

- *Configuring Chassis Clustering on an SRX Series Devices*
- DHCP Overview on page 713
- DHCP Server on page 718
- DHCP Address-Assignment Pools on page 729
- DHCP Client on page 733

CHAPTER 14

Configuration Statements

access

Syntax

```
access {
  address-assignment
  pool pool-name
  address-pool pool-name
  profile profile-name {
    accounting (Access Profile) {
      accounting-stop-on-access-deny;
      accounting-stop-on-failure;
      (authentication-order (Access Profile) (ldap radius | none);
      order (radius | none);
    }
    radius {
      accounting-server [server-addresses];
      authentication-server [server-addresses];
    }
  }
}
```

Hierarchy Level

```
[edit]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Configure authentication, authorization, and accounting (AAA) services.

The remaining statements are explained separately. See CLI Explorer.

NOTE: The **[edit access]** hierarchy is not available on QFabric systems.

Default

Not enabled

Required Privilege Level

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

Related Documentation

- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335

access (Dynamic Access Routes)

Syntax

```
access {
  route prefix {
    next-hop next-hop;
    metric route-cost;
    preference route-distance;
    tag route-tag;
    tag2 route-tag2;
  }
```

Hierarchy Level

```
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance
  routing-options],
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options
  rib routing-table-name],
[edit dynamic-profiles profile-name routing-options]
```

Release Information

Statement introduced in Junos OS Release 9.5.
Support at the **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options]** and **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name*]** hierarchy levels introduced in Junos OS Release 10.1.

Description

Dynamically configure access routes in a dynamic client profile.

NOTE: Starting in Junos OS Release 15.1, we recommend that you use only access routes for framed route support. We recommend that you do not use access-internal routes. If you configure the access-internal statement in the dynamic profile, it is ignored. The subscriber's address is stored in the session database entry before the dynamic profile installs the framed route, enabling the next-hop address to be resolved when it is not explicitly specified in the Framed-Route RADIUS attribute [22] or Framed-IPv6-Route attribute [99].

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Release History Table

Release	Description
15.1	Starting in Junos OS Release 15.1, we recommend that you use only access routes for framed route support.

Related Documentation
- *Configuring Dynamic Access Routes for Subscriber Management*

access-end

Syntax
```
access-end HH:MM;
```

Hierarchy Level
```
[edit system login class]
```

Release Information Statement introduced in Junos OS Release 10.1.

Description Configure the end time for login access.

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

Related Documentation
- *Configuring Time-Based User Access*

access-internal (Dynamic Access-Internal Routes)

Syntax

```
access-internal {
  route subscriber-ip-address {
    qualified-next-hop underlying-interface {
      mac-address address;
    }
  }
```

Hierarchy Level

```
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance
  routing-options],
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options
  rib routing-table-name],
[edit dynamic-profiles routing-options]
```

Release Information

Statement introduced in Junos OS Release 9.5.
Support at the **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options]** and **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name*]** hierarchy levels introduced in Junos OS Release 10.1.

Description

(Releases earlier than Junos OS Release 15.1) Dynamically configure access-internal routes in a dynamic client profile. Access-internal routes are optional, but are used instead of access routes if the next-hop address is not specified in the Framed-Route Attribute [22] for IPv4 or the Framed-IPv6-Route attribute [99] for IPv6.

NOTE: Starting in Junos OS Release 15.1, we recommend that you use only access routes for framed route support. We recommend that you do not use access-internal routes. If you configure the access-internal statement in the dynamic profile, it is ignored. The subscriber's address is stored in the session database entry before the dynamic profile installs the framed route, enabling the next-hop address to be resolved when it is not explicitly specified in the Framed-Route RADIUS attribute (22) or Framed-IPv6-Route attribute [99].

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Release History Table

Release	Description
15.1	Starting in Junos OS Release 15.1, we recommend that you use only access routes for framed route support.

Related Documentation
- *Configuring Dynamic Access-Internal Routes for DHCP and PPP Subscribers*

access-start

Syntax
```
access-start HH:MM;
```

Hierarchy Level
```
[edit system login class]
```

Release Information Statement introduced in Junos OS Release 10.1.

Description Configure the start time for login access.

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

Related Documentation
- *Configuring Time-Based User Access*

active-server-group

Syntax

active-server-group *server-group-name* <allow-server-change>;

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name*],
[edit forwarding-options dhcp-relay group *group-name*],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 group *group-name*],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name*],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay]
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name*],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name*]

Release Information

Statement introduced in Junos OS Release 8.3.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
allow-server-change option added in Junos OS Release 16.2R1.

Description

Apply a DHCP relay agent configuration to the named group of DHCP server addresses. The server group itself is configured with the server-group statement. You can apply an active server group globally or for specific groups of interfaces, configured with the group statement. An active server group applied to an interface group overrides a global configuration.

Options

allow-server-change—(Optional) (DHCPv4 only) Enable the relay agent to accept and forward a DHCP request (renew or rebind) ACK message to the client from any DHCP local server in the active server group. Starting in Junos OS Release 18.4R1, this option also applies to DHCP information request (DHCPINFORM) ACK messages.

Default: Forward ACK messages from only the original binding server.

server-group-name—Name of the group of DHCP or DHCPv6 server addresses to which the DHCP or DHCPv6 relay agent configuration applies.

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618
- Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups on page 667
- Configuring Group-Specific DHCP Relay Options on page 672

accounting

Syntax

```
accounting {
  events [login change-log interactive-commands];
  destination {
    radius {
      server {
        server-address {
          accounting-port port-number;
          retry number;
          routing-instance routing-instance;
          secret password;
          source-address address;
          timeout seconds;
        }
      }
    }
    tacplus {
      server {
        server-address {
          port port-number;
          routing-instance routing-instance;
          secret password;
          single-connection;
          timeout seconds;
        }
      }
    }
  }
  enhanced-avs-max <number>;
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
enhanced-avs-max statement introduced in Junos OS Release 14.1.
Support for the **source-address-inet6** statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description

Configure audit of TACACS+ or RADIUS authentication events, configuration changes, and interactive commands. Auditing these factors helps you track network usage for auditing and billing purposes.

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 System Accounting on page 200
- Configuring TACACS+ System Accounting on page 219
- enhanced-avs-max on page 1077

accounting (Access Profile)

Syntax

```
accounting {
  accounting-stop-on-access-deny;
  accounting-stop-on-failure;
  order (radius | none);
}
```

Hierarchy Level

[edit access profile *profile-name*]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Configure the authentication order for authentication, authorization, and accounting (AAA) services.

Default

Not enabled

Options

none—Use no authentication for specified subscribers.

radius—Use RADIUS authentication for specified subscribers.

The remaining statements are explained separately. See CLI Explorer.

NOTE: **The [edit access] hierarchy is not available on QFabric systems.**

Required Privilege Level

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

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335
- Understanding 802.1X and RADIUS Accounting on Switches on page 332
- Understanding RADIUS Accounting on page 199

accounting (Access Profile)

Syntax

```
accounting {
  accounting-stop-on-access-deny;
  accounting-stop-on-failure;
  address-change-immediate-update;
  ancp-speed-change-immediate-update;
  coa-immediate-update;
  coa-no-override service-class-attribute;
  duplication;
  duplication-filter;
  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. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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-options

Syntax

```
accounting-options {
  class-usage-profile profile-name {
    destination-classes {
      destination-class-name;
    }
    file filename;
    interval minutes;
    source-classes {
      source-class-name;
    }
  }
  file filename {
    archive-sites {
      site-name;
    }
    files number;
    nonpersistent;
    size bytes;
    start-time time;
    transfer-interval minutes;
  }
  filter-profile profile-name {
    counters {
      counter-name;
    }
    file filename;
    interval minutes;
  }
  interface-profile profile-name {
    fields {
      input-bytes;
      input-errors;
      input-multicast;
      input-packets;
      input-unicast;
      output-bytes;
      output-errors;
      output-multicast;
      output-packets;
      output-unicast;
      rpf-check-bytes;
      rpf-check-packets;
      rpf-check6-bytes;
      rpf-check6-packets;
      unsupported-protocol;
    }
    file filename;
    interval minutes;
  }
  mib-profile profile-name {
    file filename;
```

```
    interval minutes;
    object-names {
      mib-object-name;
    }
    operation (get | get-next | walk);
  }
  policy-decision-statistics-profile profile-name {
    application-aware-access-list-fields {
      address;
      application;
      application-group;
      input-bytes;
      input-interface;
      input-packets;
      mask;
      output-bytes;
      output-packets;
      subscriber-name;
      timestamp;
      vrf-name;
    }
    file filename;
  }
  routing-engine-profile profile-name {
    fields {
      field-name;
    }
    file filename;
    interval minutes;
  }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure options for accounting statistics collection.

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

Related Documentation

- Understanding RADIUS Accounting on page 199
- Juniper-Switching-Filter VSA Match Conditions and Actions on page 197
- Configuring RADIUS System Accounting on page 200
- Configuring Remote Template Accounts for User Authentication on page 164
- Configuring Local User Template Accounts for User Authentication on page 162

accounting-order

Syntax accounting-order (radius | [*accounting-order-data-list*]);

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

Release Information Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Specify the order in which accounting methods are used.

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

[*accounting-order-data-list*]—Set of data listing the accounting order to be used, enclosed in brackets. This can be any combination of accounting methods, up to and including a list of the entire accounting order.

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

Related Documentation

- *Configuring the Accounting Order*

always-write-option-82

Syntax

```
always-write-option-82 {
  apply-groups;
    apply-groups-except;
  }
```

Hierarchy Level

[edit forwarding-options dhcp-relay overrides]

Release Information

Statement introduced in Junos OS Release 15.1X49-D100.

Description

Override the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server. Using this option allows the DHCP relay agent to perform one of the following actions, depending on the configuration:

- If the DHCP relay agent is configured to add option 82 information to the DHCP packets, the DHCP relay agent clears the existing option 82 values from the DHCP packets and inserts the new values before forwarding the packets to the DHCP server.
- If the DHCP relay agent is not configured to add option 82 information to DHCP packets, the DHCP relay agent clears the existing option 82 values from the packets, but does not add any new values before forwarding the packets to the DHCP server.

Required Privilege Level

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

Related Documentation

- replace-ip-source-with (Before Forwarding Packet) on page 1414
- overrides (New Relay Options) on page 1317

authentication-order

Syntax authentication-order [**none** | **password** | **radius**];

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure the order of authentication, authorization, and accounting (AAA) servers to use while sending authentication messages.

Default Not enabled

Options **none**—No authentication for specified subscribers.

password—Password authentication.

radius—RADIUS authentication.

NOTE: The **[edit access]** hierarchy is not available on QFabric systems.

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

accounting-server

Syntax accounting-server[*server-addresses*];

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure the Remote Authentication Dial-In User Service (RADIUS) server for authentication. To configure multiple RADIUS servers, include multiple server addresses. 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.

Default Not enabled

Options ***server-addresses***—One or more addresses of RADIUS authentication servers.

NOTE: The **[edit access]** hierarchy is not available on QFabric systems.

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

Related Documentation

- show network-access aaa statistics authentication on page 1855
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Understanding 802.1X and RADIUS Accounting on Switches on page 332
- Understanding RADIUS Accounting on page 199

accounting-stop-on-access-deny

Syntax accounting-stop-on-access-deny;

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure the authentication order for authentication, authorization, and accounting (AAA) services to send an Acct-Stop message if the AAA server denies access to a supplicant.

NOTE: The **[edit access]** hierarchy is not available on QFabric systems.

Default Not enabled

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

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335
- **show network-access aaa statistics authentication on page 1855**

accounting-stop-on-failure

Syntax accounting-stop-on-failure;

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure RADIUS accounting to send an Acct-Stop message when a subscriber session has been successfully authenticated and authorized, but then fails before an Acct-Start message is sent. By default, an Acct-Stop message is sent only if an Acct-Start message has been exchanged with the accounting server.

Consider a situation where RADIUS address pools are used to assign IP/IPv6 addresses. After a subscriber session is successfully authenticated, the RADIUS server authorizes the session by assigning an IP address from the RADIUS address pool and conveying that address in the Framed-IP-Address attribute. If a negotiation failure occurs at this point, the session is terminated before activating. The Acct-Start message is never sent because it is initiated by session activation. By default, an Acct-Stop message cannot be sent because the Acct-Start is never sent. However, if the **acct-stop-on-failure** statement is configured, the negotiation failure causes the Acct-Stop message to be sent, which explicitly notifies the RADIUS server that the session is disconnected and that it can free the allocated IP address back to the pool.

NOTE: **The [edit access] hierarchy is not available on QFabric systems.**

Default Disabled

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

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335
- Understanding 802.1X and RADIUS Accounting on Switches on page 332
- Understanding RADIUS Accounting on page 199

add-interface-text-description

Syntax

```
add-interface-text-description;
```

Hierarchy Level

[edit protocols dot1x authenticator radius-options]

Release Information

Statement introduced in Junos OS Release 18.4R1 for EX Series switches.

Description

Configure the NAS-Port-ID attribute to include the text description of the interface to which a RADIUS client is connected. The NAS-Port-ID is a RADIUS attribute that is included in the Access-Request message sent from a client to the RADIUS server. By default, the attribute is populated with the name of the logical interface. Including the text description provides more information to the RADIUS server, which can use the information to assign the client to a different VLAN or apply a firewall filter for authentication.

The text description of the interface is configured under the [**edit interfaces** ***interface-name***] hierarchy level. When you configure the **add-interface-text-description** option under the [**edit protocols dot1x authenticator radius-options**] hierarchy level, the text description is appended to the interface name in the Access-Request message in the format *interface-name#interface-text-description*.

If there is a text description configured for the logical interface, it is used in the NAS-Port-ID; otherwise, the text description for the physical interface is used. If neither is configured then the NAS-Port-ID will only contain the interface name.

There is no character limit for the interface text description; however, the total length of the NAS-Port-ID with the interface name and description combined is restricted to 253 characters. If the total length exceeds 253 characters, the description is truncated.

Required Privilege Level

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

Related Documentation

- Understanding 802.1X and RADIUS Accounting on Switches on page 332
- Understanding Dynamic Filters Based on RADIUS Attributes on page 306
- Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 307

address (Access Control Service)

Syntax address *ip-address*;

Hierarchy Level [edit services unified-access-control infranet-controller]

Release Information Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description Specify the address through which the switch will connect to the Junos Pulse Access Control Service.

Options ***ip-address***—Specify the IP address of the NAC device.

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

Related Documentation

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 401

address-assignment (Access)

Syntax

```
address-assignment {
  abated-utilization percentage;
  abated-utilization-v6 percentage;
  high-utilization percentage;
  high-utilization-v6 percentage;
  neighbor-discovery-router-advertisement ndra-name;
  pool pool-name {
    family {
      inet {
        dhcp-attributes {
          boot-file boot-file-name;
          boot-server boot-server-name;
          domain-name domain-name;
          grace-period seconds;
          maximum-lease-time (seconds | infinite);
          name-server ipv4-address;
          netbios-node-type (b-node | h-node | m-node | p-node);
          next-server next-server-name;
          option dhcp-option-identifier-code {
            array {
              byte [8-bit-value];
              flag [ false| off |on |true];
              integer [32-bit-numeric-values];
              ip-address [ip-address];
              short [signed-16-bit-numeric-value];
              string [character string value];
              unsigned-integer [unsigned-32-bit-numeric-value];
              unsigned-short [16-bit-numeric-value];
            }
            byte 8-bit-value;
            flag (false | off | on | true);
            integer 32-bit-numeric-values;
            ip-address ip-address;
            short signed-16-bit-numeric-value;
            string character string value;
            unsigned-integer unsigned-32-bit-numeric-value;
            unsigned-short 16-bit-numeric-value;
          }
          option-match {
            option-82 {
              circuit-id match-value {
                range range-name;
              }
              remote-id match-value;
                range range-name;
              }
            }
          }
          propagate-ppp-settings [interface-name];
          propagate-settings interface-name;
          router ipv4-address;
```

```
        server-identifier ip-address;
        sip-server {
          ip-address ipv4-address;
          name sip-server-name;
        }
        tftp-server server-name;
        wins-server ipv4-address;
      }
      host hostname {
        hardware-address mac-address;
        ip-address reserved-address;
      }
      network network address;
      range range-name {
        high upper-limit;
        low lower-limit;
      }
      excluded-range range-name
        high upper-limit;
        low lower-limit;
      }
      xauth-attributes {
        primary-dns ip-address;
        primary-wins ip-address;
        secondary-dns ip-address;
        secondary-wins ip-address;
      }
    }
    inet6 {
      dhcp-attributes {
        dns-server ipv6-address;
        grace-period seconds;
        maximum-lease-time (seconds | infinite);
        option dhcp-option-identifier-code {
          array {
            byte [8-bit-value];
            flag [ false| off |on |true];
            integer [32-bit-numeric-values];
            ip-address [ip-address];
            short [signed-16-bit-numeric-value];
            string [character string value];
            unsigned-integer [unsigned-32-bit-numeric-value];
            unsigned-short [16-bit-numeric-value];
          }
          byte 8-bit-value;
          flag (false | off | on | true);
          integer 32-bit-numeric-values;
          ip-address ip-address;
          short signed-16-bit-numeric-value;
          string character string value;
          unsigned-integer unsigned-32-bit-numeric-value;
          unsigned-short 16-bit-numeric-value;
        }
        propagate-ppp-settings [interface-name];
        sip-server-address ipv6-address;
```

```
            sip-server-domain-name domain-name;
          }
          prefix ipv6-network-prefix;
          range range-name {
            high upper-limit;
            low lower-limit;
            prefix-length delegated-prefix-length;
          }
            excluded-range range-name
              high upper-limit;
              low lower-limit;
            }
        }
      link pool-name;
    }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 10.4 for SRX300, SRX320, SRX340, SRX345, SRX550HM devices.

Description The address-assignment pool feature enables you to create IPv4 and IPv6 address pools that different client applications can share. For example, multiple client applications, such as DHCPv4 or DHCPv6, can use an address-assignment pool to provide addresses for their particular clients.

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

Related Documentation

- *Dynamic VPN Overview*

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 {
    active-drain;
    family family {
      dhcp-attributes {
        protocol-specific attributes;
      }
      excluded-address ip-address;
      excluded-range name low minimum-value high maximum-value;
      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;
      }
    }
    hold-down;
    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: Support for subordinate statements is platform-specific. See individual statement topics for support information.

Options

abated-utilization—(ACX Series, MX Series only) Starting in Junos OS Release 11.2, generate SNMP traps for DHCP address pools or linked set of address pools. No

SNMP traps are generated unless a value is configured. Default: Abated utilization is not set. Delete the abated-utilization value to unset.

Values: *percentage*—Threshold below which an SNMP trap clear is generated. Range: 1 through 98.

abated-utilization-v6—(ACX Series, MX Series only) Starting in Junos OS Release 11.2, generate SNMP traps for DHCPv6 address pools or linked set of address pools. No SNMP traps are generated unless a value is configured. Default: Abated utilization is not set. Delete the abated-utilization value to unset.

Values: *percentage*—Threshold below which an SNMP trap clear is generated. Range: 1 through 98.

high-utilization—(ACX Series, MX Series only) Starting in Junos OS Release 11.2, generate an SNMP trap when the DHCP address pool or linked set of address pools use surpasses the specified percentage. Default: High utilization is not set. Delete the high-utilization value to unset.

Values: *percentage*—Percentage used to generate a trap. Range: 2 through 99.

high-utilization-v6—(ACX Series, MX Series only) Starting in Junos OS Release 11.2, generate an SNMP trap when the DHCPv6 address pool or linked set of address pools use surpasses the specified percentage. Default: High utilization is not set. Delete the high-utilization value to unset.

Values: *percentage*—Percentage used to generate a trap. Range: 2 through 99.

neighbor-discovery-router-advertisement—(M Series, MX Series, SRX Series, T Series only) Configure the name of the address-assignment pool used to assign the router advertisement prefix.

Values: *ndra-pool-name*—Name of the address-assignment pool.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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*
- *Address-Assignment Pool Configuration Overview*
- *Configuring an Address-Assignment Pool for L2TP LNS with Inline Services*
- *Configuring Address-Assignment Pool Usage Threshold Traps*
- *Configuring an Address-Assignment Pool Used for Router Advertisements*

address-pool

Syntax

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

Hierarchy Level

```
[edit access]
```

Release Information

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

Description

Allocate IP addresses for clients.

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

Options

pool-name—Name assigned to an address pool.

address—(EX Series, M Series, PTX Series, T Series only) Configure the IP address or prefix value for clients.

Values: *address-or-prefix*—An address or prefix value.

address-range—Configure the address range.

Values:

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

Required Privilege Level

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

Related Documentation

- *Configuring the Address Pool for L2TP Network Server IP Address Allocation*

address-pool (Access)

Syntax

```
address-pool pool-name {
  address address or address prefix;
  address-range {
    high upper-limit;
    low lower-limit;
    mask network-mask;
  }
  primary-dns IP address;
  primary-wins IP address;
  secondary-dns IP address;
  secondary-wins IP address;
}
```

Hierarchy Level

```
[edit access]
```

Release Information Statement introduced in Junos OS Release 10.4.

Description Create an address-pool for L2TP clients.

Options

- **pool-name**—Name assigned to the address-pool.
- **address**—Configure subnet information for the address-pool.
- **address-range**—Defines the address range available for clients.
- **primary-dns**—Specify the primary-dns IP address.
- **secondary-dns**—Specify the secondary-dns IP address.
- **primary-wins**—Specify the primary-wins IP address.
- **secondary-wins**—Specify the secondary-wins IP address.

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

Related Documentation

- *access-control*

address-protection

Syntax

```
address-protection {
  reassign-on-match;
}
```

Hierarchy Level

[edit access],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* access]

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 on EX Series switches.
reassign-on-match option added in Junos OS Release 18.4R1.

Description

Prevent IPv4 addresses and IPv6 prefixes from being assigned to more than one subscriber session when you use AAA to supply IPv4 addresses.

For IPv4:

If enabled, the router checks the following attributes received from external servers:

- *Framed-IP-Address*
- *Framed-Pool*

The router then takes one of the following actions:

- If an address matches an address in an address pool, the address is taken from the pool, provided it is available.
- If the address is already in use, it is rejected as unavailable.

For IPv6:

If enabled, the router checks the following attributes received from external servers:

- *Framed-IPv6-Prefix*
- *Framed-IPv6-Pool*

The router then takes one of the following actions:

- If a prefix matches a prefix in an address pool, the prefix is taken from the pool, provided it is available.
- If the prefix is already in use, it is rejected as unavailable.
- If the prefix length requested from the external server does not exactly match the pool's prefix length, the authentication request is denied. If configured, the Acct-Stop message includes the cause for termination.

Options

reassign-on-match—Enable reassignment of an address from an existing subscriber to a new subscriber requesting that address. The address in use must not be part of a locally configured pool and address protection must be enabled. The request from the new subscriber is still rejected, but the existing subscriber is sent a disconnect request to begin the logout process. This enables the new subscriber to renegotiate and be assigned that IP address.

If the requested address is in a locally configured pool, the existing subscriber is not disconnected.

NOTE: This option is not supported for IPv6.

Default: Rejects the address request from the new subscriber; the existing subscriber remains intact with the IP address.

Required Privilege Level

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

Related Documentation

- *Configuring Duplicate IPv4 Address Protection for AAA*
- *Configuring Duplicate IPv6 Prefix Protection for Router Advertisement*

advertisement-interval

Syntax advertisement-interval *seconds*;

Hierarchy Level [edit protocols lldp],
[edit routing-instances *routing-instance-name* protocols lldp]

Release Information Statement introduced in Junos OS Release 9.6 for MX Series and T Series routers.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure an interval for LLDP advertisement.

For switches configured for Link Layer Discovery Protocol, configure the frequency at which LLDP advertisements are sent.

The **advertisement-interval** value must be greater than or equal to four times the **transmit-delay** value, or an error will be returned when you attempt to commit the configuration.

NOTE: The default value of **transmit-delay** is 2 seconds. If you configure the **advertisement-interval** as less than 8 seconds and you do not configure a value for **transmit-delay**, the default value of **transmit-delay** is automatically changed to 1 second in order to satisfy the requirement that the **advertisement-interval** value must be greater than or equal to four times the **transmit-delay** value.

Default Disabled.

Options ***seconds***—Interval between LLDP advertisement.
Default: 30
Range: 5 through 32768

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

Related Documentation

- *Configuring LLDP*
- show lldp on page 1826
- Configuring LLDP (CLI Procedure) on page 512

- Understanding LLDP and LLDP-MED on EX Series Switches on page 518
- **transmit-delay on page 1570**
- Understanding LLDP on page 511

agent-address

Syntax agent-address outgoing-interface;

Hierarchy Level [edit snmp trap-options]

Release Information Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series and EX4600.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Set the agent address of all SNMPv1 traps generated by this router or switch. Currently, the only option is **outgoing-interface**, which sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

Options **outgoing-interface**—Value of the agent address of all SNMPv1 traps generated by this router or switch. The **outgoing-interface** option sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

Default: disabled (the agent address is not specified in SNMPv1 traps).

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

Related Documentation
- *Configuring the Agent Address for SNMP Traps*

allow-commands

Syntax allow-commands *"(regular-expression)|(regular-expression1)|(regulare-expression2)..."*;

Hierarchy Level [edit system login class *class-name*]

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 operational mode commands that members of a login class can use.

When specifying extended regular expressions using the **allow/deny-commands** and **allow/deny-configuration** statements, each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses ( ). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.

Default If you omit this statement and the **deny-commands** statement, users can issue only those commands for which they have access privileges through the **permissions** statement.

Options *regular-expression*—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

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

Related Documentation

- Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 112
- deny-commands on page 968
- user on page 1597

allow-commands-regexps

Syntax allow-commands-regexps *["regular expression 1" "regular expression 2" ....]*;

Hierarchy Level [edit system login class *class-name*]

Release Information Statement introduced in Junos OS Release 18.1.

Description Configure authorizations for operational mode commands using regular expressions. You can use the **allow-commands-regexps** statement to explicitly allow authorization for commands that would otherwise be denied by an access privilege level.

For **allow/deny-commands-regexps** statements, you configure a set of strings in which each string is a regular expression, enclosed in double quotes and separated with a space operator. Each string is evaluated against the full path of the command, which provides faster matching than the **allow/deny-command** statements. You can also include values for variables in the regular expressions, which is not supported using **allow/deny-commands**.

The statement **deny-commands-regexps** takes precedence if it is used in the same login class definition.

NOTE: The **allow/deny-commands** and **allow/deny-commands-regexps** statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the **allow/deny-commands** statement, or the **allow/deny-commands-regexps** statement. If you have existing configurations using the **allow/deny-commands** statements, using the same configuration options with the **allow/deny-commands-regexps** statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

Authorizations can also be configured remotely by specifying Juniper Networks vendor-specific TACACS+ attributes in your authentication server's configuration. For a remote user, when the authorization parameters are configured both remotely and locally, authorization parameters configured remotely and locally are both considered together for authorization. For a local user, only the authorization parameters configured locally for the class are considered.

Default If you do not configure authorizations for operational mode commands using **allow/deny-commands** or **allow/deny-commands-regexps**, users can edit only those commands for which they have access privileges set with the **permissions** statement.

Options

regular expression—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Enter as many expressions as needed.

Required Privilege Level

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

Related Documentation

- Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies on page 125
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 99
- **deny-commands-regexps on page 969**

allow-configuration

Syntax allow-configuration *"(regular-expression)|(regular-expression1)|(regulare-expression2)..."*;

Hierarchy Level [edit system login class *class-name*]

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

Description Explicitly allow configuration access to the specified levels in the hierarchy even if the permissions set with the **permissions** statement do not grant such access by default.

When specifying extended regular expressions using the **allow/deny-commands** and **allow/deny-configuration** statements, each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses ( ). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.

NOTE: The **allow/deny-configuration** and **allow/deny-configuration-regexps** statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the **allow/deny-configuration** statement, or the **allow/deny-configuration-regexps** statement. If you have existing configurations using the **allow/deny-configuration** statements, using the same configuration options with the **allow/deny-configuration-regexps** statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

Default If you omit this statement and the **deny-configuration** statement, users can edit only those commands for which they have access privileges through the **permissions** statement.

Options *regular-expression*—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

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

Related Documentation

- Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 112

- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 99
- deny-configuration on page 971
- user on page 1597

allow-configuration

Syntax

```
allow-configuration "regular-expression";
```

Hierarchy Level

```
[edit system login class class-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.2 for SRX Series devices.

Description

Explicitly allow configuration access to the specified levels in the hierarchy even if the permissions set with the **permissions** statement do not grant such access by default.

Default

If you omit this statement and the **deny-configuration** statement, users can edit only those commands for which they have access privileges through the **permissions** statement.

Options

regular-expression—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

Required Privilege Level

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

allow-configuration-regexps

Syntax allow-configuration-regexps "*regular expression 1*" "*regular expression 2*";

Hierarchy Level [edit system login **class** *class-name*]

Release Information Statement introduced in Junos OS Release 11.2.

Description Explicitly allow configuration access to specified hierarchies using regular expressions even if the permissions set with the **permissions** statement allow that access.

The statement **deny-configuration-regexps** takes precedence if it is used in the same login class definition.

Default If you do not configure this statement or the **deny-configuration-regexps** statement, users can edit only those commands for which they have access privileges set with the **permissions** statement.

Options *regular expression*—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

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

allow-configuration-regexps

Syntax allow-configuration-regexps *["regular expression 1" "regular expression 2" ....]*;

Hierarchy Level [edit system login class *class-name*]

Release Information Statement introduced in Junos OS Release 11.2.

Description Explicitly allow configuration access to specified hierarchies using regular expressions even if the permissions set with the **permissions** statement allow that access.

The statement **deny-configuration-regexps** takes precedence if it is used in the same login class definition.

NOTE: The **allow/deny-configuration** and **allow/deny-configuration-regexps** statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the **allow/deny-configuration** statement, or the **allow/deny-configuration-regexps** statement. If you have existing configurations using the **allow/deny-configuration** statements, using the same configuration options with the **allow/deny-configuration-regexps** statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

Default If you do not configure this statement or the **deny-configuration-regexps** statement, users can edit only those commands for which they have access privileges set with the **permissions** statement.

Options ***regular expression***—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Enter as many expressions as needed..

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

Related Documentation

- Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies on page 125
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 99
- deny-configuration-regexps on page 973

- user on page 1597

allow-no-end-option (DHCP Relay Agent)

Syntax

```
allow-no-end-option;
```

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group *group-name* overrides],
[edit forwarding-options dhcp-relay group *group-name* interface *interface-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 14.1X53.

Description

Enable a DHCP relay agent to process packets sent from clients without DHCP Option-255 (end-of-options).

The default behavior in Junos OS is to drop packets that do not include Option 255. To override this default behavior, configure the **allow-no-end-option** CLI statement at the **[edit forwarding-options dhcp-relay overrides]** hierarchy level.

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618
- Overriding the Default DHCP Relay Configuration Settings on page 627
- DHCP Snooping Support on page 706

allow-snooped-clients

Syntax

```
allow-snooped-clients;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name
  overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 10.2.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 12.1.

Description

Explicitly enable DHCP snooping support on the DHCP relay agent.

Use the statement at the **[edit ... dhcpv6]** hierarchy levels to explicitly enable snooping support on the router for DHCPv6 relay agent.

Default

DHCP snooping is disabled by default.

NOTE: On EX4300 and EX9200 switches, the **allow-snooped-clients** statement is enabled by default at the **[edit forwarding-options dhcp-relay overrides]** hierarchy level.

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618
- Overriding the Default DHCP Relay Configuration Settings on page 627
- DHCP Snooping Support on page 706
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent on page 710

allowed-days

Syntax allowed-days [*days-of-the-week*];

Hierarchy Level [edit system login class *class-name*]

Release Information Statement introduced in Junos OS Release 10.1.

Description Specify the days of the week when users can log in.

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

Related Documentation

- *Configuring Time-Based User Access*

always-write-giaddr

Syntax

```
always-write-giaddr;
```

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* interface *interface-name* overrides]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Overwrite the gateway IP address (giaddr) of every DHCP packet with the giaddr of the DHCP relay agent before forwarding the packet to the DHCP server.

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618
- dhcp-relay on page 997

always-write-option-82

Syntax

```
always-write-option-82;
```

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* interface *interface-name* overrides]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Override the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server. The use of this option causes the DHCP relay agent to perform one of the following actions, depending on how it is configured:

- If the DHCP relay agent is configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the DHCP packets and inserts the new values before forwarding the packets to the DHCP server.
- If the DHCP relay agent is not configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the packets, but does not add any new values before forwarding the packets to the DHCP server.

Required Privilege Level

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

Related Documentation

- Using DHCP Relay Agent Option 82 Information on page 633
- Extended DHCP Relay Agent Overview on page 618

announcement

Syntax

```
announcement text;
```

Hierarchy Level

```
[edit system login]
```

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 system login announcement. This announcement appears after a user logs in.

Options

text—Text of the announcement. If the text contains any spaces, enclose it in quotation marks.

Required Privilege Level

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

Related Documentation

- Configuring Junos OS to Display a System Login Announcement on page 55
- message on page 1234

archival

Syntax

```
archival {
  configuration {
    archive-sites {
      file://<path>/<filename>;
      ftp://username@host:<port>url-path password password;
      http://username@host:<port>url-path password password;
      pasvftp://username@host:<port>url-path password password;
      scp://username@host:<port>url-path password password;
    }
    transfer-interval interval;
    transfer-on-commit;
  }
  routing-instance routing-instance;
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Configure copying of the currently active configuration to an archive site. An archive site can be a file, or an FTP, HTTP, or SCP location.

Options

configuration—Configure the router or switch to periodically transfer its currently active configuration (or after each commit). Parameters include **archive-sites**, **transfer-interval**, and **transfer-on-commit**.

NOTE: The **[edit system archival]** hierarchy is not available on QFabric systems.

archive-sites—Specify where to transfer the current configuration files. When specifying a URL in a Junos OS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([ ]). For example: **"scp://*username*<:*password*>@[*ipv6-host-address*]<:*port*>/*url-path*"**.

If you specify more than one archive site, the router or switch attempts to transfer the configuration files to the first archive site in the list, moving to the next only if the transfer fails. The destination filename is saved in the following format, where *n* corresponds to the number of the compressed configuration rollback file that has been archived:

```
router-name_YYYYMMDD_HHMMSS_juniper.conf.n.gz
```

NOTE: The time included in the destination filename is always in Coordinated Universal Time (UTC) regardless of whether the time on the router or switch is configured as UTC or the local time zone. The default time zone on the router or switch is UTC.

transfer-interval—The frequency, in minutes, for transferring the current configuration to an archive site. Valid intervals are 15 to 2880 minutes.

transfer-on-commit—Configure the router or switch to transfer its currently active configuration to an archive site each time you commit a candidate configuration.

routing-instance—Defines the routing instance through a server is reachable.

Required Privilege Level

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

Related Documentation

- *Backing Up Configurations to an Archive Site*

archive-sites

Syntax

```
archive-sites {
  site-name;
}
```

Hierarchy Level

[edit accounting-options file *filename*]

Release Information

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

Description

Configure an archive site. If more than one site name is configured, an ordered list of archive sites for the accounting-data log files is created. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with a filename of the format ***router-name_log-filename_timestamp***.

Options

site-name—Any valid FTP/SCP URL to a destination.

Required Privilege Level

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

Related Documentation

- *Configuring Archive Sites*

attempts (DHCP Local Server)

Syntax

attempts *attempt-count*;

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group *group-name* reconfigure],
[edit system services dhcp-local-server dhcpv6 group *group-name* reconfigure]

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6 ...]** hierarchy levels introduced in Junos OS Release 10.4.

Description

Configure how many attempts are made to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces before reconfiguration is considered to have failed. A group configuration takes precedence over a DHCP local server configuration.

Options

attempt-count—Maximum number of attempts.

Range: 1 through 10

Default: 8

Required Privilege Level

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

Related Documentation

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview on page 662
- Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 664

attributes (RADIUS Attributes)

Syntax

```
attributes {
  exclude {
    attribute-name packet-type;
    standard-attribute number {
      packet-type [ access-request | accounting-off | accounting-on | accounting-start |
        accounting-stop ];
    }
    vendor-id id-number {
      vendor-attribute vsa-number {
        packet-type [ access-request | accounting-off | accounting-on | accounting-start |
          accounting-stop ];
      }
    }
  }
  ignore {
    dynamic-iflset-name;
    framed-ip-netmask;
    idle-timeout;
    input-filter;
    logical-system-routing-instance;
    output-filter;
    session-timeout;
    standard-attribute number;
    vendor-id id-number {
      vendor-attribute vsa-number;
    }
  }
}
```

Hierarchy Level

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

Release Information

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

Description

Specify how the router or switch processes RADIUS attributes.

Options

ignore—Configure the router or switch to ignore the specified attributes in RADIUS Access-Accept messages. Standard attributes and VSAs received in RADIUS messages take precedence over internally provisioned attribute values. Ignoring the attributes enables your internally provisioned values to be used instead. Contrast this behavior with that provided by the exclude statement.

Starting in Junos OS Release 18.1R1, you can specify RADIUS standard attributes with the attribute number. You can specify vendor-specific attributes (VSAs) with the IANA-assigned vendor ID and the VSA number. With this flexible configuration method, you can configure any standard attribute and VSA supported by your

platform to be ignored. The configuration has no effect if you can configure unsupported attributes, vendors, and VSAs.

The legacy method allows you to configure only those attributes and VSAs for which the statement syntax includes a specific option. Consequently, you can use the legacy method to ignore only a subset of all attributes that can be received in Access-Accept messages.

Values:

- dynamic-iflset-name—Ignore Juniper Networks VSA 26-130, Qos-Set-Name.
- framed-ip-netmask—Ignore RADIUS attribute 9, Framed-IP-Netmask.
- idle-timeout—Ignore RADIUS attribute 28, Idle-Timeout.
- input-filter—Ignore Juniper Networks VSA 26-10, Ingress-Policy-Name.
- logical-system-routing-instance—Ignore Juniper Networks VSA 26-1.
- output-filter—Ignore Juniper Networks VSA 26-11, Egress-Policy-Name.
- session-timeout—Ignore RADIUS attribute 27, Session-Timeout.
- standard-attribute *number*—RADIUS standard attribute number supported by your platform. You can enclose multiple values in square brackets to specify a list of attributes. If you configure an unsupported attribute, that configuration has no effect. Range: 1 through 255.
- vendor-attribute *vsa-number*—Number identifying a VSA belonging to the specified vendor; both must be supported by your platform. You can enclose multiple values in square brackets to specify a list of VSAs. If you configure an unsupported VSA, that configuration has no effect. Range: 1 through 255.
- vendor-id *id-number*—IANA vendor ID supported by your platform. If you configure an unsupported vendor ID, that configuration has no effect. Range: 1 through 16777215.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *RADIUS Servers and Parameters for Subscriber Access*
- *Standard and Vendor-Specific RADIUS Attributes*
- *AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS*
- *AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS*

authentication (Login)

Syntax

```
authentication {
  (encrypted-password "password" | plain-text-password);
  load-key-file URL filename;
  no-public-keys;
  ssh-dsa "public-key";
  ssh-ecdsa "public-key";
  ssh-rsa "public-key";
}
```

Hierarchy Level

[edit system login user *username*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Option **no-public-keys** introduced in Junos OS Release 15.1.

Description

Authentication methods that a user can use to log in to the router or switch. You can assign multiple authentication methods to a single user.

Options

encrypted-password "*password*"—Message Digest 5 (MD5) or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.

You cannot configure a blank password for **encrypted-password** using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

load-key-file *URL filename*—Load previously-generated RSA (SSH version 2) and DSA (SSH version 2) public keys from a named file at a specified URL location. The file contains one or more SSH keys.

For information on valid filename and URL formats, see *Format for Specifying Filenames and URLs in Junos OS CLI Commands*.

plain-text-password—When using this option, the command-line interface (CLI) prompts you for the password and then encrypts it.

no-public-keys—Disables public key authentication for the user specified.

ssh-dsa "*public-key*"—SSH version 2 authentication. Specify the DSA public key. You can specify one or more public keys for each user.

ssh-ecdsa "*public-key*"—SSH version 2 authentication. Specify the ECDSA public key. You can specify one or more public keys for each user.

ssh-rsa "*public-key*"—SSH version 2 authentication. Specify the RSA public key. You can specify one or more public keys for each user.

Required Privilege Level

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

Related Documentation

- Configuring Junos OS User Accounts by Using a Configuration Group on page 76
- root-authentication on page 1434

authentication (DHCP Local Server)

Syntax

```
authentication {
  password password-string;
  username-include {
    circuit-type;
    client-id;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-description  (device-interface | logical-interface);
    interface-name;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    relay-agent-interface-id;
    relay-agent-remote-id;
    relay-agent-subscriber-id;
    routing-instance-name;
    user-prefix user-prefix-string;
    vlan-tags;
  }
}
```

Hierarchy Level

```
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group group-name],
[edit system services dhcp-local-server group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
  services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay or DHCP local server configuration.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651

authentication (DHCP Relay Agent)

Syntax

```
authentication {
  password password-string;
  username-include {
    circuit-type;
    client-id;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-description  (device-interface | logical-interface);
    interface-name;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    relay-agent-interface-id;
    relay-agent-remote-id;
    relay-agent-subscriber-id;
    routing-instance-name;
    user-prefix user-prefix-string;
    vlan-tags;
  }
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Support at the **[edit ... dual-stack-group *dual-stack-group-name*]** hierarchy level introduced in Junos OS Release 15.1.

Description

Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay configuration. Use the statement at the **[edit...dhcpv6]** hierarchy levels to configure DHCPv6 support.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- dhcp-relay on page 997
- Using External AAA Authentication Services with DHCP on page 651

authentication-access-control (MX Series in Enhanced LAN Mode)

Syntax

```
authentication-access-control {
    traceoptions {
      file filename <files number> <size size> <world-readable | no-world-readable> <match
        regex>;
      flag flag ;
    }
  uac-policy;
    authentication-profile-name access-profile-name;
    no-mac-table-binding {
      interface  interface-names
      static  mac-address
    }
    static  mac-address {
      interface interface-names;
      vlan-assignment (vlan-id |vlan-name);
    }
    interface (all | [ interface-names ]) {
      session-expiry seconds;
      quiet-period seconds;
      reauthentication {
        interval seconds;
      }
      retries number;
      server-timeout seconds;
      supplicant (single | single-secure | multiple);
      dot1x {
        disable;
        guest-vlan (vlan-id | vlan-name);
        mac-radius {
          flap-on-disconnect;
          restrict;
        }
        maximum-requests number;
        no-reauthentication;
        server-fail (deny | permit | use-cache | vlan-id | vlan-name);
        server-reject-vlan (vlan-id | vlan-name) {
          eapol-block;
          block-interval block-interval;
        }
        supplicant-timeout seconds;
        transmit-period seconds;
      }
    }
  }
  (captive-portal | no-captive-portal);
}
```

Hierarchy Level

```
[edit protocols]
```

Release Information Statement introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description Configure an authenticator for 802.1X and captive-portal authentication.

The remaining statements are explained separately. See CLI Explorer.

NOTE: You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.

Default No static MAC address or VLAN is configured.

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

authentication-profile-name

Syntax

```
authentication-profile-name access-profile-name;
```

Hierarchy Level

```
[edit protocols dot1x authenticator]
```

Release Information Statement introduced in Junos OS Release 9.3.

Description Specify the RADIUS authentication profile to use for user authentication when establishing an IEEE 802.1x Port-Based Network Access Control (**dot1x**) connection.

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

Related Documentation

- IEEE 802.1x Port-Based Network Access Control Overview on page 443
- authenticator on page 890
- *dot1x*

authenticator

Syntax

```
authenticator {
  authentication-profile-name access-profile-name;
  interface interface-id {
    maximum-requests integer;
    quiet-period seconds;
    reauthentication (disable | interval seconds);
    retries integer;
    server-timeout seconds;
    supplicant (single);
    supplicant-timeout seconds;
    transmit-period seconds;
  }
}
```

Hierarchy Level

```
[edit protocols dot1x]
```

Release Information

Statement introduced in Junos OS Release 9.3.

Description

Specify an authentication profile for user or client authentication and configure the Ethernet interface for 802.1x protocol operation.

Options

authentication-profile-name *access-profile-name*—Specifies the RADIUS authentication profile for user or client authentication.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- IEEE 802.1x Port-Based Network Access Control Overview on page 443
- authentication-profile-name on page 889
- *dot1x*

authentication-server

Syntax authentication-server [*server-addresses*];

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

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

Options ***server-addresses***—Configure one or more RADIUS server addresses.

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

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- show network-access aaa statistics authentication on page 1855

authentication-key

Syntax authentication-key *key-number* type *md5* value <*password*>;

Hierarchy Level [edit system *ntp*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure Network Time Protocol (NTP) authentication keys so that the SRX Series device can send authenticated packets. If you configure the SRX Series device to operate in authenticated mode, you must configure a key.

Both the keys and the authentication scheme (MD5) must be identical between a set of peers sharing the same key number.

Options ***key-number***—Positive integer that identifies the key.

type *md5*—Authentication type. It can only be **md5**.

value *password*—The key itself, which can be from 1 through 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.

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

authentication-key-chains

Syntax

```
authentication-key-chains {
  key-chain key-chain-name {
    description text-string;
    key key {
      algorithm (md5 | hmac-sha-1);
      options (basic | isis-enhanced);
      secret secret-data;
      start-time yyyy-mm-dd.hh:mm:ss;
    }
    tolerance seconds;
  }
}
```

Hierarchy Level

[edit security]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos Limited edition for Junos OS Releases 15.1R8, 16.1R7, 16.2R3, 17.1R3, 17.2R3, 17.3R3, and 17.4R2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure authentication key updates for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol. When the **authentication-key-chains** statement is configured at the **[edit security]** hierarchy level, and is associated with the BGP, LDP, or IS-IS protocols at the **[edit protocols]** hierarchy level or with the BFD protocol using the **bfd-liveness-detection** statement, authentication key updates can occur without interrupting routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols on page 226
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

authentication-order

Syntax authentication-order [*method1 method2*...];

Hierarchy Level [edit system]

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 order in which the software tries different user authentication methods when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches.

Default If you do not include the **authentication-order** statement, users are verified based on their configured passwords.

Options One or more of the following authentication methods listed in the order in which they must be tried:

- **password**—Use the password configured for the user with the **authentication** statement at the **[edit system login user]** hierarchy level.
- **radius**—Use RADIUS authentication services.
- **tacplus**—Use TACACS+ authentication services.

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

Related Documentation
- Junos OS User Authentication Methods on page 161

authentication-order

Syntax authentication-order [**none** | **password** | **radius**];

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure the order of authentication, authorization, and accounting (AAA) servers to use while sending authentication messages.

Default Not enabled

Options **none**—No authentication for specified subscribers.

password—Password authentication.

radius—RADIUS authentication.

NOTE: **The [edit access] hierarchy is not available on QFabric systems.**

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

authentication-order (Access Profile)

Syntax authentication-order [(none | ldap | password | radius | secureid)];

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (EX and QFX Series only) Configure the order of authentication, authorization, and accounting (AAA) methods to use while sending authentication messages.

Default Not enabled

Options

none—No authentication for specified subscribers.

ldap— Lightweight Directory Access Protocol.

password—Locally configured password in access profile.

radius—RADIUS authentication.

securid—RSA SecurID authentication.

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

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335

authentication-order (Authenticator)

Syntax authentication-order [dot1x | mac-radius | captive-portal];

Hierarchy Level [edit protocols dot1x authenticator interface *interface-name*]

Release Information Statement introduced in Junos OS Release 15.1R3 for EX Series switches.

Description Configure the preferred order of authentication methods that the switch will use when attempting to authenticate a client. If multiple authentication methods are configured on a single interface, when one authentication method fails, the switch falls back to another method. You can configure the **authentication-order** statement to specify whether 802.1X authentication or MAC RADIUS authentication must be the first authentication method tried.

By default, the switch attempts to authenticate a client by using 802.1X authentication first. If 802.1X authentication fails because there is no response from the client, and MAC RADIUS authentication is configured on the interface, the switch falls back to MAC RADIUS authentication. If MAC RADIUS fails, and captive portal is configured on the switch, the switch falls back to captive portal.

Configuring MAC RADIUS authentication as the first method can help prevent the fallback timeout period which occurs after an 802.1X authentication attempt is made for a host that does not support 802.1X authentication. If MAC RADIUS authentication is configured as the first authentication method on an interface, then on receiving data from any client on that interface, the switch attempts to authenticate the client by using MAC RADIUS authentication. If MAC RADIUS authentication fails, then the switch falls back to 802.1X authentication. If 802.1X authentication fails, and captive portal is configured on the interface, the switch falls back to captive portal.

802.1X authentication always has the highest priority, even if a client has been authenticated using another method. If the switch receives an EAP packet from a client that has been authenticated using MAC RADIUS authentication, the switch acknowledges the EAP packet and upgrades the authentication using 802.1X authentication credentials. Similarly, if a client has been authenticated through fallback to captive portal, and the switch receives an EAP packet from that client, the switch attempts to authenticate the client by using 802.1X authentication.

The switch attempts authentication using only methods that are configured on the interface. If an authentication method is included in the authentication order, but is not configured on the interface, the switch ignores that method and attempts authentication using the next method in the order that is enabled. However, if a method is enabled on the interface, but is not included in the authentication order, the switch does not attempt using that method. For example, if captive portal is enabled for an interface, but the authentication order is configured as **[mac-radius dot1x]**, the authentication method for that interface does not fall back to captive portal.

The authentication order can be configured for all interfaces by using the **interface all** option. If the authentication order is configured for an individual interface, and there is also an authentication order configured for all interfaces, then the order for the individual interface is followed. If there is no authentication order configured for an individual interface, and there is an authentication order configured for all interfaces, then the configuration for all interfaces is followed.

Use the following guidelines when configuring the **authentication-order** statement:

- The authentication order must include at least two methods of authentication.
- 802.1X authentication must be one of the methods included in the authentication order.
- If captive portal is included in the authentication order, it must be the last method in the order.
- If **mac-radius-restrict** is configured on an interface, then the authentication order cannot be configured.

The valid combinations for **authentication-order** are as follows:

- **[dot1x mac-radius captive-portal]**
- **[dot1x captive-portal]**
- **[dot1x mac-radius]**
- **[mac-radius dot1x captive-portal]**

Default If **authentication-order** is not configured, the switch attempts to authenticate the client by using 802.1X authentication first, followed by MAC RADIUS authentication, and then captive portal, as follows:

1. 802.1X authentication—If 802.1X is configured on the interface, the switch sends EAPoL requests to the end device and attempts to authenticate the end device through 802.1X authentication. If the end device does not respond to the EAP requests, the switch checks whether MAC RADIUS authentication is configured on the interface.

2. MAC RADIUS authentication—If MAC RADIUS authentication is configured on the interface, the switch sends the MAC RADIUS address of the end device to the authentication server. If MAC RADIUS authentication is not configured, the switch checks whether captive portal is configured on the interface.

3. Captive portal authentication—If captive portal is configured on the interface, the switch attempts to authenticate the end device by using this method after attempting any other configured authentication methods.

Options

captive-portal—Configure captive portal authentication in the order of authentication methods on the interface.

dot1x—Configure 802.1X authentication in the order of authentication methods on the interface.

mac-radius—Configure MAC RADIUS authentication in the order of authentication methods on the interface.

Required Privilege Level

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

Related Documentation

- Understanding Authentication on Switches on page 268
- Configuring Flexible Authentication Order on page 389

authentication-profile-name

Syntax authentication-profile-name *access-profile-name*;

Hierarchy Level [edit protocols dot1x authenticator],
[edit services captive-portal]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Added to **[edit services captive-portal]** hierarchy in Junos OS Release 10.1 for EX Series switches.

Description Specify the name of the access profile to be used for 802.1X, MAC RADIUS, or captive portal authentication.

Default No access profile is specified.

Options *access-profile-name*—Name of the access profile. The access profile is configured at the [**edit access profile**] hierarchy level and contains the RADIUS server IP address and other information used for authentication.

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

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 326
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- *Configuring 802.1X Authentication (J-Web Procedure)*
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

authentication-protocol

Syntax

```
authentication-protocol (eap-md5 | pap);
```

Hierarchy Level

[edit protocols dot1x authenticator interface *interface-name* mac-radius]

Release Information

Statement introduced in Junos OS Release 15.1R3 for EX Series switches.
The **eap-peap** was introduced in Junos OS Release 17.2R1 for EX Series switches.

Description

Specify the protocol to be used by a supplicant to provide authentication credentials for MAC RADIUS authentication. The protocols supported for MAC RADIUS authentication are EAP-MD5, which is the default, Protected Extensible Authentication Protocol (EAP-PEAP),and Password Authentication Protocol (PAP).

Default

If **authentication-protocol** is not configured, the EAP-MD5 authentication protocol is used for MAC RADIUS authentication.

Options

eap-md5—Use the EAP-MD5 protocol for MAC RADIUS authentication. EAP-MD5 is an authentication method belonging to the Extensible Authentication Protocol (EAP) authentication framework. EAP-MD5 uses MD5 to hash the username and password. EAP-MD5 provides for a one-way client authentication. The server sends the client a random request for which the client must provide a response containing an encryption of the request and its password for establishing its identity.

eap-peap—Use the EAP-PEAP protocol, also known as Protected EAP or PEAP, for MAC RADIUS authentication. EAP-PEAP is a protocol that encapsulates EAP within a potentially encrypted and authenticated Transport Layer Security (TLS) tunnel. By encapsulating the authentication process in a TLS tunnel, PEAP addresses the vulnerabilities of an EAP like EAP-MD5.

pap—Use the PAP authentication protocol for MAC RADIUS authentication. PAP provides a simple password-based authentication for users to establish their identity by using a two-way handshake. PAP transmits plaintext passwords over the network without encryption. PAP must be configured if the Lightweight Directory Access Protocol (LDAP), which supports only plaintext passwords for client authentication, is used for RADIUS authentication.

Required Privilege Level

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

Related Documentation

- Understanding Authentication on Switches on page 268
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335

authentication-whitelist

Syntax

```
authentication-whitelist {
  mac-address {
  interface interface-name;
  vlan-assignment ( vlan-id |vlan-name);
}
```

Hierarchy Level

```
[edit ethernet-switching-options];
[edit switch-options]
```

Release Information

Statement introduced in Junos OS Release 10.1 for EX Series switches.
The **[edit switch-options]** hierarchy level was introduced in Junos OS Release 13.2X50-D10 for EX Series switches (ELS).

Description

Configure MAC addresses for which RADIUS authentication is to be bypassed.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Example: Setting Up Captive Portal Authentication on an EX Series Switch with ELS Support on page 384
- Configuring Captive Portal Authentication (CLI Procedure) on page 378
- Configuring Captive Portal Authentication (CLI Procedure) on an EX Series Switche with ELS Support on page 383

authenticator

Syntax

```
authenticator {
  authentication-profile-name access-profile-name;
  interface (all | [ interface-names ]) {
    disable;
    guest-vlan ( vlan-id | vlan-name);
    lldp-med-bypass;
    mac-radius <restrict>;
    maximum-requests number;
    no-reauthentication;
    quiet-period seconds;
    reauthentication interval;
    retries number;
    server-fail (deny | permit | use-cache | vlan-id | vlan-name);
    server-reject-vlan (vlan-id | vlan-name) {
      eapol-block;
       block-interval block-interval;
    }
    server-timeout seconds;
    supplicant (single | single-secure | multiple);
    supplicant-timeout seconds;
    transmit-period seconds;
  }
  no-mac-table-binding {
    interface interface-names;
    static mac-address;
  }
  radius-options {
    use-vlan-id;
    use-vlan-name;
  }
  static mac-address {
    vlan-assignment vlan-identifier;
  }
}
```

Hierarchy Level

```
[edit protocols dot1x]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure an authenticator for 802.1X authentication.

The remaining statements are explained separately. See CLI Explorer.

NOTE: You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.

Default 802.1X authentication is disabled.

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

Related Documentation
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- Specifying RADIUS Server Connections on Switches (CLI Procedure) on page 283
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 368

authorization

Syntax
```
authorization authorization;
```

Hierarchy Level
```
[edit snmp community community-name]
```

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Set the access authorization for SNMP **Get**, **GetBulk**, **GetNext**, and **Set** requests.

Options ***authorization***—Access authorization level:

- **read-only**—Enable **Get**, **GetNext**, and **GetBulk** requests.
- **read-write**—Enable all requests, including **Set** requests. You must configure a view to enable **Set** requests.

NOTE: **The read-write option is not supported on the QFX3000 QFabric system.**

Default: read-only

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

Related Documentation
- *Configuring the SNMP Community String*

authorization-time-interval

Syntax authorization-time-interval *minutes*;

Hierarchy Level [edit system tacplus-options]

Release Information Statement introduced in Junos OS Release 17.4R1.

Description Configure the time interval at which the JUNOS device has to fetch the authorization profile configuration from the TACACS+ server and refresh the authorization profile stored locally on the JUNOS device. The TACACS+ server sends the authorization profile once by default after the user is successfully authenticated, and the authorization profile is stored locally on the JUNOS device. The authorization profile refresh feature enables the JUNOS device to check the authorization profile configured remotely on the TACACS+ server at the configured time interval.

If there is a change in the remote authorization profile, the device fetches the authorization profile from the TACACS+ server and the authorization profile configured locally under the login class hierarchy. The device refreshes the authorization profile stored locally by combining the remote and locally-configured authorization profiles. This ensures that any changes made to the authorization profile configuration on the TACACS+ server are reflected on the JUNOS device without the user having to restart the authentication process.

To enable periodic refresh of the authorization profile, you must set the time interval at which the JUNOS device has to fetch the authorization profile configuration from the TACACS+ server and refresh the authorization profile stored locally. The time interval can be configured directly on the TACACS+ server or locally on the JUNOS device using the CLI. Use the following guidelines to determine which time interval configuration takes precedence:

- If there is no refresh time interval configured on the TACACS server for periodic refresh, the JUNOS device does not receive the time interval value in the authorization response. In this case, the value configured locally on the JUNOS device will take effect.
- If the refresh time interval is configured on the TACACS server and there is no refresh time interval configured locally on the JUNOS device, the value configured on the TACACS server will take effect.
- If refresh time interval is configured on the TACACS server and also on the JUNOS device locally, the value configured on the TACACS server will take precedence.
- If there is no refresh time interval configured on the TACACS server and there is no refresh time interval configured on the JUNOS device, there will be no periodic refresh.
- If the refresh time interval configured on the TACACS server is out of range or invalid, the refresh time interval value configured locally will take effect.

- If the refresh time interval configured on the TACACS server is out of range or invalid and there is no refresh time interval configured locally, there will be no periodic refresh.

After the periodic refresh time interval is set, if the user changes the refresh interval before the authorization request is sent from the JUNOS device, the updated refresh interval takes effect after the next immediate periodic refresh.

Default If the authorization time interval is not configured, the authorization profile is not refreshed during a TACACS+ authentication session.

Options ***minutes***—The time interval at which the authorization profile that is configured on the TACACS+ server is fetched by the JUNOS device during a TACACS+ authentication session.

Range: 15 to 1440 minutes.

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

Related Documentation

- tacplus-options on page 1525
- Configuring Periodic Refresh of the TACACS+ Authorization Profile on page 213

backoff-factor

Syntax backoff-factor *seconds*;

Hierarchy Level **[edit system login** retry-options**]**

Release Information Statement introduced in Junos OS Release 8.0.

Description Configure the length of delay after each failed login attempt, which increases for each subsequent login attempt after the value specified in the **backoff-threshold** statement.

Options *seconds*—Length of delay after each failed login attempt. The length of delay increases by this value for each subsequent login attempt after the value specified in the **backoff-threshold** option.

Range: 5 through 10

Default: 5

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

Related Documentation

- Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 60
- retry-options on page 1428

backoff-threshold

Syntax backoff-threshold *number*;

Hierarchy Level **[edit system login** retry-options**]**

Release Information Statement introduced in Junos OS Release 8.0.

Description Configure the threshold for the number of failed login attempts on the router before the user experiences a delay when attempting to reenter a password.

Options *number*—Threshold for the number of failed login attempts before the user experiences a delay when attempting to reenter a password. Use the **backoff-factor** option to specify the length of delay, in seconds.

Range: 1 through 3

Default: 2

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

Related Documentation

- Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 60
- retry-options on page 1428

bfd

Syntax

```
bfd {
  version (0 | 1 | automatic);
  minimum-interval milliseconds;
  minimum-receive-interval milliseconds;
  multiplier number;
  no-adaptation;
  transmit-interval {
    minimum-interval milliseconds;
    threshold milliseconds;
  }
  detection-time {
    threshold milliseconds;
  }
  session-mode (automatic | multihop | singlehop);
  holddown-interval milliseconds;
}
```

Hierarchy Level

[edit system services dhcp-local-server liveness-detection method],
[edit system services dhcp-local-server dhcpv6 liveness-detection method],
[edit forwarding-options dhcp-relay liveness-detection method],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method],
[edit system services dhcp-local-server group *group-name* liveness-detection method],
[edit system services dhcp-local-server dhcpv6 group *group-name* liveness-detection method],
[edit forwarding-options dhcp-relay group *group-name* liveness-detection method],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name* liveness-detection method]

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure Bidirectional Forwarding Detection (BFD) as the liveness detection method.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677

block-interval

Syntax

```
block-interval block-interval;
```

Hierarchy Level

```
[edit protocols dot1x authenticator interface (all | [interface-names]) server-reject-vlan
  (vlan-id | vlan-name)],
[edit protocols dot1x authenticator interface (all | [interface-names]) server-reject-vlan]
```

Release Information Statement introduced in Junos OS Release 11.2 for EX Series switches.

Description Specify the amount of time that the 802.1X interface ignores Extensible Authentication Protocol (EAP) start messages from the client when an EAPoL block has been enabled on the 802.1X interface.

Options ***block-interval***—The number of seconds for the interval.

Range: 120 through 65,535

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

Related Documentation

- eapol-block on page 1073
- Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 315

boot-loader-authentication

Syntax

```
boot-loader-authentication {
  (encrypted-password password | plain-text-password);
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced in Junos OS Release 13.2X51-D20 for EX Series switches.

Description

Set the boot-loader password for accessing the U-Boot CLI during the boot process. The password can be entered either as a plain-text password or as an encrypted password.

Encrypted passwords must be entered in Message Digest 5 (MD5) format. Plain-text passwords are encrypted by using MD5 by default. The encryption format for plain-text passwords can be changed by using the **set system login password format** command.

Encrypted passwords must be between 1 and 128 characters long. The password must be enclosed in quotation marks and cannot be blank within the quotation marks (“ “).

The default requirements for plain-text passwords are as follows:

- The password must be between 6 and 128 characters long
- You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
- The password must contain at least one change of case or character class.

Options

encrypted-password *password*— Enter a password that has already been encrypted. You can specify only one encrypted password.

plain-text-password—Enter a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password.

Required Privilege Level

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

Related Documentation

- Using Unattended Mode for U-Boot to Prevent Unauthorized Access on page 280
- format on page 1113
- unattended-boot on page 1583

boot-server (NTP)

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

Hierarchy Level [edit system *ntp*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the server that NTP queries when the SRX Series device boots to determine the local date and time.

When you boot the SRX Series device, it issues an **ntpdate** request, which polls a network server to determine the local date and time. You need to configure a server that the SRX Series device uses to determine the time when the SRX Series device boots. You can configure either an IP address or a hostname for the boot server. If you configure a hostname instead of an IP address, the **ntpdate** request resolves the hostname to an IP address when the SRX Series device boots up.

If you configure an NTP boot server, then when the SRX Series device boots, it immediately synchronizes with the boot server even if the NTP process is explicitly disabled or if the time difference between the client and the boot server exceeds the threshold value of 1000 seconds.

Options

- ***address***—The IP address of an NTP boot server.
- ***hostname***—The hostname of an NTP boot server.

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

Related Documentation

- *ntp*

boot-server (DHCP)

Syntax

```
boot-server (address | hostname);
```

Hierarchy Level

```
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

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 name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup.

Options

- ***address***—IP address of a DHCP boot server.
- ***hostname***—Hostname of a DHCP boot server.

Required Privilege Level

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

Related Documentation

- *boot-file*

broadcast

Syntax

```
broadcast address <key key-number> <routing-instance-name routing-instance-name> <ttl
  value> <version value>;
```

Hierarchy Level

```
[edit system ntp]
```

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the SRX Series device to operate in broadcast mode with the remote system at the specified address. In this mode, the SRX Series device sends periodic broadcast messages to a client population at the specified broadcast or multicast address. Normally, you include this statement only when the SRX Series device is operating as a transmitter.

Options

address—The broadcast address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. If the multicast address is used, it must be **224.0.1.1**.

key *key-number*—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.

Range: Any unsigned 32-bit integer

routing-instance-name *routing-instance-name*—(Optional) The routing instance name in which the interface has an address in the broadcast subnet.

Default: The default routing instance is used to broadcast packets.

ttl *value*—(Optional) Time-to-live (TTL) value to use.

Range: 1 through 255

Default: 1

version *value*—(Optional) Specify the version number to be used in outgoing NTP packets.

Range: 1 through 4

Default: 4

Required Privilege Level

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

Related Documentation

- *ntp*

broadcast-client

Syntax broadcast-client;

Hierarchy Level [edit system *ntp*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the SRX Series device to listen for broadcast messages on the local network to discover other servers on the same subnet.

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

Related Documentation
- *ntp*

ca-name

Syntax ca-name *ca-identity*;

Hierarchy Level [edit security certificates certification-authority]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify the certificate authority (CA) identity to use in the certificate request.

Options ***ca-identity***—CA identity to use in the certificate request.

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

Related Documentation
- *Specifying the Certificate Authority Name*

ca-type

Syntax

```
ca-type {
  number {
    ca-value value;
  }
}
```

Hierarchy Level

[edit protocols lldp-med interface (all | *interface-name* location civic-based)]

Release Information

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

Description

For Link Layer Discovery Protocol–Media Endpoint Device (LLDP-MED), configure the address elements. These elements are included in the location information to be advertised from the switch to the MED. This information is used during emergency calls to identify the location of the MED.

For further information about the values that can be used to comprise the location,, refer to RFC 4776, *Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information*. A subset of those values is provided below.

The **ca-value** statement is explained separately.

Default

Disabled.

Options

value—Civic address elements that represent the civic or postal address. Values are:

- **0**—A code that specifies the language used to describe the location.
- **16**—The leading-street direction, such as “N”.
- **17**—A trailing street suffix, such as “SW”.
- **18**—A street suffix or type, such as “Ave” or “Platz”.
- **19**—A house number, such as “6450”.
- **20**—A house-number suffix, such as “A” or “1/2”.
- **21**—A landmark, such as “Stanford University”.
- **22**—Additional location information, such as “South Wing”.
- **23**—The name and occupant of a location, such as “Carrillo's Holiday Market”.
- **24**—A house-number suffix, such as “95684”.
- **25**—A building structure, such as “East Library”.

Required Privilege Level

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

Related Documentation

- show lldp on page 1826
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Configuring LLDP-MED (CLI Procedure) on page 521

ca-value

Syntax

```
ca-value value;
```

Hierarchy Level

```
[edit protocols lldp-med interface (all | interface-name ) location civic-based ca-type number]
```

Release Information

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

Description

For Link Layer Discovery Protocol–Media Endpoint Device (LLDP-MED), configure location information, such as street address and city, that is indexed by the ca-type code. This information is advertised from the switch to the MED and is used during emergency calls to identify the location of the MED.

Default

Disabled.

Options

value—Specify a value that correlates to the **ca-type**. See ca-type for a list of codes and suggested values.

Required Privilege Level

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

Related Documentation

- show lldp on page 1826
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Configuring LLDP-MED (CLI Procedure) on page 521

cache-size

Syntax cache-size *bytes*;

Hierarchy Level [edit security certificates]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the cache size for digital certificates.

Options ***bytes***—Cache size for digital certificates.

Range: 64 through 4,294,967,295

Default: 2 megabytes (MB)

NOTE: We recommend that you limit your cache size to 4 MB.

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

Related Documentation

- *Configuring the Cache Size*

cache-timeout-negative

Syntax cache-timeout-negative *seconds*;

Hierarchy Level [edit security certificates]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Configure a negative cache for digital certificates.

Options ***seconds***—Negative time to cache digital certificates, in seconds.

Range: 10 through 4,294,967,295

Default: 20

CAUTION: **Configuring a large negative cache value can lead to a denial-of-service attack.**

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

Related Documentation

- *Configuring the Negative Cache*

captive-portal

Syntax

```
captive-portal {
  authentication-profile-name authentication-profile-name
  custom-options {
    banner-message string;
    footer-bgcolor color;
    footer-message string;
    footer-text-color color;
    form-header-bgcolor color;
    form-header-message string;
    form-header-text-color color;
    form-reset-label label name;
    form-submit-label label name;
    header-bgcolor color;
    header-logo filename;
    header-message string;
    header-text-color color;
    post-authentication-url url-string;
  }
  interface (all | [interface-names]) {
    quiet-period seconds;
    retries number-of-retries;
    server-timeout seconds;
    session-expiry seconds;
    supplicant (multiple | single | single-secure);
  }
  secure-authentication (http | https);
}
```

Hierarchy Level

[edit services]

Release Information

Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description

Configure captive portal to authenticate clients connected to the switch for access to the network.

The remaining statements are explained separately. See CLI Explorer.

Default

Captive portal is disabled.

Required Privilege Level

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

Related Documentation

- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Designing a Captive Portal Authentication Login Page on Switches on page 380
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 401
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 404

captive-portal (MX Series in Enhanced LAN Mode)

Syntax

```
(captive-portal | no-captive-portal);
```

Hierarchy Level

```
[edit protocols authentication-access-control]
```

Release Information Statement introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description Specify whether captive portal authentication needs to be enabled or disabled. You can set up captive portal authentication (hereafter referred to as captive portal) on a switch to redirect Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

Default Not enabled

Options **captive-portal**—Enable captive portal authentication.

no-captive-portal—Disable captive portal authentication.

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

captive-portal-custom-options (MX Series in Enhanced LAN Mode)

Syntax

```
captive-portal-custom-options {
  banner-message string;
  footer-bgcolor color;
  footer-message string;
  footer-text-color color;
  form-header-bgcolor color;
  form-header-message string;
  form-header-text-color color;
  form-reset-label label name;
  form-submit-label label name;
  header-bgcolor color;
  header-logo filename;
  header-message string;
  header-text-color color;
  post-authentication-url url-string;
}
```

Hierarchy Level [edit protocols]

Release Information Statement introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description Specify the design elements of a captive portal login page.

Options

banner-message—The first screen displayed before the captive portal login page is displayed—for example, a disclaimer message.

Range: 1–2047 characters

footer-bgcolor —The hexadecimal color code for the color of the footer bar across the bottom of the captive portal login page—for example, #2E8B57 (sea green).

Values: # symbol followed by six characters.

footer-message—Text message displayed in the footer bar across the bottom of the captive portal login page.

Range: 1–2047 characters

Default: **Copyright @2010, Juniper Networks Inc.**

footer-text-color — Color of the text in the footer.

Default: The default color is white.

form-header-bgcolor —The hexadecimal color code for the background color of the header bar across the top of the form area of the captive portal login page.

Values: # symbol followed by six characters.

form-header-message—Text message displayed in the header bar across the top of the form area of the captive portal login page.

Range: 1–255 characters

Default: Captive Portal User Authentication

form-header-text-color—Color of the text in the form header.

Default: The default color is black.

form-reset-label—Label displayed in the button that the user can select to clear the username and password fields on the form.

Range: 1–255 characters

Default: Reset

form-submit-label —Label displayed in the button that the user selects to submit their login information—for example, **Log In** .

Range: 1–255 characters

Default: Log In

header-bgcolor—The hexadecimal color code for the color of the header bar across the top of the captive portal login page.

Values: # symbol followed by six characters.

header-logo—Filename of the file containing the image of the logo displayed at the top of the captive portal login page. The image file can be in GIF, JPEG, or PNG format.

Default: The Juniper Networks logo

header-message—Text displayed in the header bar across the bottom of the captive portal login page.

Range: 1–2047 characters

Default: User Authentication

header-text-color—Color of the text in the header.

Default: The default color is white.

post-authentication-url—URL to which the users are directed upon successful authentication—for example **www.mycafe.com**.

Range: 1–255 characters

Default: The page originally requested by the user.

Required Privilege Level

routing—To view this statement in the configuration.
routing–control—To add this statement to the configuration.

certificate-verification

Syntax certificate-verification (optional | required | warning);

Hierarchy Level [edit services unified-access-control]

Release Information Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description Specify certificate verification requirement for the connection from the switch to Junos Pulse Access Control service.

Default warning

Options **optional**—The specification of a security certificate is optional.

required—The specification of a security certificate is required.

NOTE: **Do not specify this option in Junos OS Release 12.2 for EX Series switches, because the specification of a security certificate (ca-profile) is not supported in this release.**

warning—A warning is issue if a security certificate is not specified. Default.

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

Related Documentation

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 401
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 404
- Understanding Centralized Network Access Control and EX Series Switches on page 399

certificates

Syntax

```
certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority ca-profile-name {
    ca-name ca-identity;
    crl file-name;
    encoding (binary | pem);
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
  }
  enrollment-retry attempts;
  local certificate-name {
    certificate-key-string;
    load-key-file URL filename;
  }
  maximum-certificates number;
  path-length certificate-path-length;
}
```

Hierarchy Level

[edit security]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the digital certificates for IPsec.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring Digital Certificates for an ES PIC*

certification-authority

Syntax

```
certification-authority ca-profile-name {
  ca-name ca-identity;
  crl file-name;
  encoding (binary | pem);
  enrollment-url url-name;
  file certificate-filename;
  ldap-url url-name;
}
```

Hierarchy Level

[edit security certificates]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced before Junos OS Release 12.1 for the SRX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

(Encryption interface on M Series and T Series routers and EX Series switches only) Configure a certificate authority profile name.

Configure certification authority (CA) for X.509 certificate.

Options

- *profile-name*—Name of this CA configuration.
- **ca-name** ***name***—Name of the CA.
- **crl** ***filename***—Certificate revocation list (CRL) filename.
- **encoding**—Certificate encoding, either **binary** or **pem** (privacy-enhanced mail).
- **enrollment-url** ***url***—Enrollment URL.
- **file** ***filename***—Certificate filename.
- **ldap-url** ***url***—Lightweight Directory Access Protocol (LDAP) URL.

Required Privilege Level

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

Related Documentation

- *Configuring the Certificate Authority Properties for an ES PIC*
- *Configuring the Certificate Authority Properties for an ES PIC*

change-type

Syntax

```
change-type (character-sets | set-transitions);
```

Hierarchy Level

```
[edit system login password]
```

Release Information

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

Description

Set requirements for using character sets in plain-text passwords. When you combine this statement with the **minimum-changes** statement, you can check for the total number of character sets included in the password or for the total number of character-set changes in the password. Newly created passwords must meet these requirements.

Options

Specify one of the following:

- **character-sets**—The number of character sets in the password. Valid character sets include uppercase letters, lowercase letters, numbers, punctuation, and other special characters.
- **set-transitions**—The number of transitions between character sets.

Required Privilege Level

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

Related Documentation

- minimum-changes on page 1236

civic-based

Syntax

```
civic-based {
  what number;
  country-code code;
  ca-type {
    number {
      ca-value value;
    }
  }
}
```

Hierarchy Level

[edit protocols lldp-med interface (all | *interface-name*) location]

Release Information

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

Description

For Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED), configure the geographic location to be advertised from the switch to the MED. This information is used during emergency calls to identify the location of the MED.

The remaining statements are explained separately. See CLI Explorer.

Default

Disabled.

Required Privilege Level

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

Related Documentation

- show lldp on page 1826
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Configuring LLDP-MED (CLI Procedure) on page 521

ciphers

Syntax ciphers [*cipher-1 cipher-2 cipher-3* ...]

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 11.2.

Description Specify the set of ciphers the SSH server can use to perform encryption and decryption functions.

Options

- **3des-cbc**—Triple Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode.
- **aes128-cbc**—128-bit Advanced Encryption Standard (AES) in CBC mode.
- **aes128-ctr**—128-bit AES in counter mode.
- **aes128-gcm@openssh.com**—128-bit AES in Galois/Counter Mode.
- **aes192-cbc**—192-bit AES in CBC mode.
- **aes192-ctr**—192-bit AES in counter mode.
- **aes256-cbc**—256-bit AES in CBC mode.
- **aes256-ctr**—256-bit AES in counter mode.
- **aes256-gcm@openssh.com**—256-bit AES in Galois/Counter Mode.
- **arcfour**—128-bit RC4-stream cipher in CBC mode.
- **arcfour128**—128-bit RC4-stream cipher in CBC mode.
- **arcfour256**—256-bit RC4-stream cipher in CBC mode.
- **blowfish-cbc**—128-bit blowfish-symmetric block cipher in CBC mode.
- **cast128-cbc**—128-bit cast in CBC mode.
- chacha20-poly1305@openssh.com—ChaCha20 stream cipher and Poly1305 MAC

NOTE: Ciphers represent a set. To configure SSH ciphers use the set command as shown in the following example:

```
user@host#set system services ssh ciphers [ aes256-cbc aes192-cbc ]
```

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

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 232
- key-exchange on page 1185
- macs on page 1217

circuit-id (DHCP Relay Agent)

Syntax

```
circuit-id {
  include-irb-and-l2;
  keep-incoming-circuit-id ;
  no-vlan-interface-name;
  prefix prefix;
  use-interface-description (logical | device);
  use-vlan-id;
}
```

Hierarchy Level

[edit forwarding-options dhcp-relay relay-option-82],
[edit forwarding-options dhcp-relay group *group-name* relay-option-82],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay relay-option-82],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* relay-option-82],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay relay-option-82],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* relay-option-82],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay relay-option-82],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* relay-option-82]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.3 for EX Series switches.
include-irb-and-l2 , **no-vlan-interface-name**, and **use-vlan-id** options added in Junos OS Release 14.1.

Description

Specify the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82) to include in DHCP packets destined for a DHCP server. Optionally specify that the suboption includes a prefix, textual description, or VLAN tag.

NOTE: For Layer 3 interfaces, when you configure relay-option-82 only, the Agent Circuit ID is the default. If no VLAN tags are configured, then the default is the logical interface device (IFL) name. For integrated routing and bridging (IRB) interfaces, the default is the Layer 2 IFL name and bridge domain name.

The interface to bridge domain relationship may be implicit (the interface is mapped to the bridge domain by the system based on VLAN tag) or explicit (the interface is mapped to the bridge domain by configuring it in the bridge domain definition). For the explicit case, tagging might not be relevant for the mapping.

The format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces that do not use virtual LANs (VLANs), stacked VLANs (S-VLANs), or bridge domains is as follows:

```
(fe | ge)-fpc/pic/port.subunit
```

NOTE: For remote systems, the *subunit* is required and is used to differentiate an interface for remote systems.

The format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces that use VLANs is as follows:

```
(fe | ge)-fpc/pic/port:vlan-id
```

The format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs is as follows:

```
(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

In the case of an IRB interface, the format displays the Layer 2 interface instead of the IRB interface along with the bridge domain name. For IRB interfaces (or other pseudo devices) the default format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

  ```
  (fe | ge)-fpc/pic/port.subunit:bridge-domain-name
  ```

- IRB interfaces that use VLANs:

  ```
  (fe | ge)-fpc/pic/port.subunit:vlan-name
  ```

To include the IRB interface name with the Layer 2 interface name, configure the **include-irb-and-l2** statement. The format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

  ```
  (fe | ge)-fpc/pic/port:bridge-domain-name+irb.subunit
  ```

- IRB interfaces that use VLANs:

  ```
  (fe | ge)-fpc/pic/port:vlan-name+irb.subunit
  ```

To include only the IRB interface name without the Layer 2 interface and bridge domain or VLAN, configure the **no-vlan-interface-name** statement. The format is as follows:

```
irb.subunit
```

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

Related Documentation
- Using DHCP Relay Agent Option 82 Information on page 633
- *Configuring Option 82 Information*

circuit-type

Syntax
```
circuit-type;
```

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

Release Information
Statement introduced in Junos OS Release 9.1.

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

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

Related Documentation
- Using External AAA Authentication Services to Authenticate DHCP Clients on page 571

circuit-type (DHCP Local Server)

Syntax

```
circuit-type;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

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

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651

circuit-type (DHCP Relay Agent)

Syntax

```
circuit-type;
```

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name* authentication username-include],
[edit forwarding-options dhcp-relay group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay ...],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay ...],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Support at the **[edit ... dual-stack-group *dual-stack-group-name*]** hierarchy level introduced in Junos OS Release 15.1.

Description

Specify that the circuit type is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651
- Creating Unique Usernames for DHCP Clients on page 653

clear-on-abort (DHCP Local Server)

Syntax

```
clear-on-abort;
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group *group-name* reconfigure],
[edit system services dhcp-local-server dhcpv6 group *group-name* reconfigure]

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6 ...]** hierarchy levels introduced in Junos OS Release 10.4.

Description

Delete all DHCP clients or only the DHCP clients serviced by the specified group of interfaces when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success. A group configuration takes precedence over a DHCP local server configuration.

Default

Restores the original client configuration when reconfiguration fails.

Required Privilege Level

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

Related Documentation

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview on page 662

- Configuring Deletion of the Client When Dynamic Reconfiguration Fails on page 665

client-discover-match (DHCP Local Server)

Syntax

```
client-discover-match <option60-and-option82 | incoming-interface>;
```

Hierarchy Level

[edit system services dhcp-local-server overrides],
[edit system services dhcp-local-server group *group-name* overrides],
[edit system services dhcp-local-server group *group-name* interface *interface-name* overrides]
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server ... overrides],
[edit logical-systems *logical-system-name* system services dhcp-local-server ...overrides],
[edit routing-instances *routing-instance-name* system services dhcp-local-server ...overrides]

Release Information

Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
incoming-interface option added in Junos OS Release 13.3.

Description

Configure the match criteria DHCP local server uses to uniquely identify DHCP subscribers or clients when primary identification fails. The options are mutually exclusive.

Default

By default, DHCP uses the **option60-and-option82** option.

Options

incoming-interface—(Optional) Allow only one client device to connect on the interface. If the client device changes, the router deletes the existing client binding and creates a binding for the newly connected device.

NOTE: The **overrides client-discover-match incoming-interface** configuration deletes and replaces the existing binding when a new device connects. This action differs from the **overrides interface-client-limit 1** statement, which retains the existing binding and rejects the newly connected client.

option60-and-option82—(Optional) Use option 60 and option 82 information to identify subscribers.

Required Privilege Level

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

Related Documentation

- Extended DHCP Local Server Overview on page 562
- Overriding the Default DHCP Local Server Configuration Settings Overview on page 630
- DHCP Auto Logout Overview on page 643

- *Allowing Only One DHCP Client Per Interface*

client-id (DHCP Local Server)

Syntax

```
client-id;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the DHCPv6 Client-ID option (option 1) in the client PDU name is concatenated with the username during the subscriber authentication or client authentication process.

Required Privilege Level

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

Related Documentation

- Creating Unique Usernames for DHCP Clients on page 653

client-id (DHCP Relay Agent)

Syntax

```
client-id;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication
  username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay dhcpv6 ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the client ID is concatenated with the username during the subscriber authentication or client authentication process.

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651
- Creating Unique Usernames for DHCP Clients on page 653

class (Assigning a Class to an Individual User)

Syntax

```
class class-name;
```

Hierarchy Level

```
[edit system login user username]
```

Release Information

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

Description

Assign a user to a login class. You must assign each user to a login class.

Options

class-name—One of the classes defined at the **[edit system login class]** hierarchy level.

Required Privilege Level

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

Related Documentation

- Configuring Junos OS User Accounts by Using a Configuration Group on page 76

class (Defining Login Classes)

Syntax

```
class class-name {
  allow-commands "regular-expression";
  ( allow-configuration | allow-configuration-regexps) “regular expression 1” “regular
    expression 2”;
  cli {
    prompt name;
  }
  configuration-breadcrumbs;
  deny-commands "regular-expression";
  ( deny-configuration | deny-configuration-regexps )  “regular expression 1” “regular
    expression 2 ”;
  idle-timeout minutes;
  login-script filename;
  login-tip;
  no-scp-server;
  no-sftp-server;
  permissions [ permissions ];
}
```

Hierarchy Level

```
[edit system login]
```

Release Information

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

Description

Define a login class.

Options

class-name—A name you choose for the login class.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Defining Junos OS Login Classes on page 53
- user on page 1597

class (Defining Login Classes)

Syntax

```
class class-name {
  access-end;
  access-start;
  allow-commands "regular-expression";
  allow-configuration "regular-expression";
  deny-commands "regular-expression";
  deny-configuration "regular-expression";
  idle-timeout minutes;
  login-tip;
  permissions [ permissions ];
}
```

Hierarchy Level

```
[edit system login]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Define a login class.

Options

class-name—A name you choose for the login class.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Defining Junos OS Login Classes on page 53
- user on page 1596

class-usage-profile

Syntax

```
class-usage-profile profile-name {
  file filename;
  interval minutes;
  source-classes {
    source-class-name;
  }
  destination-classes {
    destination-class-name;
  }
}
```

Hierarchy Level

```
[edit accounting-options]
```

Release Information

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

Description

Create a class usage profile, which is used to log class usage statistics to a file in the **/var/log** directory. The class usage profile logs class usage statistics for the configured source classes on every interface that has **destination-class-usage** configured.

For information about configuring source classes, see the *Junos Routing Protocols Configuration Guide*. For information about configuring source class usage, see the *Junos Network Management Configuration Guide*.

Options

profile-name—Name of the destination class profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring Class Usage Profiles*

clients

Syntax

```
clients {
  address <restrict>;
}
```

Hierarchy Level

[edit snmp community *community-name*]

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Specify the IPv4 or IPv6 addresses of the SNMP client hosts that are authorized to use this community.

Default

If you omit the **clients** statement, all SNMP clients using this community string are authorized to access the router.

Options

address—Address of an SNMP client that is authorized to access this router. You must specify an address, not a hostname. To specify more than one client, include multiple ***address*** options.

restrict—(Optional) Do not allow the specified SNMP client to access the router.

Required Privilege Level

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

Related Documentation

- *Configuring SNMP Communities*

client-alive-count-max

Syntax client-alive-count-max*number*;

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 11.2.

Description Configure the number of client alive messages that can be sent without sshd receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. Client alive messages are sent through the encrypted channel. Use in conjunction with client-alive-interval to disconnect unresponsive SSH clients.

Default 3 messages

Options **Range:** 0 through 255

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

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 232

client-alive-interval

Syntax client-alive-interval *seconds*;

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 12.1.

Description Configure a timeout interval in seconds, after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. This option applies to SSH protocol version 2 only. Use in conjunction with client-alive-count-max to disconnect unresponsive SSH clients.

Default 0 seconds

Options **Range:** 1 through 65535

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

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 232

client-ia-type

Syntax

```
client-ia-type {
  ia-na;
  ia-pd;
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
[edit logical-systems logical -system-name interfaces interface-name unit logical-unit-number
  family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6
  dhcpv6-client]
```

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.
The **logical-systems** and **tenants** options are introduced in Junos OS Release 18.4R1.

Description

Configure the DHCPv6 client identity association type.

Options

ia-na— Identity association for nontemporary address

ia-pd—Identity association for prefix delegation

Required Privilege Level

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

Related Documentation

- DHCPv6 Client Overview on page 787

client-identifier (dhcp-client)

Syntax

```
client-identifier {
   user-id {ascii ascii hexadecimal hexadecimal;
   use-interface-description {logical |device};
   prefix [host-name routing-instance-name];
}
```

Hierarchy Level

[edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

Release Information

Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option **dhcp-clinet** at **[edit interfaces interface-name unit logical-unit-number family inet]** hierarchy is changed to **dhcp** to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option **dhcp**.

Description

The DHCP server identifies a client by a client-identifier value.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- DHCPv6 Client Overview on page 787

client-identifier (dhcpv6-client)

Syntax

```
client-identifier duid-type (duid-ll | duid-llt | vendor);
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical -system-name interfaces interface-name unit logical-unit-number
  family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6
  dhcpv6-client]
```

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.
The **logical-systems** and **tenants** options are introduced in Junos OS Release 18.4R1.

Description

The DHCPv6 server identifies a client by a client-identifier value.

Options

duid-type—The DHCPv6 client is identified by a DHCP unique identifier (DUID).

duid-ll—Link Layer address.

duid-llt—Link Layer address plus time.

vendor—Vendor-assigned unique ID based on the enterprise number.

Required Privilege Level

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

Related Documentation

- DHCPv6 Client Overview on page 787

client-list-name

Syntax client-list-name *client-list-name*;

Hierarchy Level [edit snmp community *community-name*]

Release Information Statement introduced in Junos OS Release 8.5 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Add a client list or prefix list to an SNMP community.

Options ***client-list-name***—Name of the client list or prefix list.

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

Related Documentation
- *Adding a Group of Clients to an SNMP Community*

client-list-name (SNMP)

Syntax client-list-name *client-list-name* ;

Hierarchy Level [edit snmp community *community-name*]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the name of the list of SNMP network management system (NSM) clients that are authorized to collect information about network operations. You cannot use an SNMP client list and individually configured SNMP clients in the same configuration.

Options ***client-list-name*** — Name of the client list. Client list is the list of IP address prefixes defined with the **prefix-list** statement in the policy-options hierarchy.

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

client-type

Syntax

```
client-type (autoconfig | stateful);
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
[edit logical-systems logical -system-name interfaces interface-name unit logical-unit-number
  family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6
  dhcpv6-client]
```

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.
The **logical-systems** and **tenants** options are introduced in Junos OS Release 18.4R1.

Description

The type of DHCPv6 client.

Options

- autoconfig—Autoconfig client type for router advertisement
- stateful— Stateful client type for address assignment

Required Privilege Level

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

Related Documentation

- DHCPv6 Client Overview on page 787

commit-delay

Syntax commit-delay *seconds*;

Hierarchy Level [edit snmp nonvolatile]

Release Information Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series switches.

Description Configure the timer for the SNMP **Set** reply and start of the commit.

Options ***seconds***—Delay between an affirmative SNMP **Set** reply and start of the commit.
Default: 5 seconds

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

Related Documentation
- *Configuring the Commit Delay Timer*

community (SNMP)

Syntax

```
community community-name {
  authorization authorization;
  client-list-name client-list-name;
  clients {
    address restrict;
  }
  view view-name;
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Define an SNMP community. An SNMP community authorizes SNMP clients based on the source IP address of incoming SNMP request packets. A community also defines which MIB objects are available and the operations (read-only or read-write) allowed on those objects.

NOTE: The **authorization read-write** option is not supported on the QFX3000 QFabric system.

The SNMP client application specifies an SNMP community name in **Get**, **GetBulk**, **GetNext**, and **Set** SNMP requests.

Default

If you omit the **community** statement, all SNMP requests are denied.

Options

community-name—Community string. If the name includes spaces, enclose it in quotation marks (" ").

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring SNMP Communities*
- *Configuring the SNMP Community String*

connection-limit

Syntax

```
connection-limit limit;
```

Hierarchy Level

```
[edit system services finger],
[edit system services ftp],
[edit system services netconf ssh],
[edit system services ssh],
[edit system services telnet],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Configure the maximum number of connections sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).

Options

limit—(Optional) Maximum number of established connections per protocol (either IPv6 or IPv4).

Range: 1 through 250

Default: 75

NOTE: The actual number of maximum connections depends on the availability of system resources, and might be fewer than the configured connection-limit value if the system resources are limited.

Required Privilege Level

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

Related Documentation

- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*
- *Configuring DTCP-over-SSH Service for the Flow-Tap Application*
- Configuring Finger Service for Remote Access to the Router on page 231
- Configuring FTP Service for Remote Access to the Router or Switch on page 231
- Configuring SSH Service for Remote Access to the Router or Switch on page 232
- Configuring Telnet Service for Remote Access to a Router or Switch on page 230

connection-limit

Syntax connection-limit *limit;*

Hierarchy Level
[edit system services finger]
[edit system services ftp]
[edit system services netconf ssh]
[edit system services ssh]
[edit system services telnet]
[edit system services xnm-clear-text]
[edit system services xnm-ssl]

Release Information Statement introduced in Junos OS Release 11.4.

Description Configure the maximum number of connection sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).

Options *limit*—Maximum number of established connections per protocol (either IPv6 or IPv4).

Range: 1 through 250

Default: 75

NOTE: The actual number of maximum connections depends on the availability of system resources, and might be fewer than the configured connection-limit value if the system resources are limited.

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

contact (SNMP)

Syntax

```
contact contact;
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Define the value of the MIB II **sysContact** object, which is the contact person for the managed system.

Options

contact—Name of the contact person. If the name includes spaces, enclose it in quotation marks (" ").

Required Privilege Level

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

Related Documentation

- *Configuring the System Contact on a Device Running Junos OS*

counters

Syntax

```
counters {
  counter-name;
}
```

Hierarchy Level

[edit accounting-options filter-profile *profile-name*]

Release Information

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

Description

Names of counters for which filter profile statistics are collected. The packet and byte counts for the counters are logged to a file in the **/var/log** directory.

Options

counter-name—Name of the counter.

Required Privilege Level

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

Related Documentation

- *Configuring the Counters*

country-code

Syntax

```
country-code code;
```

Hierarchy Level

```
[edit protocols lldp-med interface (all | interface-name)]
```

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

Description For Link Layer Discovery Protocol–Media Endpoint Device (LLDP-MED), configure the two-letter country code to include in the location information. Location information is advertised from the switch to the MED, and is used during emergency calls to identify the location of the MED. The country code is required when configuring LLDP-MED based on location.

Default Disabled.

Options ***code***—Two-letter ISO 3166 country code in capital ASCII letters; for example, US or DE.

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

Related Documentation

- show lldp on page 1826
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Configuring LLDP-MED (CLI Procedure) on page 521

crl (Encryption Interface)

Syntax

```
crl file-name;
```

Hierarchy Level

```
[edit security certificates]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.

Options

file-name—Specify the file from which to read the CRL.

Required Privilege Level

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

Related Documentation

- *Configuring the Certificate Authority Properties for an ES PIC*

custom-options

Syntax

```
custom-options {
  banner-message string;
  footer-bgcolor color;
  footer-message string;
  footer-text-color color;
  form-header-bgcolor color;
  form-header-message string;
  form-header-text-color color;
  form-reset-label label name;
  form-submit-label label name;
  header-bgcolor color;
  header-logo filename;
  header-message string;
  header-text-color color;
  post-authentication-url url-string;
}
```

Hierarchy Level [edit services captive-portal]

Release Information Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description Specify the design elements of a captive portal login page.

Options

banner-message—The first screen displayed before the captive portal login page is displayed—for example, a disclaimer message.

Range: 1–2047 characters

footer-bgcolor —The hexadecimal color code for the color of the footer bar across the bottom of the captive portal login page—for example, #2E8B57 (sea green).

Values: # symbol followed by six characters.

footer-message—Text message displayed in the footer bar across the bottom of the captive portal login page.

Range: 1–2047 characters

Default: Copyright @2010, Juniper Networks Inc.

footer-text-color — Color of the text in the footer.

Default: The default color is white.

form-header-bgcolor —The hexadecimal color code for the background color of the header bar across the top of the form area of the captive portal login page.

Values: # symbol followed by six characters.

form-header-message—Text message displayed in the header bar across the top of the form area of the captive portal login page.

Range: 1–255 characters

Default: Captive Portal User Authentication

form-header-text-color—Color of the text in the form header.

Default: The default color is black.

form-reset-label—Label displayed in the button that the user can select to clear the username and password fields on the form.

Range: 1–255 characters

Default: Reset

form-submit-label —Label displayed in the button that the user selects to submit their login information—for example, **Log In** .

Range: 1–255 characters

Default: Log In

header-bgcolor—The hexadecimal color code for the color of the header bar across the top of the captive portal login page.

Values: # symbol followed by six characters.

header-logo—Filename of the file containing the image of the logo displayed at the top of the captive portal login page. The image file can be in GIF, JPEG, or PNG format.

Default: The Juniper Networks logo

header-message—Text displayed in the header bar across the bottom of the captive portal login page.

Range: 1–2047 characters

Default: User Authentication

header-text-color—Color of the text in the header.

Default: The default color is white.

post-authentication-url—URL to which the users are directed upon successful authentication—for example **www.mycafe.com**.

Range: 1–255 characters

Default: The page originally requested by the user.

Required Privilege Level

routing—To view this statement in the configuration.
routing–control—To add this statement to the configuration.

Related Documentation

- Designing a Captive Portal Authentication Login Page on Switches on page 380
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

delegated-pool (DHCP Local Server)

Syntax

```
delegated-pool pool-name;
```

Hierarchy Level

```
[edit system services dhcp-local-server dhcpv6 overrides],
[edit system services dhcp-local-server dhcpv6 group group-name overrides],
[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name
  overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
  services dhcp-local-server dhcpv6 ...],
[edit logical-systems logical-system-name system services system services dhcp-local-server
  dhcpv6 ...],
[edit routing-instances routing-instance-name system services system services
  dhcp-local-server dhcpv6 ...]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the address pool that assigns the IA_PD address. A pool specified by RADIUS VSA 26-161 takes precedence over the pool specified by this **delegated-pool** statement.

Options

pool-name—Name of the address-assignment pool.

Required Privilege Level

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

Related Documentation

- *Specifying the Delegated Address-Assignment Pool to Be Used for DHCPv6 Prefix Delegation*
- Overriding the Default DHCP Local Server Configuration Settings Overview on page 630

delimiter (DHCP Local Server)

Syntax

delimiter *delimiter-character*;

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the character used as the delimiter between the concatenated components of the username.

Options

delimiter-character—Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.

Default: . (period)

NOTE: When you include the *interface-description* in the username, the delimiter must not be a character that is part of the interface description. For example, if the text description is configured as “Backbone connection/PHL01”, you cannot use the forward slash (/) as the delimiter.

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651

delimiter (DHCP Relay Agent)

Syntax

delimiter *delimiter-character*;

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name* authentication username-include],
[edit forwarding-options dhcp-relay group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* authentication username-include]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Support at the **[edit ... dual-stack-group *dual-stack-group-name*]** hierarchy level introduced in Junos OS Release 15.1.

Description

Specify the character used as the delimiter between the concatenated components of the username. Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

Options

delimiter-character—Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.

Default: . (period)

NOTE: When you include the *interface-description* in the username, the delimiter must not be a character that is part of the interface description. For example, if the text description is configured as “Backbone connection/PHL01”, you cannot use the forward slash (/) as the delimiter.

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651
- Creating Unique Usernames for DHCP Clients on page 653

deny-commands

Syntax deny-commands *"(regular-expression)|(regular-expression1)|(regulare-expression2)..."*;

Hierarchy Level [edit system login class]

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 operational mode commands that the user is denied permission to issue even though the permissions set with the **permissions** statement would allow it.

When specifying extended regular expressions using the **allow/deny-commands** and **allow/deny-configuration** statements, each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses ( ). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.

Default If you omit this statement and the **allow-commands** statement, users can issue only those commands for which they have access privileges through the **permissions** statement.

Options *regular-expression*—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

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

Related Documentation

- Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 112
- allow-commands on page 863
- user on page 1597

deny-commands-regexps

Syntax deny-commands-regexps *["regular expression 1" "regular expression 2" ....]*;

Hierarchy Level [edit system login class *class-name*]

Release Information Statement introduced in Junos OS Release 18.1.

Description Configure authorizations for operational mode commands using regular expressions. You can use the **deny-commands-regexps** statement to explicitly deny authorization for commands that would otherwise be permitted by an access privilege level.

For **allow/deny-commands-regexps** statements, you configure a set of strings in which each string is a regular expression, enclosed in double quotes and separated with a space operator. Each string is evaluated against the full path of the command, which provides faster matching than the **allow/deny-command** statements. You can also include values for variables in the regular expressions, which is not supported using **allow/deny-commands**.

Expressions configured with this statement take precedence over **allow-commands-regexps** if the two statements are used in the same login class definition.

NOTE: The **allow/deny-commands** and **allow/deny-commands-regexps** statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the **allow/deny-commands** statement, or the **allow/deny-commands-regexps** statement. If you have existing configurations using the **allow/deny-commands** statements, using the same configuration options with the **allow/deny-commands-regexps** statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

Authorizations can also be configured remotely by specifying Juniper Networks vendor-specific TACACS+ attributes in your authentication server's configuration. For a remote user, when the authorization parameters are configured both remotely and locally, authorization parameters configured remotely and locally are both considered together for authorization. For a local user, only the authorization parameters configured locally for the class are considered.

Default If you do not configure authorizations for operational mode commands using **allow/deny-commands** or **allow/deny-commands-regexps**, users can edit only those commands for which they have access privileges set with the **permissions** statement.

Options

regular expression—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Enter as many expressions as needed.

Required Privilege Level

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

Related Documentation

- Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies on page 125
- allow-commands-regexps on page 864

deny-configuration

Syntax deny-configuration *"(regular-expression)|(regular-expression1)|(regulare-expression2)..."*;

Hierarchy Level [edit system login class]

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

Description Explicitly deny configuration access to the specified levels in the hierarchy even if the permissions set with the **permissions** statement grant such access by default. Note that the user cannot view a particular hierarchy if configuration access is denied for that hierarchy.

When specifying extended regular expressions using the **allow/deny-commands** and **allow/deny-configuration** statements, each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses ( ). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.

NOTE: The **allow/deny-configuration** and **allow/deny-configuration-regexps** statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the **allow/deny-configuration** statement, or the **allow/deny-configuration-regexps** statement. If you have existing configurations using the **allow/deny-configuration** statements, using the same configuration options with the **allow/deny-configuration-regexps** statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

Default If you omit this statement and the **allow-configuration** statement, users can edit those levels in the configuration hierarchy for which they have access privileges through the **permissions** statement.

Options *regular-expression*—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

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

Related Documentation

- Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 112
- allow-configuration on page 866
- user on page 1597

deny-configuration

Syntax

```
deny-configuration "regular-expression";
```

Hierarchy Level

```
[edit system login class]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.2 for SRX Series devices.

Description

Explicitly deny configuration access to the specified levels in the hierarchy even if the permissions set with the **permissions** statement grant such access by default.

Default

If you omit this statement and the **allow-configuration** statement, users can edit those levels in the configuration hierarchy for which they have access privileges through the **permissions** statement.

Options

regular-expression—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

Required Privilege Level

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

deny-configuration-regexps

Syntax deny-configuration-regexps *["regular expression 1" "regular expression 2" ....]*;

Hierarchy Level [edit system login class *class-name*]

Release Information Statement introduced in Junos OS Release 11.2.

Description Explicitly deny configuration access to specified hierarchies using regular expressions even if the permissions set with the **permissions** statement allow that access.

Expressions configured with this statement take precedence over **allow-configuration-regexps** if the two statements are used in the same login class definition.

NOTE: The allow/deny-configuration and allow/deny-configuration-regexps statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the allow/deny-configuration statement, or the allow/deny-configuration-regexps statement. If you have existing configurations using the allow/deny-configuration statements, using the same configuration options with the allow/deny-configuration-regexps statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

Default If you do not configure this statement or the **deny-configuration-regexps** statement, users can edit only those commands for which they have access privileges set with the **permissions** statement.

Options *regular expression*—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Enter as many expressions as needed.

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

Related Documentation

- Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies on page 125
- allow-configuration-regexps on page 869
- user on page 1597

deny-configuration-regexps

Syntax deny-configuration-regexps "*regular expression 1*" "*regular expression 2*";

Hierarchy Level [edit system login **class** *class-name*]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.2 for SRX Series devices.

Description Explicitly deny configuration access to specified hierarchies using regular expressions even if the permissions set with the **permissions** statement allow that access.

Expressions configured with this statement take precedence over **allow-configuration-regexps** if the two statements are used in the same login class definition.

Default If you do not configure this statement or the **deny-configuration-regexps** statement, users can edit only those commands for which they have access privileges set with the **permissions** statement.

Options *regular expression*—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

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

destination (RADSEC)

Syntax

```
destination id-number {
  address ip-address;
  max-tx-buffers number;
}
```

Hierarchy Level

[edit access radsec]

Release Information

Statement introduced in Junos OS Release 19.1R1.

Description

Define the RADSEC server as a destination for RADIUS traffic. Traffic that is destined for a RADIUS server can then be redirected to the RADSEC destination. RADSEC destinations are identified by a unique numeric ID. You can configure multiple RADSEC destinations with different parameters pointing to the same RADSEC server.

Options

id-number—Globally unique ID number for the RADSEC destination.

address *ip-address*—IP address of the RADSEC server.

max-tx-buffers *number*—Maximum number of packets buffered on transmission.

NOTE: The buffer allocation should be able to accommodate the **max-outstanding-requests** for mapped RADIUS servers configured at the **[edit access radius-server]** hierarchy level.

Range: 32 through 32000

Default: 100

Required Privilege Level

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

Related Documentation

- RADIUS over TLS (RADSEC) on page 203

destination (Accounting)

Syntax

```
destination {
  radius {
    server {
      server-address {
        accounting-port port-number;
        retry number;
        routing-instance (Accounting and Authentication) routing-instance;
        secret password;
        source-address address;
        source-address-inet6 IPv6-source-address;
        timeout seconds;
      }
    }
  }
  tacplus {
    server {
      server-address {
        port port-number;
        routing-instance (Accounting and Authentication) routing-instance;
        secret password;
        single-connection;
        timeout seconds;
      }
    }
  }
}
```

Hierarchy Level

```
[edit system accounting]
```

Release Information

Statement introduced before Junos OS Release 7.4.
radius statement added in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the authentication server.

Options

source-address-inet6 ***IPv6-source-address***—A valid IPv6 address configured on one of the routers or switch interfaces.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring RADIUS System Accounting on page 200
- Configuring TACACS+ System Accounting on page 219

destination (Accounting)

Syntax

```
destination {
  radius {
    server {
      server-address {
        accounting-port port-number;
        max-outstanding-requests value;
        port port-number;
        retry value;
        secret password;
        source-address source-address;
        timeout seconds;
      }
    }
  }
  tacplus {
    server {
      server-address {
        port port-number;
        secret password;
        single-connection;
        timeout seconds;
      }
    }
  }
}
```

Hierarchy Level

```
[edit system accounting]
```

Release Information

Statement introduced before Junos OS Release 7.4.
radius statement added in Junos OS Release 7.4. Support for IPv6 source address added in Junos OS Release 12.1X47-D15 for SRX1500, SRX5400, SRX5600, and SRX5800 devices.

Description

Configure the authentication server.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

destination (Accounting)

Syntax

```
destination {
  radius {
    server {
      server-address {
        accounting-port port-number;
        retry number;
        routing-instance (Accounting and Authentication) routing-instance;
        secret password;
        source-address address;
        source-address-inet6 IPv6-source-address;
        timeout seconds;
      }
    }
  }
  tacplus {
    server {
      server-address {
        port port-number;
        routing-instance (Accounting and Authentication) routing-instance;
        secret password;
        single-connection;
        timeout seconds;
      }
    }
  }
}
```

Hierarchy Level

```
[edit system accounting]
```

Release Information

Statement introduced before Junos OS Release 7.4.
radius statement added in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the authentication server.

Options

source-address-inet6 ***IPv6-source-address***—A valid IPv6 address configured on one of the routers or switch interfaces.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring RADIUS System Accounting on page 200
- Configuring TACACS+ System Accounting on page 219

destination-classes

Syntax

```
destination-classes {
  destination-class-name;
}
```

Hierarchy Level

[edit accounting-options class-usage-profile *profile-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 15.1F6 for PTX Series routers with third-generation FPCs installed.

Description

Specify the destination classes for which statistics are collected.

Options

destination-class-name—Name of the destination class to include in the source class usage profile.

Required Privilege Level

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

Related Documentation

- *Configuring a Class Usage Profile*

detection-time

Syntax

```
detection-time {
  threshold milliseconds;
}
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options
  dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method
  bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method
  bfd]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Enable failure detection. The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. For example, the timers can adapt to a higher value if the adjacency fails, or a neighbor can negotiate a higher value for a timer than the one configured.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677

destination-host (Gx-Plus)

Syntax destination-host *hostname*;

Hierarchy Level [edit access gx-plus partition *partition-name*]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure the host on which the PCRF application resides.

Options ***hostname***—Host on which the PCRF is installed.

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

Related Documentation
- *Configuring Gx-Plus*
- *Configuring the Gx-Plus Partition*

destination-realm (Gx-Plus)

Syntax destination-realm *realm*;

Hierarchy Level [edit access gx-plus partition *partition-name*]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure the realm in which the PCRF host resides.

Options ***realm***—Realm in which the PCRF host resides.

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

Related Documentation
- *Configuring Gx-Plus*
- *Configuring the Gx-Plus Partition*

dhcp

Syntax

```
dhcp {
  boot-file filename;
  boot-server (address | hostname);
  default-lease-time seconds;
  domain-name domain-name;
  domain-search [domain-list];
  maximum-lease-time seconds;
  name-server {
    address;
  }
  next-servernext-server
  option option-identifier-code ;
  pool address/prefix-length {
    address-range {
      low address;
      high address;
    }
    exclude-address {
      address;
    }
  }
  router {
    address;
  }
  static-binding mac-address {
    fixed-address {
      address;
    }
    host-name hostname;
    client-identifier (ascii client-id | hexadecimal client-id);
  }
  wins-server {
    address;
  }
}
```

Hierarchy Level

```
[edit system services]
[edit logical-systems logical -system-name system services]
```

Release Information

Statement introduced before Junos OS Release 7.4.
The **logical-systems** option is introduced in Junos OS Release 18.4R1.

Description

Configure a router, or a switch as a DHCP server. A DHCP server can allocate network addresses and deliver configuration information to client hosts on a TCP/IP network.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *System Management Configuration Statements*
- Example: Complete DHCP Server Configuration on page 554

dhcp (DHCP Client)

Syntax

```
dhcp {
  client-identifier duid-type (duid-ll | duid-llt | vendor);
  no-dns-install;
  rapid-commit;
  options name;
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet]
[edit logical-systems name interfaces interface-name unit logical-unit-number family inet]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
The **logical-systems** and **tenants** options are introduced in Junos OS Release 18.4R1.

Description

Configure a Dynamic Host Configuration Protocol (DHCP) client for an IPv4 interface for logical systems and tenant systems.

The remaining statements are described separately.

NOTE: Starting in Junos OS Release 18.1R1, DHCPv4 and DHCPv6 clients are supported on management interfaces (fxp0 and em0) configured in the non-default management routing instance, mgmt_junos.

Options

client-identifier duid-type—Identify a client by a client-identifier value. This statement is mandatory.

no-dns-install—Configure the DHCPv6 client DNS information.

options—Specify options requested by the DHCPv4 client.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring a DHCP Client (CLI Procedure) on page 591

dhcp-client

Syntax

```
dhcp-client {
  client-identifier {
    prefix {
      host-name;
      logical-system-name;
      routing-instance-name;
    }
    use-interface-description (device | logical);
    user-id (ascii string| hexadecimal string);
  }
  force-discover;
  lease-time (length | infinite);
  no-dns-install;
  options no-hostname;
  retransmission-attempt value;
  retransmission-interval seconds;
  server-address server-address;
  update-server;
  vendor-id vendor-id ;
}
```

Hierarchy Level

[edit interfaces *interface-name* unit *logical-unit-number* family *family*]

Release Information

Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Starting with Junos OS Release 17.4R1 and Junos OS Release 15.1X49-D60, on all SRX Series devices and vSRX instances, the CLI option **dhcp-client** at **[edit interfaces interface-name unit logical-unit-number family inet]** hierarchy is changed to **dhcp** to align with other Junos platforms. There is no change in the functionality.

Description

Configure the Dynamic Host Configuration Protocol (DHCP) client.

Options

- **force-discover**—Forces the DHCP client to send a DHCP discover packet after one to three failed **dhcp-request** attempts. The **force-discover** option ensures that the DHCP server will assign the same or a new IP address to the client.
- **lease-time**—Specify the time to negotiate and exchange DHCP information.
  - **infinite**—Lease never expires.
  - **length**—Number of seconds.
- **no-dns-install**—Do not add DNS information to the DHCP client (resolve.conf) even after learn from DHCP server
- **retransmission-attempt**—Specify the number of times the device attempts to retransmit a DHCP packet fallback. Range is 0-6.
- **server-address**—Specify the preferred DHCP server address that is sent to DHCP clients.

- **update-server**—Propagate TCP/IP settings to a local DHCP server.
- **vendor-id**—Vendor class ID for the DHCP client.

Required Privilege Level

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*

dhcp-local-server

Syntax

```
dhcp-local-server {
  access-profile profile-name;
  allow-active-leasequery {
    idle-timeout seconds;
    peer-address address;
    timeout seconds;
  }
  allow-bulk-leasequery {
    max-connections number-of-connections;
    max-empty-replies number-of-replies;
    restricted-requestor;
    timeout seconds;
  }
  allow-leasequery {
    restricted-requestor;
  }
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-description  (device-interface | logical-interface);
      interface-name;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      routing-instance-name;
      user-prefix user-prefix-string;
      vlan-tags;
    }
  }
  dhcpv6 {
    access-profile profile-name;
    allow-active-leasequery {
      idle-timeout seconds;
      peer-address address;
      timeout seconds;
    }
    allow-bulk-leasequery {
      max-connections number-of-connections;
      max-empty-replies number-of-replies;
      restricted-requestor;
      timeout seconds;
    }
    allow-leasequery {
      restricted-requestor;
    }
    authentication {
      ...
```

```
}
duplicate-clients incoming-interface;
group group-name {
  access-profile profile-name;
  authentication {
    ...
  }
  interface interface-name {
    access-profile profile-name;
    exclude;
    overrides {
      asymmetric-lease-time seconds;
      asymmetric-prefix-lease-time seconds;
      delay-advertise {
        based-on (option-15 | option-16 | option-18 | option-37) {
          equals {
            ascii ascii-string;
            hexadecimal hexadecimal-string;
          }
          not-equals {
            ascii ascii-string;
            hexadecimal hexadecimal-string;
          }
          starts-with {
            ascii ascii-string;
            hexadecimal hexadecimal-string;
          }
        }
        delay-time seconds;
      }
      dual-stack dual-stack-group-name;
      interface-client-limit number;
      multi-address-embedded-option-response;
      process-inform {
        pool pool-name;
      }
      protocol-attributes attribute-set-name;
      rapid-commit;
    }
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    trace;
    upto upto-interface-name;
  }
  liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
      bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
```

```
            threshold milliseconds;
          }
          detection-time {
            threshold milliseconds;
          }
          session-mode (automatic | multihop | singlehop);
          holddown-interval milliseconds;
        }
        layer2-liveness-detection {
          max-consecutive-retries number;
          transmit-interval interval;
        }
      }
    }
    overrides {
      asymmetric-lease-time seconds;
      asymmetric-prefix-lease-time seconds;
      delay-advertise {
        based-on (option-15 | option-16 | option-18 | option-37) {
          equals {
            ascii ascii-string;
            hexadecimal hexadecimal-string;
          }
          not-equals {
            ascii ascii-string;
            hexadecimal hexadecimal-string;
          }
          starts-with {
            ascii ascii-string;
            hexadecimal hexadecimal-string;
          }
        }
        delay-time seconds;
      }
      delegated-pool;
      dual-stack dual-stack-group-name;
      interface-client-limit number;
      multi-address-embedded-option-response;
      process-inform {
        pool pool-name;
      }
      protocol-attributes attribute-set-name;
      rapid-commit;
    }
    route-suppression;
    server-duid-type type;
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
  }
  liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
      bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
```

```
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        detection-time {
          threshold milliseconds;
        }
        session-mode (automatic | multihop | singlehop);
        holddown-interval milliseconds;
      }
      layer2-liveness-detection {
        max-consecutive-retries number;
        transmit-interval interval;
      }
    }
  }
  overrides {
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    delay-advertise {
      based-on (option-15 | option-16 | option-18 | option-37) {
        equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        not-equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        starts-with {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
      }
      delay-time seconds;
    }
    delegated-pool;
    dual-stack dual-stack-group-name;
    include-option-82 {
      forcerenew;
      nak;
    }
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
      pool pool-name;
    }
    protocol-attributes attribute-set-name;
    rapid-commit;
  }
  reconfigure {
    attempts attempt-count;
```

```
      clear-on-abort;
      strict;
      support-option-pd-exclude;
      timeout timeout-value;
      token token-value;
      trigger {
        radius-disconnect;
      }
    }
    reauthenticate (<lease-renewal> <remote-id-mismatch >);
    requested-ip-network-match subnet-mask;
    route-suppression;
    server-duid-type type;
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
dual-stack-group name {
    access-profile access-profile;
    authentication {
      password password-string;
      username-include {
        circuit-type;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-description  (device-interface | logical-interface);
        interface-name;
        logical-system-name;
        mac-address;
        relay-agent-interface-id;
        relay-agent-remote-id;
        routing-instance-name;
        user-prefix user-prefix-string;
        vlan-tags;
      }
    }
    classification-key {
      circuit-id circuit-id;
      mac-address mac-address;
      remote-id remote-id;
    }
    dual-stack-interface-client-limit number;
    dynamic-profile profile-name {
      aggregate-clients (merge | replace);
      use-primary primary-profile-name;
    }
    liveness-detection {
      failure-action (clear-binding | clear-binding-if-interface-up | log-only);
      method {
        layer2-liveness-detection {
          max-consecutive-retries number;
          transmit-interval interval;
        }
      }
    }
    on-demand-address-allocation;
```

```
    protocol-master (inet | inet6);
    reauthenticate (<lease-renewal> <remote-id-mismatch >);
    service-profile service-profile;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
  }
  duplicate-clients-in-subnet (incoming-interface | option-82);
  dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
    primary-profile-name>;
  forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
  group group-name {
    authentication {
      ...
    }
    dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
      primary-profile-name>;
    interface interface-name {
      exclude;
      overrides {
        asymmetric-lease-time seconds;
        client-discover-match (option60-and-option82 | incoming-interface);
        delay-offer {
          based-on (option-60 | option-77 | option-82) {
            equals {
              ascii ascii-string;
              hexadecimal hexadecimal-string;
            }
            not-equals {
              ascii ascii-string;
              hexadecimal hexadecimal-string;
            }
            starts-with {
              ascii ascii-string;
              hexadecimal hexadecimal-string;
            }
          }
          delay-time seconds;
        }
        include-option-82 {
          forcerenew;
          nak;
        }
        dual-stack dual-stack-group-name;
        interface-client-limit number;
        process-inform {
          pool pool-name;
        }
        protocol-attributes attribute-set-name;
      }
      service-profile dynamic-profile-name;
      short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
      trace;
      upto upto-interface-name;
    }
    liveness-detection {
```

```
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
      bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        detection-time {
          threshold milliseconds;
        }
        session-mode(automatic | multihop | singlehop);
        holddown-interval milliseconds;
      }
      layer2-liveness-detection {
        max-consecutive-retries number;
        transmit-interval interval;
      }
    }
  }
  overrides {
    asymmetric-lease-time seconds;
    client-discover-match (option60-and-option82 | incoming-interface);
    delay-offer {
      based-on (option-60 | option-77 | option-82) {
        equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        not-equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        starts-with {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
      }
      delay-time seconds;
    }
    include-option-82 {
      forcerenew;
      nak;
    }
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    protocol-attributes attribute-set-name;
  }
```

```
    requested-ip-network-match subnet-mask
    route-suppression;
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
        layer2-liveness-detection {
            max-consecutive-retries number;
            transmit-interval interval;
        }
    }
}
on-demand-address-allocation;
overrides {
    asymmetric-lease-time seconds;
    client-discover-match <option60-and-option82 | incoming-interface>;
    delay-offer {
        based-on (option-60 | option-77 | option-82) {
            equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            not-equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            starts-with {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
        }
        delay-time seconds;
    }
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
```

```
    }
    protocol-attributes attribute-set-name;
  }
  pool-match-order {
    external-authority;
    ip-address-first;
    option-82;
  }
  protocol-master;
  reauthenticate (<lease-renewal> <remote-id-mismatch >);
  reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
      radius-disconnect;
    }
  }
  requested-ip-network-match subnet-mask;
  route-suppression;
  service-profile dynamic-profile-name;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
  services],
[edit logical-systems logical-system-name system services],
[edit routing-instances routing-instance-name system services],
[edit system services]
```

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 13.2X51 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure Dynamic Host Configuration Protocol (DHCP) local server options on the router or switch to enable the router or switch to function as an extended DHCP local server. The DHCP local server receives DHCP request and reply packets from DHCP clients and then responds with an IP address and other optional configuration information to the client.

The extended DHCP local server is incompatible with the DHCP server on J Series routers and, therefore, is not supported on J Series routers. Also, the DHCP local server and the DHCP/BOOTP relay server, which are configured under the **[edit forwarding-options helpers]** hierarchy level, cannot both be enabled on the router or switch at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.

The **dhcpv6** stanza configures the router or switch to support Dynamic Host Configuration Protocol for IPv6 (DHCPv6). The DHCPv6 local server is fully compatible with the extended DHCP local server and the extended DHCP relay feature.

NOTE: **When you configure the dhcp-local-server statement at the routing instance hierarchy level, you must use a routing instance type of virtual-router.**

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

Related Documentation

- Extended DHCP Local Server Overview on page 562
- DHCPv6 Local Server Overview on page 613

dhcp-relay

Syntax

```
dhcp-relay {
  access-profile profile-name;
  active-leasequery {
    idle-timeout seconds;
    peer-address address;
    timeout seconds;
    topology-discovery;
  }
  active-server-group server-group-name;
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-description  (device-interface | logical-interface);
      interface-name;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      routing-instance-name;
      user-prefix user-prefix-string;
      vlan-tags;
    }
  }
  bulk-leasequery {
    attempts number-of-attempts;
    timeout seconds;
  }
  dhcpv6 {
    access-profile profile-name;
    active-leasequery {
      idle-timeout seconds;
      peer-address address;
      timeout seconds;
      topology-discovery;
    }
    active-server-group server-group-name;
    }
    authentication {
      password password-string;
      username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-description  (device-interface | logical-interface);
        interface-name interface-name;
        logical-system-name;
        mac-address mac-address;
```

```
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
      vlan-tags;
    }
  }
  bulk-leasequery {
    attempts number-of-attempts;
    timeout seconds;
    trigger automatic;
  }
  duplicate-clients incoming-interface;
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
  }
  forward-only {
    logical-system <current | default | logical-system-name>;
    routing-instance <current | default | routing-instance-name>;
  }
  forward-only-replies;
  }
  forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
  group group-name {
    access-profile profile-name;
    active-server-group server-group-name;
    authentication {
      password password-string;
      username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-description  (device-interface | logical-interface);
        interface-name interface-name;
        logical-system-name;
        mac-address mac-address;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
        vlan-tags;
      }
    }
    dynamic-profile profile-name {
      aggregate-clients (merge | replace);
      use-primary primary-profile-name;
    }
    forward-only {
      logical-system <current | default | logical-system-name>;
      routing-instance <current | default | routing-instance-name>;
```

```
    }
    interface interface-name {
      access-profile profile-name;
      dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
      }
      exclude;
      overrides {
        allow-snooped-clients;
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-negotiation-match incoming-interface;
        delay-authentication;
        delete-binding-on-renegotiation;
        dual-stack dual-stack-group-name;
        interface-client-limit number;
        no-allow-snooped-clients;
        no-bind-on-request;
        relay-source interface-name;
        send-release-on-delete;
      }
      service-profile dynamic-profile-name;
      short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
      trace;
      upto upto-interface-name;
    }
    }
    lease-time-validation {
      lease-time-threshold seconds;
      violation-action action;
    }
    liveness-detection {
      failure-action (clear-binding | clear-binding-if-interface-up | log-only);
      method {
        bfd {
          version (0 | 1 | automatic);
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
          detection-time {
            threshold milliseconds;
          }
          session-mode(automatic | multihop | singlehop);
          holddown-interval milliseconds;
        }
        layer2-liveness-detection {
          max-consecutive-retries number;
          transmit-interval interval;
        }
```

```
    }
  }
  overrides {
    allow-snooped-clients;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delay-authentication;
    delete-binding-on-renegotiation;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    relay-source interface-name;
    send-release-on-delete;
  }
  relay-agent-interface-id {
    include-irb-and-l2;
    keep-incoming-interface-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
    use-vlan-id;
  }
  relay-agent-remote-id {
    include-irb-and-l2;
    keep-incoming-interface-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
    use-vlan-id;
  }
  relay-option {
    option-number option-number;
    default-action {
      drop;
      forward-only;
      relay-server-group relay-server-group;
    }
    equals (ascii ascii-string | hexadecimal hexadecimal-string) {
      drop;
      forward-only;
      relay-server-group relay-server-group;
    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
      drop;
      forward-only;
      relay-server-group relay-server-group;
    }
  }
  remote-id-mismatch disconnect;
  route-suppression;
  service-profile dynamic-profile-name;
```

```
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
leasequery {
    attempts number-of-attempts;
    timeout seconds;
}
lease-time-validation {
    lease-time-threshold seconds;
    violation-action action;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode(automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
        layer2-liveness-detection {
            max-consecutive-retries number;
            transmit-interval interval;
        }
        route-suppression;
        service-profile dynamic-profile-name;
    }
}
no-snoop;
overrides {
    allow-snooped-clients;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delay-authentication;
    delete-binding-on-renegotiation;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    relay-source interface-name;
    send-release-on-delete;
}
relay-agent-interface-id {
    include-irb-and-l2;
    keep-incoming-interface-id ;
```

```
      no-vlan-interface-name;
      prefix prefix;
      use-interface-description (logical | device);
      use-option-82 <strict>;
      use-vlan-id;
    }
    relay-agent-remote-id {
      include-irb-and-l2;
      keep-incoming-remote-id ;
      no-vlan-interface-name;
      prefix prefix;
      use-interface-description (logical | device);
      use-option-82 <strict>;
      use-vlan-id;
    }
    relay-option {
      option-number option-number;
      default-action {
        drop;
        forward-only;
        relay-server-group relay-server-group;
      }
      equals (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        relay-server-group relay-server-group;
      }
      starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        relay-server-group relay-server-group;
      }
    }
    relay-option-vendor-specific{
      host-name;
      location;
    remote-id-mismatch disconnect;
    route-suppression;
    server-group {
      server-group-name {
        server-ip-address;
      }
    }
    server-response-time seconds;
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
dual-stack-group dual-stack-group-name {
    access-profile profile-name;
    authentication {
      password password-string;
      username-include {
        circuit-type;
        delimiter delimiter-character;
        domain-name domain-name-string;
```

```
        interface-description  (device-interface | logical-interface);
        interface-name;
        logical-system-name;
        mac-address;
        relay-agent-interface-id;
        relay-agent-remote-id;
        routing-instance-name;
        user-prefix user-prefix-string;
        vlan-tags;
      }
    }
    classification-key {
      circuit-id circuit-id;
      mac-address mac-address;
      remote-id remote-id;
    }
    dual-stack-interface-client-limit number;
    dynamic-profile profile-name {
      aggregate-clients (merge | replace);
      use-primary primary-profile-name;
    }
    liveness-detection {
      failure-action (clear-binding | clear-binding-if-interface-up | log-only);
      method {
        layer2-liveness-detection {
          max-consecutive-retries number;
          transmit-interval interval;
        }
      }
    }
    protocol-master (inet | inet6);
    relay-agent-interface-id {
      include-irb-and-l2;
      keep-incoming-interface-id ;
      no-vlan-interface-name;
      prefix prefix;
      use-interface-description (logical | device);
      use-option-82 <strict>;
      use-vlan-id;
    }
    relay-agent-remote-id {
      include-irb-and-l2;
      keep-incoming-remote-id ;
      no-vlan-interface-name;
      prefix prefix;
      use-interface-description (logical | device);
      use-option-82 <strict>;
      use-vlan-id;
    }
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
  }
  duplicate-clients-in-subnet (incoming-interface | option-82):
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
```

```
    use-primary primary-profile-name;
}
forward-only {
    logical-system <current | default | logical-system-name>;
    routing-instance <current | default | routing-instance-name>;
}
forward-only-replies;
forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
group group-name {
    access-profile profile-name;
    active-server-group server-group-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description  (device-interface | logical-interface);
            interface-name interface-name;
            logical-system-name;
            mac-address;
            option-60;
            option-82 [circuit-id] [remote-id];
            routing-instance-name;
            user-prefix user-prefix-string;
            }
        vlan-tags;
    }
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    forward-only {
        logical-system <current | default | logical-system-name>;
        routing-instance <current | default | routing-instance-name>;
    }
    forward-only {
        logical-system <current | default | logical-system-name>;
        routing-instance <current | default | routing-instance-name>;
    }
    interface interface-name {
        access-profile profile-name;
        exclude;
        liveness-detection {
            failure-action (clear-binding | clear-binding-if-interface-up | log-only);
            method {
                bfd {
                    version (0 | 1 | automatic);
                    minimum-interval milliseconds;
                    minimum-receive-interval milliseconds;
                    multiplier number;
                    no-adaptation;
                    transmit-interval {
                        minimum-interval milliseconds;
```

```
            threshold milliseconds;
          }
          detection-time {
            threshold milliseconds;
          }
          session-mode (automatic | multihop | singlehop);
          holddown-interval milliseconds;
        }
      }
    }
    overrides {
      allow-no-end-option;
      allow-snooped-clients;
      always-write-giaddr;
      always-write-option-82;
      asymmetric-lease-time seconds;
      client-discover-match <option60-and-option82 | incoming-interface>;
      delay-authentication;
      delete-binding-on-renegotiation;
      disable-relay;
      dual-stack dual-stack-group-name;
      interface-client-limit number;
      layer2-unicast-replies;
      no-allow-snooped-clients;
      no-bind-on-request;
      proxy-mode;
      relay-source
      replace-ip-source-with;
      send-release-on-delete;
      trust-option-82;
    }
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    trace;
    upto upto-interface-name;
  }
  overrides {
    allow-no-end-option
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-discover-match (option60-and-option82 | incoming-interface);
    delay-authentication;
    delete-binding-on-renegotiation;
    disable-relay;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-bind-on-request;
    proxy-mode;
    relay-source
    replace-ip-source-with;
```

```
      send-release-on-delete;
      trust-option-82;
    }
    relay-option {
      option-number option-number;
      default-action {
        drop;
        forward-only;
        relay-server-group group-name;
      }
      equals (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        relay-server-group relay-server-group;
      }
      starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
      }
    }
    relay-option-82 {
      circuit-id {
        prefix prefix;
        use-interface-description (logical | device);
      }
      remote-id {
        prefix prefix;
        use-interface-description (logical | device);
      }
      server-id-override
    }
    remote-id-mismatch disconnect;
    route-suppression:
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
  }
  leasequery {
    attempts number-of-attempts;
    timeout seconds;
  }
  lease-time-validation {
    lease-time-threshold seconds;
    violation-action action;
  }
  liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
      bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
```

```
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        detection-time {
          threshold milliseconds;
        }
        session-mode (automatic | multihop | singlehop);
        holddown-interval milliseconds;
      }
      layer2-liveness-detection {
        max-consecutive-retries number;
        transmit-interval interval;
      }
    }
  }
  no-snoop;
  overrides {
    allow-no-end-option
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-discover-match (option60-and-option82 | incoming-interface);
    delay-authentication;
    delete-binding-on-renegotiation;
    disable-relay;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-bind-on-request;
    proxy-mode;
    relay-source
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
  }
  relay-option {
    option-number option-number;
    default-action {
      drop;
      forward-only;
      relay-server-group group-name;
    }
    equals (ascii ascii-string | hexadecimal hexadecimal-string) {
      drop;
      forward-only;
      relay-server-group relay-server-group;
    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
      drop;
      forward-only;
      local-server-group local-server-group;
```

```
      relay-server-group relay-server-group;
    }
  }
  relay-option-82 {
    circuit-id {
      prefix prefix;
      use-interface-description (logical | device);
    }
    remote-id {
      prefix prefix;
      use-interface-description (logical | device);
    }
    server-id-override
  }
  }
  remote-id-mismatch disconnect;
  route-suppression:
  server-group {
    server-group-name {
      server-ip-address;
    }
  }
  server-response-time seconds;
  service-profile dynamic-profile-name;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

Hierarchy Level

```
[edit forwarding-options],
[edit logical-systems logical-system-name forwarding-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options],
[edit routing-instances routing-instance-name forwarding-options]
```

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 13.2X51 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure extended Dynamic Host Configuration Protocol (DHCP) relay and DHCPv6 relay options on the router or switch to enable the router (or switch) to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.

DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication or client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.

The extended DHCP and DHCPv6 relay agent options configured with the **dhcp-relay** and **dhcpv6** statements are incompatible with the DHCP/BOOTP relay agent options configured with the **bootp** statement. As a result, the extended DHCP or DHCPv6 relay agent and the DHCP/BOOTP relay agent cannot both be enabled on the router (or switch) at the same time.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618
- DHCPv6 Relay Agent Overview on page 648
- DHCP Relay Proxy Overview on page 646
- Using External AAA Authentication Services with DHCP on page 651

dhcp-service

Syntax

```
dhcp-service {
  accept-max-tcp-connections max-tcp-connections;
  dhcp-snooping-file(local_pathname | remote_URL) {
    write-interval interval;
  }
  dhcpv6-snooping-file {
    location;
    write-interval seconds;
  }
  (disable | enable);
  interface-traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    level  (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
  log {
    session {
      client;
      all;
      dhcpv6 {
        client;
        server;
        relay;
        dynamic-server;
        all;
      }
      server;
      relay;
    }
  }
  ltv-syslog-interval seconds;
  persistent-storage {
    backup-interval backup-interval;
    file-name;
  }
  request-max-tcp-connections max-tcp-connections;
  traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    level  (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1 for MX Series routers.
Support for log option introduced in Junos OS Release 19.1R1 for SRX Series devices.

Description

Enable DHCP services on the device. DHCP services automate network-parameter assignment to network devices. The DHCP service process is enabled by default. However, by default, IP-MAC bindings in the DHCP snooping database do not persist through device reboots. You can inprove performance after rebooting by configuring the IP-MAC bindings to persist, by configuring a storage location for the DHCP database file. When specifying the location for the DHCP database, you must also specify how frequently the switch writes the database entries into the DHCP snooping database file.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Configuring Persistent Bindings in the DHCP or DHCPv6 (ELS)*

dhcpv6 (DHCP Local Server)

Syntax

```
dhcpv6 {
  access-profile profile-name;
  allow-active-leasequery {
    idle-timeout seconds;
    peer-address address;
    timeout seconds;
  }
  allow-bulk-leasequery {
    max-connections number-of-connections;
    max-empty-replies number-of-replies;
    restricted-requestor;
    timeout seconds;
  }
  allow-leasequery {
    restricted-requestor;
  }
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-description  (device-interface | logical-interface);
      logical-system-name;
      mac-address;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
      vlan-tags;
    }
  }
  duplicate-clients incoming-interface;
  group group-name {
    access-profile profile-name;
    authentication {
    ...
    interface interface-name {
      access-profile profile-name;
      exclude;
      liveness-detection {
        failure-action (clear-binding | clear-binding-if-interface-up | log-only);
        method {
          bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
```

```
            transmit-interval {
              minimum-interval milliseconds;
              threshold milliseconds;
            }
            detection-time {
              threshold milliseconds;
            }
            session-mode(automatic | multihop | singlehop);
            holddown-interval milliseconds;
          }
        }
      }
      overrides {
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-negotiation-match incoming-interface;
        delay-advertise {
          based-on (option-15 | option-16 | option-18 | option-37) {
            equals {
              ascii ascii-string;
              hexadecimal hexadecimal-string;
            }
            not-equals {
              ascii ascii-string;
              hexadecimal hexadecimal-string;
            }
            starts-with {
              ascii ascii-string;
              hexadecimal hexadecimal-string;
            }
          }
          delay-time seconds;
        }
        delete-binding-on-renegotiation;
        interface-client-limit number;
        multi-address-embedded-option-response;
        process-inform {
          pool pool-name;
        }
        protocol-attributes attribute-set-name;
        rapid-commit;
      }
      service-profile dynamic-profile-name;
      short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
      trace;
      upto upto-interface-name;
    }
    liveness-detection {
      failure-action (clear-binding | clear-binding-if-interface-up | log-only);
      method {
        bfd {
          version (0 | 1 | automatic);
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
```

```
            no-adaptation;
            transmit-interval {
              minimum-interval milliseconds;
              threshold milliseconds;
            }
            detection-time {
              threshold milliseconds;
            }
            session-mode(automatic | multihop | singlehop);
            holddown-interval milliseconds;
          }
          layer2-liveness-detection {
            max-consecutive-retries number;
            transmit-interval interval;
          }
        }
      }
      overrides {
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-negotiation-match incoming-interface;
        delay-advertise {
          based-on (option-15 | option-16 | option-18 | option-37) {
            equals {
              ascii ascii-string;
              hexadecimal hexadecimal-string;
            }
            not-equals {
              ascii ascii-string;
              hexadecimal hexadecimal-string;
            }
            starts-with {
              ascii ascii-string;
              hexadecimal hexadecimal-string;
            }
          }
          delay-time seconds;
        }
        delegated-pool;
        delete-binding-on-renegotiation;
        interface-client-limit number;
        multi-address-embedded-option-response;
        process-inform {
          pool pool-name;
        }
        protocol-attributes attribute-set-name;
        rapid-commit;
      }
      route-suppression;
      service-profile dynamic-profile-name;
      short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    }
    liveness-detection {
      failure-action (clear-binding | clear-binding-if-interface-up | log-only);
      method {
```

```
      bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        detection-time {
          threshold milliseconds;
        }
        session-mode(automatic | multihop | singlehop);
        holddown-interval milliseconds;
      }
      layer2-liveness-detection {
        max-consecutive-retries number;
        transmit-interval interval;
      }
    }
  }
  overrides {
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delay-advertise {
      based-on (option-15 | option-16 | option-18 | option-37) {
        equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        not-equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        starts-with {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
      }
      delay-time seconds;
    }
    delegated-pool;
    delete-binding-on-renegotiation;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
      pool pool-name;
    }
    protocol-attributes attribute-set-name;
    rapid-commit;
    reconfigure {
      attempts attempt-count;
      clear-on-abort;
```

```
      strict;
      timeout timeout-value;
      token token-value;
      trigger {
        radius-disconnect;
      }
    }
  }
  reauthenticate (<lease-renewal> <remote-id-mismatch >);
  reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    support-option-pd-exclude;
    timeout timeout-value;
    token token-value;
    trigger {
      radius-disconnect;
    }
  }
  requested-ip-network-match subnet-mask;
  route-suppression;
  server-duid-type type;
  service-profile dynamic-profile-name;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
  services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]
```

Release Information

Statement introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Configure DHCPv6 local server options on the router or switch to enable the router or switch to function as a server for the DHCP protocol for IPv6. The DHCPv6 local server sends and receives packets using the IPv6 protocol and informs IPv6 of the routing requirements of router clients. The local server works together with the AAA service framework to control subscriber access (or DHCP client access) and accounting.

The DHCPv6 local server is fully compatible with the extended DHCP local server and DHCP relay agent.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- DHCPv6 Local Server Overview on page 613

dhcpv6 (DHCP Relay Agent)

Syntax

```
dhcpv6 {
  access-profile profile-name;
  active-leasequery {
    idle-timeout seconds;
    peer-address address;
    timeout seconds;
    topology-discovery;
  }
  active-server-group server-group-name;
  }
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-description  (device-interface | logical-interface);
      interface-name interface-name;
      logical-system-name;
      mac-address mac-address;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
      vlan-tags;
    }
  }
  bulk-leasequery {
    attempts number-of-attempts;
    timeout seconds;
    trigger automatic;
  }
  duplicate-clients incoming-interface;
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
  }
  forward-only {
    logical-system <current | default | logical-system-name>;
    routing-instance <current | default | routing-instance-name>;
  }
  forward-only-replies;
  }
  forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
  group group-name {
    access-profile profile-name;
    active-server-group server-group-name;
    authentication {
```

```
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-description  (device-interface | logical-interface);
      interface-name;
      logical-system-name;
      mac-address;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
      vlan-tags;
    }
  }
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
  }
  forward-only {
    logical-system <current | default | logical-system-name>;
    routing-instance <current | default | routing-instance-name>;
  }
  interface interface-name {
    access-profile profile-name;
    dynamic-profile profile-name {
      aggregate-clients (merge | replace);
      use-primary primary-profile-name;
    }
    exclude;
    overrides {
      allow-snooped-clients;
      asymmetric-lease-time seconds;
      asymmetric-prefix-lease-time seconds;
      client-negotiation-match incoming-interface;
      delay-authentication;
      delete-binding-on-renegotiation;
      dual-stack dual-stack-group-name;
      interface-client-limit number;
      no-allow-snooped-clients;
      no-bind-on-request;
      relay-source interface-name;
      send-release-on-delete;
    }
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    trace;
    upto upto-interface-name;
  }
  }
  lease-time-validation {
    lease-time-threshold seconds;
```

```
    violation-action action;
  }
  liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
      bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        detection-time {
          threshold milliseconds;
        }
        session-mode(automatic | multihop | singlehop);
        holddown-interval milliseconds;
      }
      layer2-liveness-detection {
        max-consecutive-retries number;
        transmit-interval interval;
      }
    }
  }
  overrides {
    allow-snooped-clients;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delay-authentication;
    delete-binding-on-renegotiation;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    relay-source interface-name;
    send-release-on-delete;
  }
  relay-agent-interface-id {
    include-irb-and-l2;
    keep-incoming-interface-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
  }
  relay-agent-remote-id {
    include-irb-and-l2;
    keep-incoming-interface-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
```

```
      use-option-82 <strict>;
    }
    relay-option {
      option-number option-number;
      default-action {
        drop;
        forward-only;
        relay-server-group relay-server-group;
      }
      equals (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        relay-server-group relay-server-group;
      }
      starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        relay-server-group relay-server-group;
      }
    }
    remote-id-mismatch disconnect;
    route-suppression;
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
  }
  leasequery {
    attempts number-of-attempts;
    timeout seconds;
  }
  lease-time-validation {
    lease-time-threshold seconds;
    violation-action action;
  }
  liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
      bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        detection-time {
          threshold milliseconds;
        }
        session-mode(automatic | multihop | singlehop);
        holddown-interval milliseconds;
      }
      layer2-liveness-detection {
        max-consecutive-retries number;
        transmit-interval interval;
```

```
      }
      route-suppression;
      service-profile dynamic-profile-name;
    }
  }
  no-snoop;
  overrides {
    allow-snooped-clients;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delay-authentication;
    delete-binding-on-renegotiation;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    relay-source interface-name;
    send-release-on-delete;
  }
  relay-agent-interface-id {
    include-irb-and-l2;
    keep-incoming-interface-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
  }
  relay-agent-remote-id {
    include-irb-and-l2;
    keep-incoming-interface-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
  }
  relay-option {
    option-number option-number;
    default-action {
      drop;
      forward-only;
      relay-server-group relay-server-group;
    }
    equals (ascii ascii-string | hexadecimal hexadecimal-string) {
      drop;
      forward-only;
      relay-server-group relay-server-group;
    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
      drop;
      forward-only;
      relay-server-group relay-server-group;
    }
  }
  relay-option-vendor-specific{
```

```
    host-name;
    location;
  remote-id-mismatch disconnect;
  route-suppression;
  server-group {
    server-group-name {
      server-ip-address;
    }
  }
  server-response-time seconds;
  service-profile dynamic-profile-name;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit logical-systems logical-system-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.
Support for **forward-snooped-clients** introduced in Junos OS Release 15.1X53-D56 for EX Series switches and Junos OS Release 17.1R1.

Description

Configure DHCPv6 relay options on the router or switch and enable the router or switch to function as a DHCPv6 relay agent. A DHCPv6 relay agent forwards DHCPv6 request and reply packets between a DHCPv6 client and a DHCPv6 server.

The DHCPv6 relay agent server is fully compatible with the extended DHCP local server and DHCP relay agent. However, the options configured with the **dhcpv6** statement are incompatible with the DHCP/BOOTP relay agent options configured with the **bootp** statement. As a result, the DHCPv6 relay agent and the DHCP/BOOTP relay agent cannot be enabled on the router or switch at the same time.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- dhcp-relay on page 997
- DHCPv6 Relay Agent Overview on page 648
- Using External AAA Authentication Services with DHCP on page 651

dhcpv6 (System Services)

Syntax

```
dhcpv6 {
  authentication {
    password password;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name;
      interface-name;
      logical-system-name;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix;
    }
  }
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
    junos-default-profile;
    use-primary dynamic-profile-name;
  }
  group group-name {
    authentication {
      password password;
      username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name;
        interface-name;
        logical-system-name;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix;
      }
    }
    dynamic-profile {
      profile-name;
      aggregate-clients {
        merge;
        replace;
      }
      junos-default-profile;
      use-primary dynamic-profile;
```

```
}
interface interface-name {
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
    junos-default-profile;
    use-primary dynamic-profile-name;
  }
  exclude;
  overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    rapid-commit ;
  }
  service-profile service-profile-name
  trace ;
  upto interface-name;
}
liveness-detection {
  failure-action {
    clear-binding;
    clear-binding-if-interface-up;
    log-only;
  }
  method {
    bfd {
      detection-time {
        threshold milliseconds;
      }
      holddown-interval interval;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      session-mode (automatic | multihop | single-hop);
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
    version (0 | 1 | automatic);
  }
}
overrides {
  delegated-pool pool-name;
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
  rapid-commit ;
```

```
    }
    reconfigure {
      attempts number;
      clear-on-abort;
      strict;
      timeout number;
      token token-name;
      trigger {
        radius-disconnect;
      }
    }
    service-profile service-profile-name;
  }
  liveness-detection {
    failure-action {
      clear-binding;
      clear-binding-if-interface-up;
      log-only;
    }
    method {
      bfd {
        detection-time {
          threshold milliseconds;
        }
        holddown-interval interval;
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        session-mode (automatic | multihop | single-hop);
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
      version (0 | 1 | automatic);
    }
  }
  overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    rapid-commit ;
  }
  reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
      radius-disconnect;
    }
  }
```

```
  service-profile service-profile-name;
}
```

Hierarchy Level

```
[edit system services]
```

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Configure DHCPv6 server to provide IPv6 addresses to clients.

NOTE: SRX Series devices do not support client authentication.

Options

- **duplicate-clients-on-interface**—Allow duplicate clients on different interfaces in a subnet.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*

dhcpv6-client

Syntax

```
dhcpv6-client {
  client-ia-type {
    ia-na;
    ia-pd;
  }
  client-identifier duid-type (duid-ll | duid-llt | vendor);
  client-type (autoconfig | stateful);
  rapid-commit;
  req-option (dns-server | domain | fqdn | nis-domain | nis-server | ntp-server | sip-domain
    | sip-server |time-zone | vendor-spec);
  retransmission-attempt number;
  update-router-advertisement {
    interface interface-name;
  }
  update-server;
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet6]
[edit logical-systems name interfaces name unit name family inet6]
[edit tenants tenant-name interfaces name unit name family inet6]
```

Release Information Statement introduced in Junos OS Release 12.1X45-D10.
The **logical-systems** and **tenants** options are introduced in Junos OS Release 18.4R1.

Description Configure the Dynamic Host Configuration Protocol version 6 (DHCPv6) client.

NOTE: Starting in Junos OS Release 18.1R1, DHCPv4 and DHCPv6 clients are supported on management interfaces (fxp0 and em0) configured in the non-default management routing instance, **mgmt_junos**.

Options

client-ia-type— Identity association type for DHCPv6 client. This statement is mandatory.

client-identifier duid-type— Identity a client by a client-identifier value. This statement is mandatory.

client-type— Identify the type of DHCPv6 client. This statement is mandatory.

rapid-commit— The use of the two-message exchange for address assignment.

req-option— Specify options requested by the DHCPv6 client.

retransmission-attempt number— Specify the number of times the device retransmits a DHCPv6 client packet if a DHCPv6 server fails to respond. After the specified number of attempts, no further attempts at reaching a server are made.

update-router-advertisement— Specify the interface used to delegate prefixes.

update-server— Propagate TCP/IP settings to the DHCPv6 server.

For detailed information about these commands, see CLI Explorer.

Required Privilege Level

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*
- Minimum DHCPv6 Client Configuration on page 787

dhcp-attributes (Access IPv4 Address Pools)

Syntax

```
dhcp-attributes {
  boot-file boot-file-name;
  boot-server boot-server-name;
  domain-name domain-name;
  grace-period seconds;
  maximum-lease-time (seconds | infinite);
  name-server ipv4-address;
  netbios-node-type (b-node | h-node | m-node | p-node);
  next-server next-server-name;
  option dhcp-option-identifier-code {
    array {
      byte [8-bit-value];
      flag [ false| off |on |true];
      integer [32-bit-numeric-values];
      ip-address [ip-address];
      short [signed-16-bit-numeric-value];
      string [character string value];
      unsigned-integer [unsigned-32-bit-numeric-value];
      unsigned-short [16-bit-numeric-value];
    }
    byte 8-bit-value;
    flag (false | off | on | true);
    integer 32-bit-numeric-values;
    ip-address ip-address;
    short signed-16-bit-numeric-value;
    string character string value;
    unsigned-integer unsigned-32-bit-numeric-value;
    unsigned-short 16-bit-numeric-value;
  }
  option-match {
    option-82 {
      circuit-id match-value {
        range range-name;
      }
      remote-id match-value;
        range range-name;
      }
    }
  }
  propagate-ppp-settings [interface-name];
  propagate-settings interface-name;
  router ipv4-address;
  server-identifier ip-address;
  sip-server {
    ip-address ipv4-address;
    name sip-server-name;
  }
  tftp-server server-name;
  wins-server ipv4-address;
}
```

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

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure attributes for IPv4 address pools that can be used by different clients. The DHCP attributes for this statement uses standard IPv4 DHCP options.

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*

dhcp-attributes (Access IPv6 Address Pools)

Syntax

```
dhcp-attributes {
  dns-server ipv6-address;
  grace-period seconds;
  maximum-lease-time (seconds | infinite);
  option dhcp-option-identifier-code {
    array {
      byte [8-bit-value];
      flag [ false| off |on |true];
      integer [32-bit-numeric-values];
      ip-address [ip-address];
      short [signed-16-bit-numeric-value];
      string [character string value];
      unsigned-integer [unsigned-32-bit-numeric-value];
      unsigned-short [16-bit-numeric-value];
    }
    byte 8-bit-value;
    flag (false | off | on | true);
    integer 32-bit-numeric-values;
    ip-address ip-address;
    short signed-16-bit-numeric-value;
    string character string value;
    unsigned-integer unsigned-32-bit-numeric-value;
    unsigned-short 16-bit-numeric-value;
  }
  propagate-ppp-settings [interface-name];
  sip-server-address ipv6-address;
  sip-server-domain-name domain-name;
}
```

Hierarchy Level

```
[edit access address-assignment pool pool-name family inet6]
```

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure attributes for address pools that can be used by different clients.

Options

- **dns-server** ***IPv6-address***—Specify a DNS server to which clients can send DNS queries.
- **grace-period** ***seconds*** —Specify the grace period offered with the lease.

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

  Default: 0 (no grace period)

- **maximum-lease-time** ***seconds***—Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.

  Range: 30 through 4,294,967,295 seconds

  Default: 86,400 seconds (24 hours)

- **option** ***dhcp-option-identifier-code***—Specify the DHCP option identifier code.
- **propagate-ppp-settings [***interface-name***—**Specify PPP interface name for propagating DNS or WINS settings.
- **sip-server-address** ***IPv6-address***—Specify the IPv6 address of the SIP outbound proxy server.
- **sip-server-domain-name** ***domain-name***—Specify the domain name of the SIP outbound proxy server.

Required Privilege Level

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*

dhcp-local-server (System Services)

Syntax

```
dhcp-local-server {
  dhcpv6 {
    authentication {
      password password;
      username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name;
        interface-name;
        logical-system-name;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix;
      }
    }
    dynamic-profile {
      profile-name;
      aggregate-clients {
        merge;
        replace;
      }
      junos-default-profile;
      use-primary dynamic-profile-name;
    }
    group group-name {
      authentication {
        password password;
        username-include {
          circuit-type;
          client-id;
          delimiter delimiter-character;
          domain-name domain-name;
          interface-name;
          logical-system-name;
          relay-agent-interface-id;
          relay-agent-remote-id;
          relay-agent-subscriber-id;
          routing-instance-name;
          user-prefix user-prefix;
        }
      }
      dynamic-profile {
        profile-name;
        aggregate-clients {
          merge;
          replace;
        }
        junos-default-profile;
```

```
    use-primary dynamic-profile;
  }
  interface interface-name {
    dynamic-profile {
      profile-name;
      aggregate-clients {
        merge;
        replace;
      }
      junos-default-profile;
      use-primary dynamic-profile-name;
    }
    exclude;
    overrides {
      delegated-pool pool-name;
      interface-client-limit number;
      process-inform {
        pool pool-name;
      }
      rapid-commit ;
    }
    service-profile service-profile-name
    trace ;
    upto interface-name;
  }
  liveness-detection {
    failure-action {
      clear-binding;
      clear-binding-if-interface-up;
      log-only;
    }
    method {
      bfd {
        detection-time {
          threshold milliseconds;
        }
        holddown-interval interval;
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        session-mode (automatic | multihop | single-hop);
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
      version (0 | 1 | automatic);
    }
  }
  overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
```

```
      rapid-commit ;
    }
    reconfigure {
      attempts number;
      clear-on-abort;
      strict;
      timeout number;
      token token-name;
      trigger {
        radius-disconnect;
      }
    }
    service-profile service-profile-name;
  }
  liveness-detection {
    failure-action {
      clear-binding;
      clear-binding-if-interface-up;
      log-only;
    }
    method {
      bfd {
        detection-time {
          threshold milliseconds;
        }
        holddown-interval interval;
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        session-mode (automatic | multihop | single-hop);
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
      version (0 | 1 | automatic);
    }
  }
  overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    rapid-commit ;
  }
  reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
      radius-disconnect;
    }
```

```
    }
    service-profile service-profile-name;
  }
  group group-name {
    interface interface-name {
      exclude;
      upto upto-interface-name;
    }
  }
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure DHCP Local Server for DHCPv6, forwarding snoop (unicast) packets, and setting traceoptions.

NOTE: SRX Series devices do not support client authentication.

Options The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*

disable (802.1X)

Syntax

```
disable;
```

Hierarchy Level

```
[edit protocols dot1x authenticator interface (all | [interface-names])]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Disable 802.1X authentication on a specified interface or all interfaces.

Default

802.1X authentication is disabled on all interfaces.

Required Privilege Level

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

Related Documentation

- show dot1x on page 1799
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 343
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 368
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- *Configuring 802.1X Authentication (J-Web Procedure)*

disable (802.1X)

Syntax

```
disable;
```

Hierarchy Level

[edit protocols dot1x authenticator interface (all | [*interface-names*])]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Disable 802.1X authentication on a specified interface or all interfaces.

Default

802.1X authentication is disabled on all interfaces.

Required Privilege Level

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

Related Documentation

- show dot1x on page 1799
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 343
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 368
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- *Configuring 802.1X Authentication (J-Web Procedure)*

disable (LLDP)

Syntax

```
disable;
```

Hierarchy Level

[edit protocols lldp],
[edit protocols interface lldp]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Disable the LLDP configuration on the switch or on one or more interfaces.

Default

If you do not configure LLDP, it is disabled on the switch and on specific switch interfaces.

Required Privilege Level

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

Related Documentation

- show lldp on page 1826
- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518
- Understanding LLDP on page 511

disable (LLDP-MED)

Syntax
```
disable;
```

Hierarchy Level
```
[edit protocols lldp-med],
[edit protocols lldp-med interface]
```

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

Description Disable the LLDP-MED configuration on the switch or on one or more interfaces.

Default If you do not configure LLDP-MED, it is disabled on the switch and on specific switch interfaces.

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

Related Documentation
- show lldp on page 1826
- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

disable (LLDP Power Negotiation)

Syntax
```
disable;
```

Hierarchy Level
```
[edit protocols lldp interface (all | interface-name) power-negotiation]
```

Release Information Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description Disable Link Layer Discovery Protocol (LLDP) power negotiation, which negotiates with Power over Ethernet (PoE)-powered devices to allocate power.

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

Related Documentation
- Configuring LLDP (CLI Procedure) on page 512
- *Configuring PoE on EX Series Switches (CLI Procedure)*

disable-relay

Syntax

```
disable-relay;
```

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* interface *interface-name* overrides]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Disable DHCP relay on specific interfaces in a group.

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618

diameter-instance (Diameter Applications)

Syntax

```
diameter-instance instance-name;
```

Hierarchy Level

```
[edit access gx-plus partition partition-name]
[edit access ocs partition partition-name],
[edit access pcrf partition partition-name]
```

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support at the **[edit access ocs partition *partition-name*]** and **[edit access pcrf partition *partition-name*]** hierarchy levels introduced in Junos OS Release 16.2.

Description

Specify the Diameter instance associated with the Gx-Plus, OCS, or PCRF partition.

Options

instance-name—Name of the Diameter instance. Currently, only **master** is supported.

Required Privilege Level

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

Related Documentation

- *Configuring Gx-Plus*
- *Configuring the Gx-Plus Partition*
- *Configuring the OCS Partition*
- *Understanding Gx Interactions Between the Router and the PCRF*
- *Understanding Gy Interactions Between the Router and the OCS*

disable (System Services)

Syntax

```
disable;
```

Hierarchy Level

```
[edit system services dns dnssec]
```

Release Information Statement introduced in Junos OS Release 10.2 .

Description Disables DNSSEC in the DNS server.

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*

dlv

Syntax

```
dlv {
  domain-name domain-name trusted-anchor  trusted-anchor;
  }
```

Hierarchy Level

```
[edit system services dns dnssec]
```

Release Information Statement introduced in Junos OS Release 10.2 .

Description Configure DNSSEC Lookaside Validation (DLV).

Options

- **domain-name *domain-name***—Specify the secure domain server name.
- **trusted-anchor *trusted-anchor***—Specify the trusted DLV anchor.

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*

domain (Domain Map)

Syntax

```
domain {
  delimiter [delimiter-character];
  map domain-map-name {
    aaa-logical-system logical-system-name {
      aaa-routing-instance routing-instance-name;
    }
    aaa-routing-instance routing-instance-name;
    access-profile profile-name;
    address-pool pool-name;
    dynamic-profile profile-name;
    padn destination-address {
      mask destination-mask;
      metric route-metric;
    }
    strip-domain;
    target-logical-system logical-system-name {
      target-routing-instance routing-instance-name;
    }
    target-routing-instance routing-instance-name;
    tunnel-profile profile-name;
  }
  parse-direction (left-to-right | right-to-left);
  parse-order (domain-first | realm-first);
  realm-delimiter [delimiter-character];
  realm-parse-direction (left-to-right | right-to-left);
}
```

Hierarchy Level

```
[edit access]
```

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Configure a domain map, which is used to map access options and session parameters for subscriber sessions.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Configuring a Domain Map*

domain-name-server (Routing Instances and Access Profiles)

Syntax

```
domain-name-server dns-address;
```

Hierarchy Level

```
[edit access];
[edit access profile]
```

Release Information

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the **[edit access]** hierarchy level or for an access profile at the **[edit access profile *profile-name*]** hierarchy level. You can configure more than one address by including the statement multiple times.

NOTE: A DNS name server address configured with this statement is less preferred than one configured with the domain-name-server-inet statement. That is, the server with the address configured with the domain-name-server-inet takes precedence over a server configured with this statement.

Options

dns-address—IPv4 address of the DNS name server.

Required Privilege Level

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

Related Documentation

- *Configuring DNS Name Server Addresses for Subscriber Management*
- *DNS Name Server Address Overview*

domain-name-server-inet (Routing Instances and Access Profiles)

Syntax

```
domain-name-server-inet dns-address;
```

Hierarchy Level

```
[edit access],
[edit access profile]
```

Release Information

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the **[edit access]** hierarchy level or for an access profile at the **[edit access profile *profile-name*]** hierarchy level. You can configure more than one address by including the statement multiple times.

NOTE: A DNS name server address configured with this statement is higher in preference than one configured with the domain-name-server statement. That is, the server with the address configured with the domain-name-server-inet takes precedence over a server configured with the domain-name-server statement.

Options

dns-address—IPv4 address of the DNS name server.

Required Privilege Level

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

Related Documentation

- *Configuring DNS Name Server Addresses for Subscriber Management*
- *DNS Name Server Address Overview*

domain-name-server-inet6 (Routing Instances and Access Profiles)

Syntax domain-name-server-inet6 *dns-address*;

Hierarchy Level [edit access],
[edit access profile]

Release Information Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure an IPv6 address for a DNS name server. You can configure an address globally for a routing instance at the **[edit access]** hierarchy level or for an access profile at the **[edit access profile *profile-name*]** hierarchy level. You can configure more than one address by including the statement multiple times.

Options ***dns-address***—IPv6 address of the DNS name server.

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

Related Documentation

- *Configuring DNS Name Server Addresses for Subscriber Management*
- *DNS Name Server Address Overview*

dot1x

Syntax

```
dot1x {
  authenticator {
    authentication-profile-name access-profile-name;
    interface (all | [ interface-names ]) {
      disable;
      guest-vlan (vlan-id | vlan-name);
      lldp-med-bypass;
      mac-radius <restrict>;
      maximum-requests number;
      no-reauthentication;
      quiet-period seconds;
      reauthentication {
        interval seconds;
      }
      retries number;
      server-fail (deny | permit | use-cache | vlan-id | vlan-name);
      server-reject-vlan (vlan-id | vlan-name) {
        eapol-block;
        block-interval block-interval;
      }
      server-timeout seconds;
      supplicant (single | single-secure | multiple);
      supplicant-timeout seconds;
      transmit-period seconds;
    }
    no-mac-table-binding;
    static  mac-address {
      interface interface-names;
      vlan-assignment (vlan-id |vlan-name);
    }
  }
}
```

Hierarchy Level

[edit protocols]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure 802.1X authentication for Port-Based Network Access Control. 802.1X authentication is supported on interfaces that are members of private VLANs (PVLANs).

The remaining statements are explained separately. See CLI Explorer.

Default

802.1X is disabled.

Required Privilege Level

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

Related Documentation

- show dot1x on page 1799
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 343
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 368
- Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 326
- Configuring RADIUS Server Fail Fallback (CLI Procedure) on page 287

domain-name (DHCP)

Syntax

```
domain-name domain-name;
```

Hierarchy Level

```
[edit system services dhcp
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

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 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.

Options

domain-name—Name of the domain.

Required Privilege Level

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

Related Documentation

- Configuring a DHCP Server on Switches (CLI Procedure) on page 588

domain-name (DHCP Local Server)

Syntax

domain-name *domain-name-string*;

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the domain name that is concatenated with the username during the subscriber authentication or DHCP client authentication process.

Options

domain-name-string—Domain name formatted string.

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

Related Documentation
- Using External AAA Authentication Services with DHCP on page 651

domain-name (DHCP Relay Agent)

Syntax

domain-name *domain-name-string*;

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name* authentication username-include],
[edit forwarding-options dhcp-relay group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include]
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* authentication username-include]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Support at the **[edit ... dual-stack-group *dual-stack-group-name*]** hierarchy level introduced in Junos OS Release 15.1.

Description

Specify the domain name that is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

Options

domain-name-string—Domain name formatted string.

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

Related Documentation
- Using External AAA Authentication Services with DHCP on page 651
- Creating Unique Usernames for DHCP Clients on page 653

domain-search

Syntax
```
domain-search [domain-list ];
```

Hierarchy Level
```
[edit system],
[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

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 list of domains to search (in the case where you want to configure access to multiple DNS servers for redundancy, and/or to resolve hosts that the previous server could not).

Options
domain-list—List of domain servers to search. The list can contain up to six domain names, separated by a space, with a total of up to 256 characters.

For example to search **domain1.net**, and if it fails to resolve the host, **domain2.net**, and if fails to resolve the host, **domain3.net**, you would configure the following domain list at the **domain-search** hierarchy level:

```
[edit system]
set domain-search [domain1.net domain2.net domain3.net]
```

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

Related Documentation
- Configuring a Domain Name and Domain Search List for a DHCP Server Host on page 551
- *Configuring a DNS Name Server for Resolving a Hostname into Addresses*

drop (DHCP Relay Agent Option)

Syntax

```
drop;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option (default-action | equals | starts-with)],
[edit forwarding-options dhcp-relay dhcpv6 relay-option (default-action | equals |
  starts-with)],
[edit forwarding-options dhcp-relay group group-name relay-option (default-action | equals
  | starts-with)],
[edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option (default-action
  | equals | starts-with)],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 12.3.

Description

Drop (discard) specified DHCP client packets when you use DHCP relay agent selective processing. You can configure the drop operation globally or for a group of interfaces, and for either DHCP or DHCPv6 relay agent.

Required Privilege Level

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

Related Documentation

- *Using DHCP Option Information to Selectively Process DHCP Client Traffic*

dynamic-pool

Syntax

```
address-assignment {
  dynamic-pool <dynamic-pool>{
    family {
      inet6 {
        from-interface <interface>;
        delegated-prefix-length <network-prefix-length>;
        range <range-name> {
          masked-low <masked-low>;
          masked-high <masked-high>;
          prefix-length <prefix-length>;
        }
        dhcp-attributes {
          dns-server <address>;
          t1-percentage <t1-percentage>;
          t2-percentage <t2-percentage>;
          preferred-lifetime <preferred-lifetime>;
          valid-lifetime <valid-lifetime>;
        }
      }
    }
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 15.1X49-D70.

Description Configure the dynamic pool updated by the client running on the WAN interface.

Options The remaining statements are explained separately.

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

Related Documentation

- Configuring Address-Assignment Pools on page 730
- address-assignment (Access) on page 852

dynamic-profile (DHCP Local Server)

Syntax

```
dynamic-profile profile-name {
  aggregate-clients (merge | replace);
  use-primary primary-profile-name;
}
```

Hierarchy Level

```
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name],
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server group group-name interface interface-name],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
  services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]
```

Release Information

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Options **aggregate-clients** and **use-primary** introduced in Junos OS Release 9.3.
Support at the **[edit ... interface]** hierarchy levels introduced in Junos OS Release 11.2.

Description

Specify the dynamic profile that is attached to all interfaces, a named group of interfaces, or a specific interface.

Options

profile-name—Name of the dynamic profile.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
- *Configuring a Default Subscriber Service*

dynamic-profile (DHCP Relay Agent)

Syntax

```
dynamic-profile profile-name {
  aggregate-clients (merge | replace);
  use-primary primary-profile-name;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay group group-name interface interface-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 9.2.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Support at the **[edit ... dual-stack-group *dual-stack-group-name*]** hierarchy level introduced in Junos OS Release 15.1.

Description

Specify the dynamic profile that is attached to all interfaces, to a named group of interfaces, or to a specific interface.

M120 and M320 routers do not support DHCPv6.

Options

profile-name—Name of the dynamic profile.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- dhcp-relay on page 997
- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
- Grouping Interfaces with Common DHCP Configurations on page 670
- *Configuring a Default Subscriber Service*

dynamic-profile-options

Syntax

```
dynamic-profile-options {
  versioning;
}
```

Hierarchy Level

[edit system]

Release Information

Statement introduced in Junos OS Release 11.4.

Description

Configure global dynamic profile options.

The remaining statement is explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Versioning for Dynamic Profiles*

dynamic-server

Syntax

```
dhcpv6 {
  dynamic-server {
    group <group> {
      neighbor-discovery-router-advertisement <ndra-pool>;
      interface <interface> {
        overrides {
          delegated-pool <delegated-pool>;
          ia-na-pool <ia-na-pool>;
          process-inform {
            pool <pool>;
          }
        }
      }
    }
  }
}
```

Hierarchy Level

```
[edit system services]
```

Release Information Statement introduced in Junos OS Release 15.1X49-D70.

Description Configure the server running on a LAN interface.

Options The remaining statements are explained separately.

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

Related Documentation

- dhcp-local-server (System Services) on page 1034
- dhcp-client on page 985

group (DHCP Local Server)

Syntax

```
group group-name {
  access-profile profile-name;
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-description  (device-interface | logical-interface);
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      relay-agent-interface-id
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
      vlan-tags;
    }
  }
  dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
    primary-profile-name>;
  interface interface-name {
    access-profile profile-name;
    exclude;
    overrides {
      asymmetric-lease-time seconds;
      asymmetric-prefix-lease-time seconds;
      client-discover-match <option60-and-option82>;
      client-negotiation-match incoming-interface;
      delay-advertise {
        based-on (option-15 | option-16 | option-18 | option-37) {
          equals {
            ascii ascii-string;
            hexadecimal hexadecimal-string;
          }
          not-equals {
            ascii ascii-string;
            hexadecimal hexadecimal-string;
          }
          starts-with {
            ascii ascii-string;
            hexadecimal hexadecimal-string;
          }
        }
        delay-time seconds;
      }
      delay-offer {
        based-on (option-60 | option-77 | option-82) {
```

```
            equals {
              ascii ascii-string;
              hexadecimal hexadecimal-string;
            }
            not-equals {
              ascii ascii-string;
              hexadecimal hexadecimal-string;
            }
            starts-with {
              ascii ascii-string;
              hexadecimal hexadecimal-string;
            }
          }
          delay-time seconds;
        }
        dual-stack dual-stack-group-name;
        interface-client-limit number;
        process-inform {
          pool pool-name;
        }
        rapid-commit;
      }
      service-profile dynamic-profile-name;
      short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
      trace;
      upto upto-interface-name;
    }
    liveness-detection {
      failure-action (clear-binding | clear-binding-if-interface-up | log-only);
      method {
        bfd {
          version (0 | 1 | automatic);
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
          detection-time {
            threshold milliseconds;
          }
          session-mode(automatic | multihop | singlehop);
          holddown-interval milliseconds;
        }
        layer2-liveness-detection {
          max-consecutive-retries number;
          transmit-interval interval;
        }
      }
    }
    overrides {
      asymmetric-lease-time seconds;
      asymmetric-prefix-lease-time seconds;
```

```
    client-discover-match <option60-and-option82>;
    client-negotiation-match incoming-interface;
    delay-advertise {
      based-on (option-15 | option-16 | option-18 | option-37) {
        equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        not-equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        starts-with {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
      }
      delay-time seconds;
    }
    delay-offer {
      based-on (option-60 | option-77 | option-82) {
        equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        not-equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        starts-with {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
      }
      delay-time seconds;
    }
    delegated-pool;
    delete-binding-on-renegotiation;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    protocol-attributes attribute-set-name;
    rapid-commit;
  }
  reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
      radius-disconnect;
    }
```

```
  }
  route-suppression;
  service-profile dynamic-profile-name;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

Hierarchy Level

```
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
  services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]
```

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Configure a group of interfaces that have a common configuration, such as authentication parameters. A group must contain at least one interface.

Options

group-name—Name of the group.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Extended DHCP Local Server Overview on page 562
- Grouping Interfaces with Common DHCP Configurations on page 670
- Using External AAA Authentication Services with DHCP on page 651
- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets on page 686

group (DHCP Relay Agent)

Syntax

```
group group-name {
  access-profile profile-name;
  active-server-group server-group-name;
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-description  (device-interface | logical-interface);
      interface-name interface-name;
      logical-system-name;
      mac-address mac-address;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
      vlan-tags;
    }
  }
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
  }
  forward-only {
    logical-system <current | default | logical-system-name>;
    routing-instance <current | default | routing-instance-name>;
  }
  interface interface-name {
    access-profile profile-name;
    exclude;
    liveness-detection {
      failure-action (clear-binding | clear-binding-if-interface-up | log-only);
      method {
        bfd {
          version (0 | 1 | automatic);
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
          detection-time {
            threshold milliseconds;
          }
          session-mode (automatic | multihop | singlehop);
          holddown-interval milliseconds;
```

```
        }
      }
    }
    overrides {
      allow-no-end-option;
      allow-snooped-clients;
      always-write-giaddr;
      always-write-option-82;
      asymmetric-lease-time seconds;
      asymmetric-prefix-lease-time seconds;
      client-discover-match <option60-and-option82 | incoming-interface>;
      client-negotiation-match incoming-interface;
      delay-authentication;
      delete-binding-on-renegotiation;
      disable-relay;
      dual-stack dual-stack-group-name;
      interface-client-limit number;
      layer2-unicast-replies;
      no-allow-snooped-clients;
      no-bind-on-request;
      proxy-mode;
      relay-source
      replace-ip-source-with;
      send-release-on-delete;
      trust-option-82;
    }
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    trace;
    upto upto-interface-name;
  }
  liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
      bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        detection-time {
          threshold milliseconds;
        }
        session-mode (automatic | multihop | singlehop);
        holddown-interval milliseconds;
      }
      layer2-liveness-detection {
        max-consecutive-retries number;
        transmit-interval interval;
      }
    }
```

```
}
overrides {
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-discover-match <option60-and-option82>;
    client-negotiation-match incoming-interface;
    disable-relay;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-bind-on-request;
    proxy-mode;
    relay-source
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
}
relay-agent-interface-id {
    include-irb-and-l2;
    keep-incoming-interface-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
    use-vlan-id;
}
relay-agent-remote-id {
    include-irb-and-l2;
    keep-incoming-remote-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
    use-vlan-id;
}
relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    equals (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
```

```
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
      }
    }
    relay-option-82 {
      circuit-id {
        prefix prefix;
        use-interface-description (logical | device);
        use-option-82;
      }
      remote-id {
        prefix prefix;
        use-interface-description (logical | device);
      }
      server-id-override
    }
    remote-id-mismatch disconnect;
    route-suppression;
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 8.3.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Specify the name of a group of interfaces that have a common DHCP or DHCPv6 relay agent configuration. A group must contain at least one interface. Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

Options

group-name—Name of a group of interfaces that have a common DHCP or DHCPv6 relay agent configuration.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618
- *Understanding the Extended DHCP Relay Agent for EX Series Switches*
- Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure) on page 611
- Configuring Group-Specific DHCP Relay Options on page 672
- Grouping Interfaces with Common DHCP Configurations on page 670
- Using External AAA Authentication Services with DHCP on page 651
- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets on page 686

group (System Services DHCP)

Syntax

```
group group-name {
  authentication {
    password password;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name;
      interface-name;
      logical-system-name;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix;
    }
  }
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
    junos-default-profile;
    use-primary dynamic-profile;
  }
  interface interface-name {
    dynamic-profile {
      profile-name;
      aggregate-clients {
        merge;
        replace;
      }
      junos-default-profile;
      use-primary dynamic-profile-name;
    }
    exclude;
    overrides {
      delegated-pool pool-name;
      interface-client-limit number;
      process-inform {
        pool pool-name;
      }
      rapid-commit ;
    }
    service-profile service-profile-name
    trace ;
    upto interface-name;
  }
  liveness-detection {
    failure-action {
```

```
        clear-binding;
        clear-binding-if-interface-up;
        log-only;
      }
      method {
        bfd {
          detection-time {
            threshold milliseconds;
          }
          holddown-interval interval;
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          session-mode (automatic | multihop | single-hop);
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
        version (0 | 1 | automatic);
      }
    }
    overrides {
      delegated-pool pool-name;
      interface-client-limit number;
      process-inform {
        pool pool-name;
      }
      rapid-commit ;
    }
    reconfigure {
      attempts number;
      clear-on-abort;
      strict;
      timeout number;
      token token-name;
      trigger {
        radius-disconnect;
      }
    }
    service-profile service-profile-name;
}
```

Hierarchy Level [edit system services dhcp-local-server dhcpv6]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure a group of interfaces that have a common configuration.

The remaining statements are explained separately. See CLI Explorer.

Options

- *group-name*—Name of the group.

NOTE: SRX Series devices do not support DHCP client authentication.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*
- DHCP Server Configuration Overview on page 719

eapol-block

Syntax

```
eapol-block {
  server-fail {
    seconds;
  }
  mac-radius;
  captive-portal;
}
```

Hierarchy Level

```
[edit protocols dot1x authenticator interface (interface-names)],
[edit protocols dot1x authenticator interface (all | [interface-names]) server-reject-vlan],
[edit protocols dot1x authenticator interface (all | [interface-names]) server-reject-vlan
  (vlan-id | vlan-name)]
```

Release Information

Statement introduced in Junos OS Release 11.2 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.
Support at the [**edit protocols dot1x authenticator interface** *interface-name*] hierarchy level introduced in Junos OS Releases 14.1X53-D40 and 15.1X53-D51 for EX Series switches.
Support for options **mac-radius** and **captive-portal** introduced in Junos OS Release 17.2R1.

Description

Enable the switch to ignore Extensible Authentication Protocol over LAN (EAPoL)-Start messages received from a client that has been authenticated so that the switch does not trigger re-authentication. The switch typically attempts to restart the authentication procedure by contacting the authentication server when it receives an EAPoL-Start message from a client—even for authenticated clients. You can configure the **eapol-block** statement to help prevent unnecessary downtime that can occur when the switch waits for a response from the authentication server.

If you configure the switch to block EAPol-Start messages, when the switch receives an EAPoL-Start message from an authenticated client, the switch ignores the message and does not attempt to contact the authentication server for reauthentication. The existing authentication session that was established for the client remains open.

The EAPoL-Start messages are blocked only if the client is in the authenticated state. EAPoL-Start messages from new clients are accepted.

Default

If the **eapol-block** statement is not configured, the switch attempts to contact the authentication server to authenticate the client when it receives an EAPoL-Start message.

Options

server-fail ***seconds***—Configure the switch to ignore EAP-Start messages received from a client that has been authenticated using server fail fallback or server reject VLAN methods. Configure the time interval, in seconds, during which the switch will not attempt to contact the authentication server to re-authenticate a client that has already been authenticated using server fail fallback.

Default: 120 seconds.

Range: 120 through 65,535 seconds.

mac-radius (EX4300 and EX9200 switches only)—Configure the switch to ignore EAP-Start messages received from a client that has been authenticated using MAC RADIUS authentication. The **mac-radius** option is also valid for clients authenticated using central Web authentication (CWA).

captive-portal (EX4300 and EX9200 switches only)—Configure the switch to ignore EAP-Start messages received from a client that has been authenticated using captive portal authentication.

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

Related Documentation
- block-interval on page 910
- Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 315

elin

Syntax
```
elin number;
```

Hierarchy Level
```
[edit protocols lldp-med interface (all | interface-name location)]
```

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

Description
For Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED), configure the Emergency Line Identification Number (ELIN) as location information. Location information is advertised from the switch to the MED device and is used during emergency calls to identify the location of the MED device.

Default
Disabled.

Options
number—Configure a 10-digit number (area code and telephone number).

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

Related Documentation
- show lldp on page 1826
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Configuring LLDP-MED (CLI Procedure) on page 521

encoding

Syntax

```
encoding (binary | pem);
```

Hierarchy Level

[edit security ike policy *ike-peer-address*],
[edit security certificates certification-authority *ca-profile-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

(Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file format used for the **local-certificate** and **local-key-pair** statements.

Options

binary—Binary file format.

pem—Privacy-enhanced mail (PEM), an ASCII base 64 encoded format.

Default: **binary**

Required Privilege Level

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

Related Documentation

- *Configuring the Type of Encoding Your CA Supports*
- *Configuring an IKE Policy for Digital Certificates for an ES PIC*

enhanced-accounting

Syntax

```
enhanced-accounting;
```

Hierarchy Level

```
[edit system radius-options]
[edit system tacplus-options],
```

Release Information Statement introduced in Junos OS Release 14.1.

Description Configure audit of TACACS+ or RADIUS authentication events such as access method, remote port, and access privileges.

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

Related Documentation

- radius-options on page 1379
- tacplus-options on page 1525
- Configuring RADIUS System Accounting on page 200
- Configuring TACACS+ System Accounting on page 219

enhanced-avs-max

Syntax enhanced-avs-max <*number*>;

Hierarchy Level [edit system accounting]

Release Information Statement introduced in Junos OS Release 14.1.

Description Configure the number of attribute values to be displayed.

Options <*number*>—Number of attribute values.
Range: 7 through 15
Default: 7

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

Related Documentation

- accounting on page 839
- enhanced-accounting on page 1076
- Configuring RADIUS System Accounting on page 200
- Configuring TACACS+ System Accounting on page 219

enrollment-retry

Syntax enrollment-retry *attempts*;

Hierarchy Level [edit security certificates]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify how many times a router or switch can resend a digital certificate request.

Options ***attempts***—Number of enrollment retries.

Range: 0 through 100

Default: 0

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

Related Documentation

- *Configuring the Number of Enrollment Retries*

enrollment-url

Syntax enrollment-url *url-name*;

Hierarchy Level [edit security certificates certification-authority *ca-profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify where your router or switch sends Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests (certificate authority URL).

Options *url-name*—Certificate authority URL.

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

Related Documentation
- *Specifying an Enrollment URL*

ethernet-switching-options

List of Syntax

EX Series on page 1080
QFX Series, QFabric, EX4600 on page 1083

EX Series

```
ethernet-switching-options {
  analyzer (Port Mirroring) {
    name {
      loss-priority priority;
      ratio number;
      input {
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
        egress {
          interface (all | interface-name);
        }
      }
      output {
        interface interface-name;
        vlan (vlan-id | vlan-name) {
        no-tag;
        }
      }
    }
  }
  bpdu-block {
    disable-timeout timeout;
    interface (all | [interface-name]) {
      (disable | drop | shutdown);
      }
  }
  dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100);
  }
  interfaces interface-name {
    no-mac-learning;
  }
  mac-lookup-length number-of-entries;
}
  mac-notification {
    notification-interval seconds;
  }
  mac-table-aging-time seconds;
  nonstop-bridging;
  port-error-disable {
    disable-timeout timeout;
  }
  redundant-trunk-group {
    group name {
      interface interface-name <primary>;
      interface interface-name;
```

```
    }
}
secure-access-port {
    dhcp-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    dhcpv6-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    interface (all | interface-name) {
        allowed-mac {
            mac-address-list;
        }
        (dhcp-trusted | no-dhcp-trusted);
        fcoe-trusted;
        mac-limit limit action (drop | log | none | shutdown);
        no-allowed-mac-log;
        persistent-learning;
        static-ip ip-address {
            vlan  vlan-name;
            mac mac-address;
        }
        static-ipv6 ip-address {
            vlan  vlan-name;
            mac mac-address;
        }
    }
    vlan (all | vlan-name) {
        (arp-inspection | no-arp-inspection) [
            forwarding-class class-name;
        }
        dhcp-option82 {
            circuit-id {
                prefix hostname;
                use-interface-description;
                use-vlan-id;
            }
            remote-id {
                prefix hostname | mac | none;
                use-interface-description;
                use-string string;
            }
            vendor-id [string];
        }
        (examine-dhcp | no-examine-dhcp) {
            forwarding-class class-name;
        }
        (examine-dhcpv6 | no-examine-dhcpv6) {
            forwarding-class class-name;
        }
        examine-fip {
```

```
        fc-map fc-map-value;
      }
      (ip-source-guard | no-ip-source-guard);
      (ipv6-source-guard | no-ipv6-source-guard);
      mac-move-limit limit action (drop | log | none | shutdown);
      }
      (neighbor-discovery-inspection | no-neighbor-discovery-inspection);
    no-option-37;
    static {
      vlan name {
        mac mac-address {
          next-hop interface-name;
        }
      }
    }
    storm-control {
      action-shutdown;
      interface (all | interface-name) {
        bandwidth bandwidth;
        level level;
        multicast;
        no-broadcast;
        no-multicast;
        no-registered-multicast;
        no-unknown-unicast;
        no-unregistered-multicast;
      }
    }
    traceoptions {
      file filename <files number> <no-stamp> <replace> <size size> <world-readable |
        no-world-readable>;
      flag flag <disable>;
    }
    unknown-unicast-forwarding {
      vlan (all | vlan-name) {
        interface interface-name;
      }
    }
    voip {
      interface (all | [interface-name | access-ports]) {
        vlan vlan-name;
        forwarding-class (assured-forwarding | best-effort | expedited-forwarding |
          network-control);
      }
    }
}
```

QFX Series, QFabric, EX4600

```
ethernet-switching-options {
  analyzer {
    name {
      input {
        egress {
          interface (all | interface-name);
        }
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
      output {
        interface interface-name;
        ip-address ip-address;
        vlan (vlan-id | vlan-name);
      }
    }
  }
  bpdu-block {
    interface (all | [interface-name]);
    disable-timeout timeout;
  }
  dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100)
  }
  interfaces interface-name {
    no-mac-learning;
  }
  mac-table-aging-time seconds {
  }
  port-error-disable {
    disable-timeout timeout;
  }
  secure-access-port {
    dhcp-snooping-file {
      location local_pathname | remote_URL;
      timeout seconds;
      write-interval seconds;
    }
    interface (all | interface-name) {
      allowed-mac {
        mac-address-list;
      }
      (dhcp-trusted | no-dhcp-trusted);
      fcoe-trusted;
      mac-limit limit action action;
      no-allowed-mac-log;
    }
    vlan (all | vlan-name) {
      (arp-inspection | no-arp-inspection) [
        forwarding-class (for DHCP Snooping or DAI Packets) class-name;
      }
      dhcp-option82 {
        circuit-id {
          prefix (Circuit ID for Option 82) hostname;
```

```
            use-interface-description;
            use-vlan-id;
          }
          remote-id {
            prefix (Remote ID for Option 82) hostname | mac | none;
            use-interface-description;
            use-string string;
          }
          vendor-id <string>;
        }
        (examine-dhcp | no-examine-dhcp) {
          forwarding-class (for DHCP Snooping or DAI Packets) class-name;
        }
        examine-fip {
          examine-vn2vn {
            beacon-period milliseconds;
          }
          fc-map fc-map-value;
        }
        mac-move-limit limit <fabric-limit limit action action;
      }
    }
    static {
      vlan vlan-id {
        mac mac-address next-hop interface-name;
      }
    }
    storm-control {
      interface (all | interface-name) {
        bandwidth bandwidth;
        no-broadcast;
        no-multicast;
        no-unknown-unicast;
      }
    }
    traceoptions {
      file filename <files number> <no-stamp> <replace> <size size> <world-readable |
        no-world-readable>;
      flag flag <disable>;
    }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure Ethernet switching options.

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation
- *Understanding Port Mirroring*
- *Understanding How to Protect Access Ports from Common Attacks*
- *Port Security Features*
- *Understanding BPDU Protection for STP, RSTP, and MSTP*
- *Understanding Redundant Trunk Links (Legacy RTG Configuration)*
- *Understanding Storm Control*
- Understanding 802.1X and VoIP on EX Series Switches on page 406
- *Understanding Q-in-Q Tunneling and VLAN Translation*
- *Understanding and Preventing Unknown Unicast Forwarding*
- *Understanding MAC Notification on EX Series Switches*
- *Understanding FIP Snooping*
- *Understanding Nonstop Bridging on EX Series Switches*

events

Syntax
```
events (change-log | interactive-commands | login);
```

Hierarchy Level
```
[edit system accounting]
```

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 types of events to track and log.

Options
change-log—Audit configuration changes.

interactive-commands—Audit interactive commands (any command-line input).

login—Audit logins.

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

Related Documentation
- Specifying TACACS+ Auditing and Accounting Events on page 220

exclude (RADIUS Attributes)

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 ];
  acc-loop-encap [ access-request | accounting-start | accounting-stop ];
  acc-loop-remote-id [ access-request | accounting-start | accounting-stop ];
  accounting-authentic [ accounting-off | accounting-on | accounting-start | accounting-stop
    ]
  accounting-delay-time [ accounting-off | accounting-on | accounting-start |
    accounting-stop ];
  accounting-session-id access-request;
  accounting-terminate-cause accounting-off;
  acct-request-reason [ accounting-start | accounting-stop ];
  acct-tunnel-connection [ access-request | accounting-start | accounting-stop ];
  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 ];
  chargeable-user-identity access-request;
  class [ accounting-start | accounting-stop ];
  cos-shaping-rate [ accounting-start | accounting-stop ];
  delegated-ipv6-prefix [ accounting-start | accounting-stop ];
  dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
  dhcp-header access-request;
  dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
  dhcp-options [ access-request | accounting-start | accounting-stop ];
  dhcpv6-header access-request;
  dhcpv6-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 ];
  dynamic-iflset-name [ accounting-start | accounting-stop ];
  event-timestamp [ accounting-off | accounting-on | accounting-start | accounting-stop
    ];
  filter-id [ accounting-start | accounting-stop ];
  first-relay-ipv4-address [ access-request | accounting-start | accounting-stop ];
  first-relay-ipv6-address [ access-request | accounting-start | accounting-stop ];
  framed-interface-id [ access-request | accounting-start | accounting-stop ];
  framed-ip-address [ access-request | accounting-start | accounting-stop ];
  framed-ip-netmask [ access-request | accounting-start | accounting-stop ];
  framed-ip-route [ accounting-start | accounting-stop ];
  framed-ipv6-address [ access-request | accounting-start | accounting-stop ];
  framed-ipv6-pool [ accounting-start | accounting-stop ];
  framed-ipv6-prefix [ accounting-start | accounting-stop ];
  framed-ipv6-route [ accounting-start | accounting-stop ];
```

```
    framed-pool [ accounting-start | accounting-stop ]; input-ipv6-gigawords accounting-stop;
    input-filter [ accounting-start | accounting-stop ];
    input-gigapackets accounting-stop;
    input-gigawords accounting-stop;
    input-ipv6-octets accounting-stop;
    input-ipv6-packets accounting-stop;
    interface-description [ access-request | accounting-start | accounting-stop ];
    l2c-downstream-data [ access-request | accounting-start | accounting-stop ];
    l2c-upstream-data [ access-request | accounting-start | accounting-stop ];
    l2tp-rx-connect-speed [ access-request | accounting-start | accounting-stop ];
    l2tp-tx-connect-speed [ 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-off | accounting-on | 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;
    output-ipv6-gigawords accounting-stop;
    output-ipv6-octets accounting-stop;
    output-ipv6-packets accounting-stop;
    pppoe-description [ access-request | accounting-start | accounting-stop ];
    standard-attribute number {
      packet-type [ access-request | accounting-off | accounting-on | accounting-start |
        accounting-stop ];
    }
    tunnel-assignment-id [ access-request | accounting-start | accounting-stop ];
    tunnel-client-auth-id [ access-request | accounting-start | accounting-stop ];
    tunnel-client-endpoint [ access-request | accounting-start | accounting-stop ];
    tunnel-medium-type [ access-request | accounting-start | accounting-stop ];
    tunnel-server-auth-id [ access-request | accounting-start | accounting-stop ];
    tunnel-server-endpoint [ access-request | accounting-start | accounting-stop ];
    tunnel-type [ access-request | accounting-start | accounting-stop ];
    upstream-calculated-qos-rate [ access-request | accounting-start | accounting-stop ];
    vendor-id id-number {
      vendor-attribute vsa-number {
        packet-type [ access-request | accounting-off | accounting-on | accounting-start |
          accounting-stop ];
      }
    }
    virtual-router [ 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.
downstream-calculated-qos-rate, **dsl-forum-attributes**, and **upstream-calculated-qos-rate** options added in Junos OS Release 11.4.
cos-shaping-rate and **filter-id** options added in Junos OS Release 13.2.
pppoe-description option added in Junos OS Release 14.2.
virtual-router option added in Junos OS Release 15.1.
first-relay-ipv4-address and **first-relay-ipv6-address** options added in Junos OS Release 16.1.
acc-loop-encap and **acc-loop-remote-id** options added in Junos OS Release 16.1R4.
access-request option support for all tunnel attributes added in Junos OS Release 15.1R7, 16.1R5, 16.2R2, 17.1R2, 17.2R2, and 17.3R1 for MX Series.
packet-type, **standard-attribute**, **vendor-attribute**, and **vendor-id** options added in Junos OS Release 18.1R1.

Description Configure the router or switch to exclude the specified attributes from being sent in the specified type of RADIUS message. Exclusion can be useful, for example, for attributes that do not change values over the lifetime of a subscriber. By not sending these attributes, you reduce the packet size without losing information. Contrast this behavior with that provided by the **ignore** statement.

You can specify attribute exclusion for multiple RADIUS message types by enclosing the message types, separated by spaces, within brackets ([ ]). You do not need brackets when specifying a single message type.

Starting in Junos OS Release 18.1R1, you can specify standard RADIUS attributes with the attribute number. You can specify VSAs with the IANA-assigned vendor ID and the VSA number. With this flexible configuration method, you can configure any standard attribute and VSA supported by your platform to be excluded. The configuration has no effect if you configure unsupported attributes, vendors, and VSAs.

The legacy method allows you to configure only those attributes and VSAs for which the statement syntax includes a specific option. Consequently, you can use the legacy method to exclude only a subset of all attributes that can be received in Access-Accept messages.

Not all attributes are available in all types of RADIUS messages.

NOTE: If you exclude an attribute from Acct-Off messages, the attributes are then excluded from Interim-Acct messages.

NOTE: VSAs with dedicated option names include Juniper Networks (IANA vendor ID 4874) and DSL Forum (vendor ID 3561) VSAs.

Options RADIUS attribute—RADIUS standard attribute or VSA:

- **acc-aggr-cir-id-asc**—Exclude Juniper Networks VSA 26-112, Acc-Aggr-Cir-Id-Asc.
- **acc-aggr-cir-id-bin**—Exclude Juniper Networks VSA 26-111, Acc-Aggr-Cir-Id-Bin.
- **acc-loop-cir-id**—Exclude Juniper Networks VSA 26-110, Acc-Loop-Cir-Id.
- **acc-loop-encap**—Exclude Juniper Networks VSA 26-183, Acc-Loop-Encap.
- **acc-loop-remote-id**—Exclude Juniper Networks VSA 26-182, Acc-Loop-Remote-Id.
- **accounting-authentic**—Exclude RADIUS attribute 45, Acct-Authentic.
- **accounting-delay-time**—Exclude RADIUS attribute 41, Acct-Delay-Time.
- **accounting-session-id**—Exclude RADIUS attribute 44, Acct-Session-Id.
- **accounting-terminate-cause**—Exclude RADIUS attribute 49, Acct-Terminate-Cause.
- **acct-request-reason**—Exclude Juniper Networks VSA 26-210, Acct-Request-Reason.
- **acct-tunnel-connection**—Exclude RADIUS attribute 68, Acct-Tunnel-Connection.
- **act-data-rate-dn**—Exclude Juniper Networks VSA 26-114, Act-Data-Rate-Dn.
- **act-data-rate-up**—Exclude Juniper Networks VSA 26-113, Act-Data-Rate-Up.
- **act-interlv-delay-dn**—Exclude Juniper Networks VSA 26-126, Act-Interlv-Delay-Dn.
- **act-interlv-delay-up**—Exclude Juniper Networks VSA 26-124, Act-Interlv-Delay-Up.
- **att-data-rate-dn**—Exclude Juniper Networks VSA 26-118, Att-Data-Rate-Dn.
- **att-data-rate-up**—Exclude Juniper Networks VSA 26-117, Att-Data-Rate-Up.
- **called-station-id**—Exclude RADIUS attribute 30, Called-Station-Id.
- **calling-station-id**—Exclude RADIUS attribute 31, Calling-Station-Id.
- **chargeable-user-identity**—Exclude RADIUS attribute 89, Chargeable-User-Identity.
- **class**—Exclude RADIUS attribute 25, Class.
- **cos-shaping-rate**—Exclude Juniper Networks VSA 26-177, Cos-Shaping-Rate.
- **delegated-ipv6-prefix**—Exclude RADIUS attribute 123, Delegated-IPv6-Prefix.
- **dhcp-gi-address**—Exclude Juniper Networks VSA 26-57, DHCP-GI-Address.
- **dhcp-header**—Exclude Juniper Networks VSA 26-208, DHCP-Header.
- **dhcp-mac-address**—Exclude Juniper Networks VSA 26-56, DHCP-MAC-Address.
- **dhcp-options**—Exclude Juniper Networks VSA 26-55, DHCP-Options.
- **dhcpv6-header**—Exclude Juniper Networks VSA 26-209, DHCPv6-Header.
- **dhcpv6-options**—Exclude Juniper Networks VSA 26-207, DHCPv6-Options.
- **dynamic-iflset-name**—Exclude Juniper Networks VSA 26-130, Qos-Set-Name.
- **downstream-calculated-qos-rate**—Exclude Juniper Networks VSA 26-141.

- **dsl-forum-attributes**—Exclude DSL Forum VSA (vendor ID 3561) as described in RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*.
- **dsl-line-state**—Exclude Juniper Networks VSA 26-127, DSL-Line-State.
- **dsl-type**—Exclude Juniper Networks VSA 26-128, DSL-Type.
- **event-timestamp**—Exclude RADIUS attribute 55, Event-Timestamp.
- **filter-id**—Exclude RADIUS attribute 11, Filter-Id.
- **first-relay-ipv4-address** —Exclude Juniper Networks VSA 26-189, DHCP-First-Relay-IPv4-Address.
- **first-relay-ipv6-address** —Exclude Juniper Networks VSA 26-190, DHCP-First-Relay-IPv6-Address.
- **framed-interface-id**—Exclude RADIUS attribute 96, Framed-Interface-ID.
- **framed-ip-address**—Exclude RADIUS attribute 8, Framed-IP-Address.
- **framed-ip-netmask**—Exclude RADIUS attribute 9, Framed-IP-Netmask.
- **framed-ip-route**—Exclude RADIUS attribute 22, Framed-Route.
- **framed-ipv6-address**—Exclude RADIUS attribute 168, Framed-IPv6-Address.
- **framed-ipv6-pool**—Exclude RADIUS attribute 100, Framed-IPv6-Pool.
- **framed-ipv6-prefix**—Exclude RADIUS attribute 97, Framed-IPv6-Prefix.
- **framed-ipv6-route**—Exclude RADIUS attribute 99, Framed-IPv6-Route.
- **framed-pool**—Exclude RADIUS attribute 88, Framed-Pool.
- **input-filter**—Exclude Juniper Networks VSA 26-10, Ingress-Policy-Name.
- **input-gigapackets**—Exclude Juniper Networks VSA 26-42, Acct-Input-Gigapackets.
- **input-gigawords**—Exclude RADIUS attribute 52, Acct-Input-Gigawords.
- **input-ipv6-gigawords**—Exclude Juniper Networks VSA 26-155, Acct-Input-IPv6-Gigawords.
- **input-ipv6-octets**—Exclude Juniper Networks VSA 26-151, Acct-Input-IPv6-Octets.
- **input-ipv6-packets**—Exclude Juniper Networks VSA 26-153, Acct-Input-IPv6-Packets.
- **interface-description**—Exclude Juniper Networks VSA 26-53, Interface-Desc.
- **l2c-downstream-data**—Exclude Juniper Networks VSA 26-93, L2C-Down-Stream-Data.
- **l2c-upstream-data**—Exclude Juniper Networks VSA 26-92, L2C-Up-Stream-Data.
- **l2tp-rx-connect-speed**—Exclude Juniper Networks VSA 26-163, Rx-Connect-Speed.
- **l2tp-tx-connect-speed**—Exclude Juniper Networks VSA 26-162, Tx-Connect-Speed.
- **max-data-rate-dn**—Exclude Juniper Networks VSA 26-120, Max-Data-Rate-Dn.
- **max-data-rate-up**—Exclude Juniper Networks VSA 26-119, Max-Data-Rate-Up.
- **max-interlv-delay-dn**—Exclude Juniper Networks VSA 26-125, Max-Interlv-Delay-Dn.

- **max-interlv-delay-up**—Exclude Juniper Networks VSA 26-123, Max-Interlv-Delay-Up.
- **min-data-rate-dn**—Exclude Juniper Networks VSA 26-116, Min-Data-Rate-Dn.
- **min-data-rate-up**—Exclude Juniper Networks VSA 26-115, Min-Data-Rate-Up.
- **min-lp-data-rate-dn**—Exclude Juniper Networks VSA 26-122, Min-Lp-Data-Rate-Dn.
- **min-lp-data-rate-up**—Exclude Juniper Networks VSA 26-121, Min-Lp-Data-Rate-Up.
- **nas-identifier**—Exclude RADIUS attribute 32, NAS-Identifier.
- **nas-port**—Exclude RADIUS attribute 5, NAS-Port.
- **nas-port-id**—Exclude RADIUS attribute 87, NAS-Port-Id.
- **nas-port-type**—Exclude RADIUS attribute 61, NAS-Port-Type.
- **output-filter**—Exclude Juniper Networks VSA 26-11, Egress-Policy-Name.
- **output-gigapackets**—Exclude Juniper Networks VSA 26-43, Acct-Output-Gigapackets.
- **output-gigawords**—Exclude RADIUS attribute 53, Acct-Output-Gigawords.
- **output-ipv6-gigawords**—Exclude Juniper Networks VSA 26-156, Acct-Output-IPv6-Gigawords.
- **output-ipv6-octets**—Exclude Juniper Networks VSA 26-152, Acct-Output-IPv6-Octets.
- **output-ipv6-packets**—Exclude Juniper Networks VSA 26-154, Acct-Output-IPv6-Packets.
- **packet-type**—Specify the RADIUS message type to exclude; term required when excluding a standard attribute or VSA by number rather than name. You can enclose multiple values in square brackets to specify a list of message types. Message types include Access-Request, Accounting-Off, Accounting-Off, Accounting-Start, and Accounting-Stop.
- **pppoe-description**—Exclude Juniper Networks VSA 26-24, PPPoE-Description.
- **standard-attribute** ***number***—RADIUS standard attribute number supported by your platform. If you configure an unsupported attribute, that configuration has no effect. When you use this option, you must use the **packet-type** term to specify the message from which the attribute is excluded.
- **tunnel-assignment-id**—Exclude RADIUS attribute 82, Tunnel-Assignment-ID.
- **tunnel-client-auth-id**—Exclude RADIUS attribute 90. Tunnel-Client-Auth-ID.
- **tunnel-client-endpoint**—Exclude RADIUS attribute 66, Tunnel-Client-Endpoint.
- **tunnel-medium-type**—Exclude RADIUS attribute 65, Tunnel-Medium-Type.
- **tunnel-server-auth-id**—Exclude RADIUS attribute 91, Tunnel-Server-Auth-ID.
- **tunnel-server-endpoint**—Exclude RADIUS attribute 67, Tunnel-Server-Endpoint.
- **tunnel-type**—Exclude RADIUS attribute 64, Tunnel-Type.
- **upstream-calculated-qos-rate**—Exclude Juniper Networks VSA 26-142

- **vendor-attribute** ***vsa-number***—Number identifying a VSA belonging to the specified vendor; both must be supported by your platform. If you configure an unsupported VSA, that configuration has no effect. When you use this option, you must use the **packet-type** term to specify the message from which the attribute is excluded.
- **vendor-id** ***id-number***—IANA vendor ID supported by your platform. If you configure an unsupported vendor ID, that configuration has no effect.
- **virtual-router**—Exclude Juniper Networks VSA 26-1.

RADIUS message type:

- **access-request**—RADIUS Access-Request 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

- *Filtering RADIUS Attributes and VSAs from RADIUS Messages*
- *RADIUS Servers and Parameters for Subscriber Access*
- *Standard and Vendor-Specific RADIUS Attributes*

excluded-address

Syntax

```
excluded-address;
```

Hierarchy Level

```
[edit access address assignment-address pool]
```

Release Information

Statement introduced in Junos OS Release 15.1X49-D20.

Description

Allows you to exclude select IPv4 or IPv6 addresses from a DHCP address pool. Within a configured address pool, you can specifically exclude up to 20 addresses. Junos OS will not assign these excluded addresses to any clients. If you configure an excluded address that has already been assigned to a DHCP client, that excluded address will be revoked from the client.

NOTE: Excluded addresses must match the address family of the configured address pool. For example, you cannot exclude an IPv4 address within an IPv6 address pool.

Required Privilege Level

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

Related Documentation

- address-assignment (Access) on page 852

external-authority

Syntax

```
external-authority;
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server pool-match-order],
[edit logical-systems *logical-system-name* system services dhcp-local-server pool-match-order],
[edit routing-instances *routing-instance-name* system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that an external authority (for example, RADIUS or Diameter) provides the address assignment.

When RADIUS is the external authority, the router uses the Framed-IPv6-Pool attribute (RADIUS attribute 100) to select the pool. When Diameter is the external authority, the router uses the Diameter counterpart of RADIUS Framed-IPv6-Pool attribute.

Required Privilege Level

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

Related Documentation

- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 701
- Extended DHCP Local Server Overview on page 562
- *Address-Assignment Pools Overview*

failure-action

Syntax

```
failure-action (clear-binding | clear-binding-if-interface-up | log-only);
```

Hierarchy Level

[edit system services dhcp-local-server liveness-detection],
[edit system services dhcp-local-server dhcpv6 liveness-detection],
[edit forwarding-options dhcp-relay liveness-detection],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection],
[edit system services dhcp-local-server group *group-name* liveness-detection],
[edit system services dhcp-local-server dhcpv6 group *group-name* liveness-detection],
[edit forwarding-options dhcp-relay group *group-name* liveness-detection],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name* liveness-detection]

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the action the router (or switch) takes when a liveness detection failure occurs.

Options

Default: clear-binding

clear-binding—The DHCP client session is cleared when a liveness detection failure occurs, except when **maintain-subscribers interface-delete** setting is configured and active.

clear-binding-if-interface-up—The DHCP client session is cleared only when a liveness detection failure occurs and the local interface is detected as being up. Use this setting to distinguish failures from between a liveness detection failure due to a local network error, and a host disconnecting from the network. If the client binding is in the maintain-binding Finite State Machine (FSM) state when the liveness detection failure detection occurs, then the binding is not deleted. Not supported for Layer 2 ARP/ND liveness detection on MX Series routers.

log-only—A message is logged to indicate the event; no action is taken and DHCP is left to manage the failure and maintain the client binding. Not supported for Layer 2 ARP/ND liveness detection on MX Series routers.

Required Privilege Level

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

Related Documentation

- DHCP Liveness Detection Overview on page 674
- Configuring Detection of DHCP Local Server Client Connectivity with BFD on page 680
- Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD on page 675
- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682

- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677

family (Security Forwarding Options)

Syntax

```
family {
  inet6 {
    mode (drop | flow-based | packet-based);
  }
  iso {
    mode packet-based;
  }
  mpls {
    mode packet-based;
  }
}
```

Hierarchy Level

```
[edit security forwarding-options]
```

Release Information Statement introduced in Junos OS Release 8.5 .

Description Determine the protocol family to be used for packet forwarding.

NOTE: Packet-based processing is not supported on the following SRX Series devices: SRX5400, SRX5600, and SRX5800.

Options The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation

- *MPLS Overview*

falling-threshold (Health Monitor)

Syntax falling-threshold *percentage*;

Hierarchy Level [edit snmp health-monitor]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Set the lower threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options ***percentage***—Lower threshold for the alarm entry.

Range: 1 through 100

Default: 70 percent of the maximum possible value

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

Related Documentation

- rising-threshold on page 1432
- *Configuring Health Monitoring*

fast-start (LLDP-MED)

Syntax fast-start *count*;

Hierarchy Level [edit protocols lldp-med]

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

Description Configure the number of Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) advertisements sent from the switch in the first second after it has detected an LLDP-MED device (such as an IP telephone).

Options **count**—Number of advertisements.
Range: 1 through 10
Default: 3

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

Related Documentation

- show lldp on page 1826
- Configuring LLDP-MED (CLI Procedure) on page 521
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

fields (for Interface Profiles)

Syntax

```
fields {
  field-name;
}
```

Hierarchy Level

[edit accounting-options interface-profile *profile-name*]

Release Information

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

Description

Statistics to collect in an accounting-data log file for an interface.

Options

field-name—Name of the field:

- **input-bytes**—Input bytes
- **input-errors**—Generic input error packets
- **input-multicast**—Input packets arriving by multicast
- **input-packets**—Input packets
- **input-unicast**—Input unicast packets
- **output-bytes**—Output bytes
- **output-errors**—Generic output error packets
- **output-multicast**—Output packets sent by multicast
- **output-packets**—Output packets
- **output-unicast**—Output unicast packets

Required Privilege Level

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

Related Documentation

- *Configuring the Interface Profile*

file

Syntax file *certificate-filename*;

Hierarchy Level [edit security certificates certification-authority *ca-profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file from which to read the digital certificate.

Options *certificate-filename*—File from which to read the digital certificate.

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

Related Documentation
- *Specifying a File to Read the Digital Certificate*

file (Associating with a Profile)

Syntax

```
file filename;
```

Hierarchy Level

```
[edit accounting-options class-usage-profile profile-name],
[edit accounting-options filter-profile profile-name],
[edit accounting-options interface-profile profile-name],
[edit accounting-options mib-profile profile-name],
[edit accounting-options routing-engine-profile profile-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
The **[edit accounting-options mib-profile *profile-name*]** hierarchy added in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series Switches.

Description

Specify the accounting log file associated with the profile.

Options

filename—Name of the log file. You must specify a filename already configured in the **file** statement at the **[edit accounting-options]** hierarchy level.

Required Privilege Level

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

Related Documentation

- *Configuring the Interface Profile*
- *Configuring the Filter Profile*
- *Configuring the MIB Profile*
- *Configuring the Routing Engine Profile*

file (Configuring a Log File)

Syntax

```
file filename {
  archive-sites {
    site-name;
  }
  backup-on-failure (master-and-slave | master-only);
  compress;
  files number;
  nonpersistent;
  push-backup-to-master;
  size bytes;
  start-time time;
  transfer-interval minutes;
}
```

Hierarchy Level

```
[edit accounting-options]
```

Release Information

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

Description

Specify a log file to be used for accounting data.

Options

filename—Name of the file in which to write accounting data.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring Accounting-Data Log Files*
- *Configuring Flat-File Accounting for Layer 2 Wholesale*
- *Configuring Flat-File Accounting for Extensible Subscriber Services Management*
- *Flat-File Accounting Overview*

file (System Logging)

Syntax

```
file name {
  allow-duplicates;
  archive name password password routing-instance routing-instance <(binary-data |
    no-binary-data)> <files files> <size bytes> <start-time start-time> <transfer-interval
    minutes> <(world-readable | no-world-readable)>;
  contents (any | authorization | change-log | conflict-log | daemon | dfc | external | firewall
    | ftp | interactive-commands | kernel | local0 | lpr | mail | news | ntp | pfe | privileged |
    security | syslog | user | uucp) {
  }
  explicit-priority;
  match match;
  match-strings [ match-strings ... ];
  structured-data (brief | detail);
}
```

Hierarchy Level

```
[edit system syslog]
```

Release Information Statement introduced before Junos OS Release 12.1X47 for SRX Series.

Description Specify the file in which to log data.

Options

- *filename*—Specify the name of the file in which to log data.
- *allow-duplicates*—Do not suppress the repeated messages.
- *any*—Specify all facilities information.
  - *alert*—Specify the conditions that should be corrected immediately.
  - *critical*—Specify the critical conditions.
  - *emergency*—Specify the conditions that cause security functions to stop.
  - *error*—Specify the general error conditions.
  - *info*—Specify the information about normal security operations.
  - *none*—Do not specify any messages.
  - *notice*—Specify the conditions that should be handled specifically.
  - *warning*—Specify the general warning conditions.
- *archive*—Specify the archive file information.
  - *archive-sites*—Specify a list of destination URLs for the archived log files.
    - *url*—Specify the primary and failover URLs to receive archive files.
  - *binary-data*—Mark file such that it contains binary data.
  - *no-binary-data*—Do not mark the file such that it contains binary data.

    - *files*—Specify the number of files to be archived. Range: 1 through 1000 files.
    - *size*—Specify the size of files to be archived. Range: 65,536 through 1,073,741,824 bytes.
    - *world-readable*—Allow any user to read the log file.
    - *no-world-readable*—Do not allow any user to read the log file.
    - *start-time*—Specify the start time for file transmission. Enter the start time in the yyyy-mm-dd.hh:mm format.
    - *transfer-interval*—Specify the frequency at which to transfer the files to archive sites.
- *authorization*—Specify the authorization system.
- *change-log*—Specify the configuration change log.
- *conflict-log*—Specify the configuration conflict log.
- *daemon*—Specify the various system processes.
- *dfc*—Specify the dynamic flow capture.
- *explicit-priority*—Include the priority and facility in messages.
- *external*—Specify the local external applications.
- *firewall*—Specify the firewall filtering system.
- *ftp*—Specify the FTP process.
- *interactive-commands*—Specify the commands executed by the UI.
- *kernel*—Specify the kernel information.
- *match*—Specify the regular expression for lines to be logged.
- *ntp*—Specify the NTP process.
- *pfe*—Specify the Packet Forwarding Engine.
- *security*—Specify the security-related information.
- *structured-data*—Log the messages in structured log format.
    - *brief*—Omit English language text from the end of the logged message.
- *user*—Specify the user processes.
    - *info*—Specify the informational messages.

Required Privilege Level

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

files

Syntax files *number*;

Hierarchy Level [edit accounting-options file *filename*]

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 maximum number of log files to be used for accounting data.

Options ***number***—The maximum number of files. When a log file (for example, **profilelog**) reaches its maximum size, it is renamed **profilelog.0**, then **profilelog.1**, and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. The minimum value for ***number*** is 3 and the default value is 10.

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

Related Documentation

- *Configuring Accounting-Data Log Files*

filter-duplicates

Syntax filter-duplicates;

Hierarchy Level [edit snmp]

Release Information Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Filter duplicate **Get**, **GetNext**, or **GetBulk** SNMP requests.

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

Related Documentation

- *Filtering Duplicate SNMP Requests*
- *Understanding the Implementation of SNMP on the QFabric System*
- *Example: Configuring SNMP*

filter-profile

Syntax

```
filter-profile profile-name {
  counters {
    counter-name;
  }
  file filename;
  interval minutes;
}
```

Hierarchy Level

```
[edit accounting-options]
```

Release Information

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

Description

Create a profile to filter and collect packet and byte count statistics and write them to a file in the **/var/log** directory. To apply the profile to a firewall filter, you include the **accounting-profile** statement at the **[edit firewall filter *filter-name*]** hierarchy level. For more information about firewall filters, see *Firewall Filters Overview*.

Options

profile-name—Name of the filter profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Firewall Filters Overview*
- *Configuring the Filter Profile*

filter-profile

Syntax

```
filter-profile profile-name {
  counters {
    counter-name;
  }
  file filename;
  interval minutes;
}
```

Hierarchy Level

```
[edit accounting-options]
```

Release Information

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

Description

Create a profile to filter and collect packet and byte count statistics and write them to a file in the **/var/log** directory. To apply the profile to a firewall filter, you include the **accounting-profile** statement at the **[edit firewall filter *filter-name*]** hierarchy level. For more information about firewall filters, see *Firewall Filters Overview*.

Options

profile-name—Name of the filter profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Firewall Filters Overview*
- *Configuring the Filter Profile*

finger

Syntax

```
finger {
  connection-limit limit;
  rate-limit limit;
}
```

Hierarchy Level

[edit system services]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Allow finger requests from remote systems to the local router.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring Finger Service for Remote Access to the Router on page 231

fingerprint-hash

Syntax fingerprint-hash (md5 | sha2-256);

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 16.1.

Description Configure the hash algorithm used by the SSH server when it displays key fingerprints.

Options **md5**—Enable the SSH server to use the MD5 algorithm.

sha2-256—Enable the SSH server to use the sha2-256 algorithm. The default is sha2-256.

NOTE: **The FIPS image does not permit the use of MD5 fingerprints. On systems in FIPS mode, sha2-256 is the only available option.**

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

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 232

flow-tap-dtcp

Syntax

```
flow-tap-dtcp {
  ssh {
    connection-limit limit;
    rate-limit limit;
  }
}
```

Hierarchy Level

[edit system services]

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Configure Dynamic Tasking Control Protocol (DTCP) sessions to run over SSH in support of the flow-tap, FlowTapLite, or radius-flow-tap services. Note that the flow-tap feature is not supported on outbound, or egress, traffic. Only inbound, or ingress, traffic is supported.

This statement is required for DTCP-initiated subscriber secure policy mirroring (radius-flow-tap service).

Options

connection-limit *limit*—(Optional) Maximum number of connections allowed.

Range: 1 through 250

Default: 75

rate-limit *limit*— (Optional) Maximum number of connection attempts allowed per minute.

Range: 1 through 250

Default: 150

Required Privilege Level

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

Related Documentation

- *Configuring a DTCP-over-SSH Connection to the Mediation Device*
- *Configuring Flow-Tap Security Properties on MX, M and T Series Routers*
- *Configuring FlowTapLite on MX Series Routers and M320 Routers with FPCs*
- *Configuring DTCP-over-SSH Service for the Flow-Tap Application*

force-discover (dhcp-client)

Syntax

```
force-discover ;
```

Hierarchy Level

[edit interfaces *interface-name* unit *logical-unit-number* dhcp-client force-discover]

Release Information

Statement introduced in Junos OS Release 15.1X49-D80.
Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option **dhcp-clinet** at **[edit interfaces interface-name unit logical-unit-number family inet]** hierarchy is changed to **dhcp** to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option **dhcp**.

Description

Forces the DHCP client to send a DHCP discover packet after one to three failed **dhcp-request** attempts. The **force-discover** option ensures that the DHCP server will assign the same or a new IP address to the client.

Required Privilege Level

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

Related Documentation

- Configuring Optional DHCP Client Attributes on page 735
- Minimum DHCP Client Configuration on page 734

format (System Login)

Syntax
```
format ( md5 | sha1 | sha256 | sha512);
```

Syntax (Junos OS Evolved)
```
format ( md5 | sha256 | sha512);
```

Hierarchy Level
```
[edit system login password]
```

Release Information
Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Option **sha1** is not supported in Junos OS Evolved.

Description
Configure the authentication algorithm for plain-text passwords.

Default
For Junos OS, the default encryption format is **md5**. For Junos-FIPS software, the default encryption format is **sha1**.

Options
The hash algorithm that authenticates the password can be one of these algorithms:

- **md5**—Produces a 128-bit digest.
- **sha1**—Produces a 160-bit digest. The option sha1 is not supported in Junos OS Evolved.
- **sha256**—Produces a 256-bit digest.
- **sha512**—Produces a 512-bit digest.

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

forward-snooped-clients (DHCP Local Server)

Syntax

```
forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
  services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]
```

Release Information

Statement introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure how the DHCP local server filters and handles DHCP snooped packets on the specified interfaces.

Options

all-interfaces—Perform the action on all interfaces.

configured-interfaces—Perform the action only on interfaces that are configured as part of an interface group.

non-configured-interfaces—Perform the action only on interfaces that are not configured as part of a group.

Required Privilege Level

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

Related Documentation

- DHCP Snooping Support on page 706
- *Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server*

forward-snooped-clients (DHCP Relay Agent)

Syntax

```
forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit logical-systems logical-system-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay]
```

Release Information

Statement introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [**edit forwarding-options dhcp-relay dhcpv6**] hierarchy level introduced in Junos OS Release 15.1X53-D56 for EX Series switches and Junos OS Release 17.1R1.

Description

Configure how DHCP relay agent filters and handles DHCP snooped packets on the specified interfaces. The router or switch determines the DHCP snooping action to perform based on a combination of the **forward-snooped-clients** configuration and the configuration of either the **allow-snooped-clients** statement or the **no-allow-snooped-clients** statement.

The router (or switch) also uses this statement to determine how to handle snooped BOOTREPLY packets received on non-configured interfaces.

Options

all-interfaces—Perform the action on all interfaces.

Default: On EX Series switches, the action is performed on all interfaces by default.

configured-interfaces—Perform the action only on interfaces that are configured as part of an interface group.

non-configured-interfaces—Perform the action only on interfaces that are not part of a group.

Required Privilege Level

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

Related Documentation

- DHCP Snooping Support on page 706
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent on page 710

forwarding-class (VoIP)

Syntax

```
forwarding-class <assured-forwarding | best-effort | expedited-forwarding |network-control>;
```

Hierarchy Level

```
[edit ethernet-switching-options voip interface <all | interface-name | access-ports]>
```

```
[edit switch-options voip interface <all | interface-name | access-ports]>
```

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

Description For EX Series switches, configure the forwarding class used to handle packets on the VoIP interface.

NOTE: The **forwarding-class** statement at the **[edit ethernet-switching-options voip interface *interface-name*]** hierarchy level is used only by LLDP-MED for advertising capabilities VoIP phones. It is not used to classify VoIP traffic.

Default Disabled.

Options *class*—Forwarding class:

- **assured-forwarding**— Assured forwarding (AF)—Provides a group of values you can define and includes four subclasses: AF1, AF2, AF3, and AF4, each with three drop probabilities: low, medium, and high.
- **best-effort**—Provides no service profile. For the best effort forwarding class, loss priority is typically not carried in a class-of-service (CoS) value, and random early detection (RED) drop profiles are more aggressive.
- **expedited-forwading**—Provides a low loss, low latency, low jitter, assured bandwidth, end-to-end service.
- **network-control**—Provides a typically high priority because it supports protocol control.

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

Related Documentation

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication on page 426

forwarding-options (Security)

Syntax

```
forwarding-options {
  family {
    inet6 {
      mode (drop | flow-based | packet-based);
    }
    iso {
      mode packet-based;
    }
    mpls {
      mode packet-based;
    }
  }
}
```

Hierarchy Level

```
[edit security]
```

Release Information

Statement introduced in Junos OS Release 8.5 .

Description

Determine how the **inet6, iso**, and **mpls** protocol families manage security forwarding options.

NOTE:

- Packet-based processing is not supported on the following SRX Series devices: SRX5400, SRX5600, and SRX5800.
- On SRX Series devices, the default mode for processing traffic is flow mode. To configure an SRX Series device as a border router, you must change the mode from flow-based processing to packet-based processing. Use the **set security forwarding-options family mpls mode packet-based** statement to configure the SRX device to packet mode. You must reboot the device for the configuration to take effect.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *MPLS Overview*
- *Understanding Packet-Based Processing*
- *Understanding Traffic Processing on Security Devices*

ftp

Syntax

```
ftp {
  authentication-order [authentication-methods];
  connection-limit limit;
  rate-limit limit;
}
```

Hierarchy Level

[edit system services]

Release Information

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

Description

Allow FTP requests from remote systems to the local router or switch.

Options

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring FTP Service for Remote Access to the Router or Switch on page 231

full-name

Syntax full-name *complete-name*;

Hierarchy Level [edit system login user]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure the complete name of a user.

Options ***complete-name***—Full name of the user. If the name contains spaces, enclose it in quotation marks.

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

Related Documentation

- Configuring Junos OS User Accounts by Using a Configuration Group on page 76
- user on page 1597

global (Gx-Plus)

Syntax

```
global {
  include-ipv6;
  max-outstanding-requests number;
}
```

Hierarchy Level

[edit access gx-plus]

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure global attributes for the Gx-Plus application.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Configuring Gx-Plus*

gx-plus (Gx-Plus)

Syntax

```
gx-plus {
  global {
    include-ipv6;
    max-outstanding-requests number;
  }
  partition partition-name {
    diameter-instance instance-name;
    destination-host hostname;
    destination-realm realm;
  }
}
```

Hierarchy Level

[edit access]

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure the Gx-Plus application to interact with a PCRF to authorize and provision subscribers.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Configuring Gx-Plus*

guest-vlan

Syntax

```
guest-vlan (vlan-id | vlan-name);
```

Hierarchy Level

```
[edit protocols dot1x authenticator interface (all | [interface-names ])]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Specify the VLAN to which an interface is moved when no 802.1X supplicants are connected on the interface. The VLAN specified must already exist on the switch.

Default

None

Options

vlan-id—VLAN tag identifier of the guest VLAN.

vlan-name—Name of the guest VLAN.

Required Privilege Level

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

Related Documentation

- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 343
- Understanding Guest VLANs for 802.1X on Switches on page 308

health-monitor

Syntax

```
health-monitor {
  falling-threshold percentage;
  interval seconds;
  rising-threshold percentage;
}
```

Hierarchy Level

[edit snmp]

Release Information

Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure health monitoring.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring Health Monitoring*
- *Understanding Health Monitoring*

hold-multiplier

Syntax hold-multiplier *number*;

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for QFX Series.

Description Specify the multiplier used in combination with the advertisement-interval value to determine the length of time LLDP information is held before it is discarded. The default value is 4 (or 120 seconds).

Default Disabled.

Options *number*—A number used as a multiplier.
Range: 2 through 10
Default: 4 (or 120 seconds)

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

Related Documentation

- show lldp on page 1826
- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518
- Understanding LLDP on page 511

holddown-interval

Syntax

```
holddown-interval milliseconds;
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options
  dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method
  bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method
  bfd]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the time (in milliseconds) for which Bidirectional Forwarding Detection (BFD) holds a session up notification.

Options

milliseconds—Interval specifying how long a BFD session must remain up before a state change notification is sent.

Range: 0 through 255,000

Default: 0

Required Privilege Level

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

Related Documentation

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677

host (SSH Known Hosts)

Syntax

```
host hostname {
  dsa-key dsa-key;
  ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key;
  ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key;
  ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key;
  ed25519-key ed25519-key
  rsa-key rsa-key;
  rsa1-key rsa1-key;
}
```

Hierarchy Level

```
[edit security ssh-known-hosts]
```

Release Information Statement modified in Junos OS Release 8.5.

Description Configure the type of base-64 encoded host key.

Options

- ***hostname***—Name of the SSH known host.
- **dsa-key *dsa-key***—Digital Signature Algorithm (DSA) for SSH version 2
- **ecdsa-sha2-nistp256-key *ecdsa-sha2-nistp256-key***—Elliptic Curve Digital Signature Algorithm (ECDSA)
- **ecdsa-sha2-nistp384-key *ecdsa-sha2-nistp384-key***—Elliptic Curve Digital Signature Algorithm (ECDSA)
- **ecdsa-sha2-nistp521-key *ecdsa-sha2-nistp521-key***—Elliptic Curve Digital Signature Algorithm (ECDSA)
- **ed25519-key *ed25519-key***—Elliptic Curve Digital Signature Algorithm (ed25519 for ECDSA)
- **rsa-key *rsa-key***—RSA public key algorithm, which supports encryption and digital signatures for SSH version 1 and SSH version 2
- **rsa1-key *rsa1-key***—RSA public key algorithm, which supports encryption and digital signatures for SSH version 1

Required Privilege Level

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

Related Documentation

- Generating SSL Certificates for Secure Web Access (SRX Series Devices) on page 253
- Generating a Self-Signed SSL Certificate Automatically on page 254

hostkey-algorithm

Syntax

```
hostkey-algorithm {
  (no-ssh-dss | ssh-dss);
  (no-ssh-rsa | ssh-rsa);
  (no-ssh-ecdsa | ssh-ecdsa);
  (no-ssh-ed25519 | ssh-ed25519);
}
```

Hierarchy Level

```
[edit system services ssh]
```

Release Information Statement introduced in Junos OS Release 11.2.

Description Allow or disallow a host-key algorithm to authenticate another host through SSH protocol. The host-key uses RSA, ECDSA, ED25519, and DSS algorithms.

The following are the behaviors when the **hostkey-algorithm** option is configured with SSH client and SSH server:

- On SSH client the host-key algorithms that are supported when talking to a server are:
  a. RSA: Equal or greater-than to 1024 bit
  b. ECDSA: 256, 384, or 521 bit
  c. ED25519: 256 bit
  d. DSS: 1024 bit
- On SSH server the host-key algorithms that are generated and stored are:
  a. RSA: 2048 bit
  b. ECDSA: 256 bit
  c. ED25519: 256 bit
  d. DSS: 1024 bit

Options

- **ssh-ecdsa**—Allow generation of an ECDSA host-key. Key pair sizes of 256, 384, or 521 bits are compatible with ECDSA.
- **ssh-dss**—Allow generation of a 1024-bit DSA host-key.

NOTE: DSA keys are not supported in FIPS, so the ssh-dss option is not available on systems operating in FIPS mode.

- **ssh-rsa**—Allow generation of RSA host-key. Key pair sizes greater than or equal to 1024 are compatible with RSA.

- **no-ssh-dss**—Do not allow generation of a 1024-bit Digital Signature Algorithm (DSA) host-key.
- **no-ssh-ecdsa**—Do not allow generation of an Elliptic Curve Digital Signature Algorithm (ECDSA) host-key.
- **no-ssh-rsa**—Do not allow generation of an RSA host-key.

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

Related Documentation
- Generating SSL Certificates for Secure Web Access (SRX Series Devices) on page 253
- Generating a Self-Signed SSL Certificate Automatically on page 254

http

Syntax

```
http {
    interfaces [ interface-names ];
    port port;
}
```

Hierarchy Level

[edit system services web-management]

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 and interfaces for HTTP service, which is unencrypted.

Options
interfaces [*interface-names*]—Name of one or more interfaces on which to allow the HTTP service. By default, HTTP access is allowed through built-in Fast Ethernet or Gigabit Ethernet interfaces only.

The remaining statement is explained separately. See CLI Explorer.

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

Related Documentation
- *Configuring Management Access for the EX Series Switch (J-Web Procedure)*
- *J-Web Interface User Guide*
- https on page 1129
- port on page 1337
- web-management on page 1622

https

Syntax

```
https {
  interfaces [ interface-names ];
  local-certificate name;
  port port;
}
```

Hierarchy Level

[edit system services web-management]

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 secure version of HTTP (HTTPS) service, which is encrypted.

Options

interfaces [*interface-names*]—Name of one or more interfaces on which to allow the HTTPS service. By default, HTTPS access is allowed through any ingress interface, but HTTP access is allowed through built-in Fast Ethernet or Gigabit Ethernet interfaces only.

local-certificate *name*—Name of the X.509 certificate for a Secure Sockets Layer (SSL) connection. An SSL connection is configured at the **[edit security certificates local]** hierarchy.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring Management Access for the EX Series Switch (J-Web Procedure)*
- *J-Web Interface User Guide*
- http on page 1128
- port on page 1337
- web-management on page 1622

icmpv4-rate-limit

Syntax

```
icmpv4-rate-limit {
  bucket-size seconds;
  packet-rate pps;
}
```

Hierarchy Level

```
[edit system internet-options]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure rate-limiting parameters for ICMPv4 messages sent.

Options

bucket-size *seconds*—Number of seconds in the rate-limiting bucket.

Range: 0 through 4294967295 seconds

Default: 5

packet-rate *pps*—Rate-limiting packets earned per second.

Range: 0 through 4294967295 pps

Default: 1000

Required Privilege Level

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

Related Documentation

- *Rate Limiting ICMPv4 and ICMPv6 Traffic*
- *Configuring Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages*

idle-timeout (System-Login)

Syntax idle-timeout *minutes*;

Hierarchy Level [edit system login class *class-name*]

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

Description For a login class, configure the maximum time that a session can be idle before the user is logged out of the router or switch. The session times out after remaining at the CLI operational mode prompt for the specified time.

Default If you omit this statement, a user is never forced off the system after extended idle times.

NOTE: After you log in to a device from a shell prompt such as csh, if you start another program to run in the foreground of the CLI, the idle timer control is stopped from being computed. The calculation of idle time of the CLI session is restarted only after the foreground process exits and the control is returned to the shell prompt. When the restart of the idle-timer occurs, if no interaction from the user occurs on the shell, the user is automatically logged out after the expiry of the idle timeout value.

Options ***minutes***—Maximum idle time.

Range: 0 through 4294967295 minutes

NOTE: The timeout feature is disabled if the value of *minutes* is set to 0.

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

Related Documentation

- Configuring the Timeout Value for Idle Login Sessions on page 58
- user on page 1597

idle-timeout (Access)

Syntax idle-timeout *seconds*;

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

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

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

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

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

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

Default: 0

NOTE: **The [edit access] hierarchy is not available on QFabric systems.**

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*
- *Configuring PPP Properties for a Client-Specific Profile*
- *Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile*

idle-timeout

Syntax idle-timeout *minutes*;

Hierarchy Level [edit system login class *class-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description For a login class, configure the maximum time that a session can be idle before the user is logged off the switch. The session times out after remaining at the CLI operational mode prompt for the specified time.

Default If you omit this statement, a user is never forced off the system after extended idle times.

Options ***minutes***—Maximum idle time.
Range: 0 through 4294967295 minutes

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

Related Documentation
- Configuring the Timeout Value for Idle Login Sessions on page 58

idle-timeout (System)

Syntax idle-timeout *idle-timeout*;

Hierarchy Level [edit system login]

Release Information Statement introduced in Junos OS Release 16.1 for the M Series, MX Series, and PTX Series.
Statement introduced in Junos OS Release 15.1X49-D70 for the vSRX, SRX4100, SRX4200 and SRX1500 devices.

Description Configure the maximum time for which the C shell or CLI console session can be idle. The user (including the root user) is logged out after the expiry of **idle-timeout**.

Options ***idle-timeout***— Maximum idle time before logout.

Range: 1 through 60 minutes

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

idle-timeout (System-Login)

Syntax idle-timeout *minutes*;

Hierarchy Level [edit system login class *class-name*]

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

Description For a login class, configure the maximum time that a session can be idle before the user is logged out of the router or switch. The session times out after remaining at the CLI operational mode prompt for the specified time.

Default If you omit this statement, a user is never forced off the system after extended idle times.

NOTE: After you log in to a device from a shell prompt such as csh, if you start another program to run in the foreground of the CLI, the idle timer control is stopped from being computed. The calculation of idle time of the CLI session is restarted only after the foreground process exits and the control is returned to the shell prompt. When the restart of the idle-timer occurs, if no interaction from the user occurs on the shell, the user is automatically logged out after the expiry of the idle timeout value.

Options *minutes*—Maximum idle time.

Range: 0 through 4294967295 minutes

NOTE: The timeout feature is disabled if the value of *minutes* is set to 0.

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

Related Documentation

- Configuring the Timeout Value for Idle Login Sessions on page 58
- user on page 1597

ignore-port-bounce

Syntax ignore-port-bounce;

Hierarchy Level [edit protocols dot1x authenticator interface *interface-name* mac-radius]

Release Information Statement introduced in Junos OS Release 17.3R1 for EX Series switches.

Description Ignore the port-bounce command contained in a Change of Authorization (CoA) request. CoA requests are RADIUS messages that are used to dynamically modify an authenticated user session already in progress. CoA requests are sent from the authentication, authorization, and accounting (AAA) server to the switch, and are typically used to change the VLAN for the host based on device profiling. End devices such as printers do not have a mechanism to detect the VLAN change, so they do not renew the lease for their DHCP address in the new VLAN. The port bounce feature is used to force the end device to initiate DHCP re-negotiation by causing a link flap on the authenticated port. There is no configuration required to enable the port bounce feature.

Default The port bounce feature is supported by default. If you do not configure the **ignore-port-bounce** statement, the switch responds to a port-bounce command by flapping the link to re-initiate DHCP negotiation for the end device.

Required Privilege Level routing

Related Documentation

- Understanding RADIUS-Initiated Changes to an Authorized User Session on page 294

ip-address-first

Syntax

```
ip-address-first;
```

Hierarchy Level

[edit logical-systems *logical-system-name* system services dhcp-local-server pool-match-order],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server pool-match-order],
[edit routing-instances *routing-instance-name* system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]

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 extended DHCP local server to use the IP address method to determine which address-assignment pool to use. The local server uses the IP address in the gateway IP address if one is present in the DHCP client PDU. If no gateway IP address is present, the local server uses the IP address of the receiving interface to find the address-assignment pool. The DHCP local server uses this method by default when no method is explicitly specified.

Required Privilege Level

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

Related Documentation

- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 701
- Extended DHCP Local Server Overview on page 562
- *Address-Assignment Pools Overview*

immediate-update

Syntax immediate-update;

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

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

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

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

Related Documentation
- *Configuring Per-Subscriber Session Accounting*
- *RADIUS Servers and Parameters for Subscriber Access*

include-ipv6 (Gx-Plus)

Syntax include-ipv6;

Hierarchy Level [edit access gx-plus global]

Release Information Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Include IPv6 subscribers in Gx-Plus provisioning requests.

Default By default, IPv6 subscribers are not included.

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

Related Documentation
- *Configuring Gx-Plus Global Attributes*
- *Configuring Gx-Plus*

include-irb-and-l2

Syntax

```
include-irb-and-l2;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id |
  relay-agent-remote-id)],
[edit forwarding-options dhcp-relay dhcpv6 group group-name (relay-agent-interface-id |
  relay-agent-remote-id)],
[edit forwarding-options dhcp-relay relay-option-82 (circuit-id | remote-id)],
[edit forwarding-options dhcp-relay group group-name relay-option-82 (circuit-id |
  remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay dhcpv6
  (relay-agent-interface-id | relay-agent-remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay ... relay-option-82
  (circuit-id | remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6
  (relay-agent-interface-id | relay-agent-remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...
  relay-option-82 (circuit-id | remote-id)],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-18],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-37]
```

Release Information

Statement introduced in Junos OS Release 14.1.

NOTE: The EX Series switches that support the **include-irb-and-l2** statement are the EX4300, EX4600, and EX9200 switches.

Description

Include both the integrated routing and bridging (IRB) interface name and Layer 2 interface name in the **circuit-id** or **remote-id** value in the DHCP option 82 information. VLAN tags are global.

For leasequery and bulk leasequery operations that involve integrated routing and bridging (IRB) interfaces, you must configure DHCP relay agent to include the layer 2 interface name along with IRB name in the circuit ID of option 82. DHCP relay agent uses the layer 2 interface name when using leasequery or bulk leasequery to restore the lease database.

When you configure the **include-irb-and-l2** statement without including the **no-vlan-interface** statement, the format is as follows:

- Bridge domain:

  (fe | ge)-*fpc/pic/port.subunit*:*bridge-domain-name*+irb.*subunit*

- VLAN:

  (fe | ge)-*fpc/pic/port.subunit*:*vlan-name*+irb.*subunit*

NOTE: For remote systems, the *subunit* is required and is used to differentiate an interface.

When you configure both the **include-irb-and-l2** statement and the **use-vlan-id** statement, the format is as follows:

```
(fe | ge)-fpc/pic/port.subunit:svlan-id-vlan-id+irb.subunit
```

NOTE: The *svlan-id-vlan-id* represents the VLANs associated with the bridge domain.

When you configure both the **include-irb-and-l2** and **no-vlan-interface-name** statements, the format is as follows:

```
(fe | ge)-fpc/pic/port.subunit+irb.subunit
```

When you configure both the **include-irb-and-l2** and **use-interface-description** statements, the format displays the description for the Layer 2 interface:

```
l2_descr:vlan-name+irb.subunit
```

If you configure both the **include-irb-and-l2** and **use-interface-description** statements, and no description for the Layer 2 interface is found, the format displays the Layer 2 logical interface name:

```
(fe | ge)-fpc/pic/port.subunit:vlan-name+irb.subunit
```

When you configure the **include-irb-and-l2** statement with both the **no-vlan-interface-name** and **use-interface-description** statements, the format displays as follows:

```
l2_descr+irb.subunit
```

If you configure the **include-irb-and-l2** statement with both the **no-vlan-interface-name** and **use-interface-description** statements, and no description is found for the Layer 2 interface, the format displays as follows:

```
(fe | ge)-fpc/pic/port.subunit+irb.subunit
```

Required Privilege Level

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

Related Documentation

- *Including a Textual Description in DHCP Options*
- Using DHCP Relay Agent Option 82 Information on page 633
- *Configuring DHCPv6 Relay Agent Options*

infranet-controller

Syntax

```
infranet-controller hostname {
  address ip-address;
  interface interface-name;
  password password;
  port port-number;
}
```

Hierarchy Level

[edit services unified-access-control]

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Configure the switch's connection to the Junos Pulse Access Control Service network access control (NAC) device.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 401
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 404

interface (802.1X)

Syntax

```
interface (all | [ interface-names ]) {
  disable;
  guest-vlan (vlan-name | vlan-id);
  lldp-med-bypass;
  mac-radius <restrict>;
  maximum-requests number;
  no-reauthentication;
  quiet-period seconds;
  reauthentication {
    interval seconds;
  }
  retries number;
  server-fail (deny | permit | use-cache | vlan-id | vlan-name);
  server-reject-vlan (vlan-id | vlan-name) {
    eapol-block;
    block-interval block-interval;
  }
  server-timeout seconds;
  supplicant (single | single-secure | multiple);
  supplicant-timeout seconds;
  transmit-period seconds;
}
```

Hierarchy Level

[edit protocols dot1x authenticator]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure 802.1X authentication for Port-Based Network Access Control for all interfaces or for specific interfaces.

Options

all—Configure all interfaces for 802.1X authentication.

[***interface-names***]— List of names of interfaces to configure for 802.1X authentication.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- show dot1x on page 1799
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 343

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 326
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- *Configuring 802.1X Authentication (J-Web Procedure)*

interface (802.1X)

Syntax

```
interface (all | [ interface-names ]) {
  disable;
  guest-vlan (vlan-name | vlan-id);
  lldp-med-bypass;
  mac-radius <restrict>;
  maximum-requests number;
  no-reauthentication;
  quiet-period seconds;
  reauthentication {
    interval seconds;
  }
  retries number;
  server-fail (deny | permit | use-cache | vlan-id | vlan-name);
  server-reject-vlan (vlan-id | vlan-name) {
    eapol-block;
    block-interval block-interval;
  }
  server-timeout seconds;
  supplicant (single | single-secure | multiple);
  supplicant-timeout seconds;
  transmit-period seconds;
}
```

Hierarchy Level

[edit protocols dot1x authenticator]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure 802.1X authentication for Port-Based Network Access Control for all interfaces or for specific interfaces.

Options

all—Configure all interfaces for 802.1X authentication.

[***interface-names***]— List of names of interfaces to configure for 802.1X authentication.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- show dot1x on page 1799
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 343

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 326
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- *Configuring 802.1X Authentication (J-Web Procedure)*

interface (IEEE 802.1x)

Syntax

```
interface interface-id {
  maximum-requests integer;
  quiet-period seconds;
  reauthentication (disable | interval seconds);
  retries integer;
  server-timeout seconds;
  supplicant (single);
  supplicant-timeout seconds;
  transmit-period seconds;
}
```

Hierarchy Level

```
[edit protocols dot1x authenticator]
```

Release Information Statement introduced in Junos OS Release 9.3.

Description Use this statement to configure the 802.1x Port-Based Network Access Control protocol-specific Ethernet interface options.

Default The default values are provided for the options below on the respective statement pages.

Options

maximum-requests—Specify the maximum number of retransmission times for an EAPOL Request packet to the client before it times out the authentication session.

quiet-period—Specify the number of seconds the port remains in the wait state following a failed authentication exchange with the client, before reattempting the authentication.

reauthentication—Includes two options:

- **disable**—Periodic reauthentication of the client is disabled.
- **interval**—Specify the periodic reauthentication time interval.

retries—Specify the number of tries after which the port remains in the wait state for **quiet-period** seconds before reattempting the authentication.

server-timeout—Specify the number of seconds the port waits for a reply when relaying a response from the client to the authentication server before timing out and invoking the server-fail action.

supplicant (*single*)—Specify supplicant single mode. See the usage guidelines to configure other modes.

supplicant-timeout—Specify the number of seconds the port waits for a response when relaying a request from the authentication server to the client before resending the request.

transmit-period—Specify the number of seconds the port waits before retransmitting the initial EAPOL PDUs to the client.

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

Related Documentation
- IEEE 802.1x Port-Based Network Access Control Overview on page 443
- authenticator on page 890
- *dot1x*

interface (Access Control Service)

Syntax
```
interface interface-name;
```

Hierarchy Level
```
[edit services unified-access-control infranet-controller]
```

Release Information
Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description
Specify the interface through which the switch will connect to the Junos Pulse Access Control Service.

Options
interface-name—Name of the interface that will connect the switch to the Access Control Service.

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

Related Documentation
- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 401
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 404

interface (Captive Portal)

Syntax

```
interface (all | [interface-names]) {
  quiet-period seconds;
  retries number-of-retries;
  server-timeout seconds;
  session-expiry seconds;
  supplicant ( multiple | single | single-secure);
}
```

Hierarchy Level

```
[edit services captive-portal]
```

Release Information Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description Configure captive portal authentication for all interfaces or for specific interfaces.

Options

all—All interfaces to be configured for captive portal authentication.

[*interface-names*]—List of names of interfaces to be configured for captive portal authentication.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

routing—To view this statement in the configuration.
routing–control—To add this statement to the configuration.

Related Documentation

- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

interface (DHCP Local Server)

Syntax

```
interface interface-name {
  access-profile profile-name;
  exclude;
  overrides {
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-discover-match <option60-and-option82 | incoming-interface>;
    client-negotiation-match incoming-interface;
    delay-advertise {
      based-on (option-15 | option-16 | option-18 | option-37) {
        equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        not-equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        starts-with {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
      }
      delay-time seconds;
    }
    delay-offer {
      based-on (option-60 | option-77 | option-82) {
        equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        not-equals {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
        starts-with {
          ascii ascii-string;
          hexadecimal hexadecimal-string;
        }
      }
      delay-time seconds;
    }
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    rapid-commit;
  }
  service-profile dynamic-profile-name;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
  trace;
  upto upto-interface-name;
}
```

Hierarchy Level

[edit system services dhcp-local-server group *group-name*],
[edit system services dhcp-local-server dhcpv6 group *group-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server ...],
[edit logical-systems *logical-system-name* system services dhcp-local-server ...],
[edit routing-instances *routing-instance-name* system services dhcp-local-server ...]

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Options **upto** and **exclude** introduced in Junos OS Release 9.1.

Description

Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the **interface** ***interface-name*** statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP relay agent.

NOTE: DHCP values are supported in integrated routing and bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently supports only static DHCP configurations.

Options

exclude—Exclude an interface or a range of interfaces from the group. This option and the **overrides** option are mutually exclusive.

interface-name—Name of the interface. You can repeat this option multiple times.

upto-interface-name—Upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the ***upto-interface-name*** must be the same as the device name of the ***interface-name***.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Extended DHCP Local Server Overview on page 562
- Grouping Interfaces with Common DHCP Configurations on page 670
- Using External AAA Authentication Services with DHCP on page 651

interface (DHCP Relay Agent)

Syntax

```
interface dhcp-interface-name {
  access-profile profile-name;
  exclude;
  overrides {
    allow-no-end-option
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-discover-match <option60-and-option82 | incoming-interface>;
    client-negotiation-match incoming-interface;
    disable-relay;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    proxy-mode;
    relay-source
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
  }
  service-profile dynamic-profile-name;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
  trace;
  upto upto-interface-name;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 8.3.
Options **upto** and **exclude** introduced in Junos OS Release 9.1.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP or DHCPv6 relay agent is enabled. You can repeat the **interface *interface-name*** statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP local server. Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

EX Series switches do not support DHCPv6.

NOTE: DHCP values are supported in integrated routing and bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently only supports static DHCP configurations. .

Options

exclude—Exclude an interface or a range of interfaces from the group. This option and the **overrides** option are mutually exclusive.

interface-name—Name of the interface. You can repeat this option multiple times.

overrides—Override the specified default configuration settings for the interface. The overrides statement is described separately.

upto-interface-name—Upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the ***upto-interface-name*** must be the same as the device name of the ***interface-name***.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618
- Grouping Interfaces with Common DHCP Configurations on page 670
- Using External AAA Authentication Services with DHCP on page 651

interface (LLDP)

Syntax

```
interface (all | interface-name) {
  disable;
  power-negotiation {
    disable;
  }
}
```

Hierarchy Level

[edit protocols lldp]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure Link Layer Discovery Protocol (LLDP) on all interfaces or on a specific interface.

NOTE: On EX4300 switches, LLDP cannot be configured on the me0 or vme interface. Issuing the command **set protocols lldp interface me0** generates the following error message:

```
error: name: 'me0': Invalid interface
error: statement creation failed: interface
```

Issuing the command **set protocols lldp interface vme** generates the following error message:

```
error: name: 'vme': Invalid interface
error: statement creation failed: interface
```

Default

None

Options

all—All interfaces on the switch.

interface-name—Name of a specific interface.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518
- Understanding LLDP on page 511

interface (LLDP-MED)

Syntax

```
interface (all | interface-name) {
  disable;
  location {
    elin number;
    civic-based {
      what number;
      country-code code;
      ca-type {
        number {
          ca-value value;
        }
      }
    }
  }
}
```

Hierarchy Level

[edit protocols lldp-med]

Release Information

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

Description

Configure Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) on all interfaces or on a specific interface.

Default

Not enabled

Options

all—All interfaces on the switch.

interface-name—Name of a specific interface.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- show lldp on page 1826
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Configuring LLDP-MED (CLI Procedure) on page 521
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

interface (Static MAC Bypass)

Syntax

```
interface [interface-names];
```

Hierarchy Level

[edit protocols dot1x authenticator authentication-profile-name static *mac-address*],
[edit ethernet-switching-options authentication-whitelist *mac-address*],
[edit switch-options authentication-whitelist *mac-address*]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement added to the **[edit ethernet-switching-options authentication-whitelist]** hierarchy in Junos OS Release 10.1 for EX Series switches.
Statement added to the **[edit switch-options authentication-whitelist]** hierarchy in Junos OS Release 13.2X50-D10 for EX Series switches (ELS).
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure interfaces on which the specified MAC addresses are allowed to bypass RADIUS authentication and allowed to connect to the LAN without authentication.

Options

interface-names—List of interfaces.

Required Privilege Level

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

Related Documentation

- show dot1x static-mac-address on page 1811
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 368
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

interface (Static MAC Bypass)

Syntax
interface [*interface-names*];

Hierarchy Level
[edit protocols authentication-access-control]

Release Information
Statement introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description
Configure interfaces on which the specified MAC addresses are allowed to bypass RADIUS authentication and allowed to connect to the LAN without authentication.

Options
interface-names—List of interfaces.

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

Related Documentation

interface (VoIP)

Syntax

```
interface (all | [interface-name] | access-ports) {
  vlan vlan-name );
  forwarding-class <assured-forwarding | best-effort | expedited-forwarding |
    network-control>;
}
```

Hierarchy Level

- For platforms with ELS:

  [edit switch-options voip]

- For platforms without ELS:

  [edit ethernet-switching-options voip],

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level **[edit switch-options]** introduced in Junos OS Release 13.2X50-D10. (See *Using the Enhanced Layer 2 Software CLI* for information about ELS.)

Description

Enable voice over IP (VoIP) on interfaces.

Options

all—Enable VoIP on all interfaces.

interface-name—Enable VoIP on a specific interface.

all—(Switches without ELS only) Enable VoIP on all access ports.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication on page 426
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 421

interface (System Services DHCP)

Syntax

```
interface interface-name {
  exclude;
  overrides {
    interface-client-limit number;
  }
  trace;
  upto upto-interface-name;
}
```

Hierarchy Level

```
[edit system services dhcp-local-server dhcpv6 group group-name]
```

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the interface interface-name statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group.

Options

- *interface-name*—Name of the interface.
- **trace**—Enable tracing of the interface specified by the *interface-name* argument.
- **upto** *upto-interface-name*—The upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the *upto-interface-name* must be the same as the device name of the *interface-name*.

Required Privilege Level

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*
- DHCP Server Configuration Overview on page 719

interface-client-limit (DHCP Local Server)

Syntax

```
interface-client-limit number;
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides],
[edit logical-systems *logical-system-name* system services dhcp-local-server overrides],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 overrides],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* overrides],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides],
[edit routing-instances *routing-instance-name* system services dhcp-local-server overrides],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 overrides],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* overrides],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides],
[edit system services dhcp-local-server overrides],
[edit system services dhcp-local-server dhcpv6 overrides],
[edit system services dhcp-local-server dhcpv6 group *group-name* overrides],
[edit system services dhcp-local-server dhcpv6 group interface *interface-name group-name* overrides],
[edit system services dhcp-local-server group *group-name* overrides],
[edit system services dhcp-local-server group *group-name* interface *interface-name* overrides]

Release Information

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Set the maximum number of DHCP subscribers or DHCP clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group.

Default

No limit

Options

number—Maximum number of clients allowed.

Range: 1 through 500,000

Required Privilege Level

system—To view this statement in the configuration.

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

Related Documentation

- Specifying the Maximum Number of DHCP Clients Per Interface on page 656
- Overriding the Default DHCP Local Server Configuration Settings Overview on page 630

interface-client-limit (DHCP Relay Agent)

Syntax

```
interface-client-limit number;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group
  group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
  overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6
  overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group
  group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group
  group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group
  group-name interface interface-name overrides]
```

Release Information

Statement introduced in Junos OS Release 9.2.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Set the maximum number of DHCP (or DHCPv6) subscribers or clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group. Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

M120 and M320 routers do not support DHCPv6.

Default

No limit

Options

number—Maximum number of clients allowed.

Range: 1 through 500,000

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

Related Documentation
- dhcp-relay on page 997
- Extended DHCP Relay Agent Overview on page 618
- Configuring Group-Specific DHCP Relay Options on page 672
- Overriding the Default DHCP Relay Configuration Settings on page 627

interface-delete (Subscriber Management or DHCP Client Management)

Syntax
```
interface-delete;
```

Hierarchy Level
```
[edit system services subscriber-management maintain-subscriber]
```

Release Information
Statement introduced in Junos OS Release 11.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
On router—Configure the router to maintain, rather than log out, subscribers when the subscriber interface is deleted. By default, the router logs out subscribers when the subscriber interface is deleted.

On switch—Configure the switch to maintain rather than log out DHCP clients when the client interface is deleted. By default, the switch logs out DHCP clients when the client interface is deleted.

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

Related Documentation
- *Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events*

interface-description-format

Syntax

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

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
exclude-adapter and **exclude-sub-interface** options added in Junos OS Release 10.4.
exclude-channel option added in Junos OS Release 17.3R1.

Description

Specify the information that is excluded from the interface description that the device passes to RADIUS for inclusion in the RADIUS attributes such as NAS-Port-ID (87) or Calling-Station-ID (31).

The default format for nonchannelized interfaces is as follows:

***interface-type-slot/adapter/port.subinterface*[:*svlan-vlan*]**

For example, consider physical interface ge-1/2/0, with a subinterface of 100 and SVLAN identifier of 100. The interface description used in the NAS-Port-ID is ge-1/2/0.100:100. If you exclude the subinterface, the description becomes ge-1/2/0:100.

The default format for channelized interfaces is as follows:

***interface-type-slot/adapter/channel.subinterface*[:*svlan-vlan*]**

The channel information (logical port number) is determined by this formula:

Logical port number = 100 + (*actual-port-number* x 20) + *channel-number*.

For example, consider a channelized interface 3 on port 2 where the:

- Physical interface is xe-0/1/2:3.
- Subinterface is 4.
- SVLAN is 5.
- VLAN is 6.

Using the formula, the logical port number = 100 + (2 x 20) + 3 = 143. Consequently, the default interface description is xe-0/1/143.4-5.6. If you exclude the channel information, the description becomes xe-0/1/2.4-5.6.

Options

exclude-adapter——(Optional) Exclude the adapter from the interface description.

exclude-channel—(Optional) Exclude the channel information from the interface description.

exclude-sub-interface——(Optional) Exclude the subinterface from the interface description.

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

Related Documentation
- *Interface Text Descriptions for Inclusion in RADIUS Attributes*
- *RADIUS Servers and Parameters for Subscriber Access*

interface-name (DHCP Local Server)

Syntax
```
interface-name;
```

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

Release Information
Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Specify that the interface name is concatenated with the username during the subscriber authentication or DHCP client authentication process. Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

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

Related Documentation
- Creating Unique Usernames for DHCP Clients on page 653

interface-profile

Syntax

```
interface-profile profile-name {
  allow-clear;
  fields {
    field-name;
  }
  file filename;
  interval minutes;
}
```

Hierarchy Level

```
[edit accounting-options]
```

Release Information

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

Description

Create a profile to filter and collect error and packet statistics and write them to a file in the **/var/log** directory. You can specify an interface profile for either a physical or a logical interface.

Options

profile-name—Name of the interface profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring the Interface Profile*
- *Accounting Options Configuration*

interface-traceoptions (System Services DHCP)

Syntax

```
interface-traceoptions {
  file {
    filename ;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

Hierarchy Level

```
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]
```

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure extended DHCP local server tracing operations that can be enabled on a specific interface or group of interfaces. You use the **interface *interface-name* trace** statement at the **[edit system services group *group-name*]** hierarchy level to enable the tracing operation on the specific interfaces.

Options ***file-name***—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (“ ”). All files are placed in a file named **jdhcpd** in the directory **/var/log**. If you include the **file** statement, you must specify a filename.

files *number*—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all events
- **dhcpv6-packet**—Trace DHCPv6 packet decoding operations.
- **dhcpv6-packet-option**—Trace DHCPv6 option decoding operations.
- **dhcpv6-state**—Trace changes in state for DHCPv6 operations.
- **packet**—Trace packet decoding operations

- **packet-option**—Trace DHCP option decoding operations
- **state**—Trace changes in state

match ***regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size ***size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*
- DHCP Server Configuration Overview on page 719

interfaces (ARP)

Syntax

```
interfaces {
  interface-name {
    aging-timer minutes;
  }
}
```

Hierarchy Level

[edit system arp]

Release Information

Statement introduced before Junos OS Release 9.4.

Description

Specify the Address Resolution Protocol (ARP) aging timer in minutes for a logical interface.

Options

aging-timer *minutes*—Time between ARP updates, in minutes.

Range: 1 through 240

Default: 20

Required Privilege Level

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*
- DHCP Server Configuration Overview on page 719

interval

Syntax

```
interval minutes;
```

Hierarchy Level

```
[edit accounting-options class-usage-profile profile-name],
[edit accounting-options filter-profile profile-name],
[edit accounting-options interface-profile profile-name],
[edit accounting-options mib-profile profile-name],
[edit accounting-options routing-engine-profile profile-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
The **[edit accounting-options mib-profile *profile-name*]** hierarchy level added in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Specify how often statistics are collected for the accounting profile.

Options

minutes—Length of time between each collection of statistics.

Range: 1 through 2880 minutes

Default: 30 minutes

Required Privilege Level

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

Related Documentation

- *Configuring the Interface Profile*
- *Configuring the Filter Profile*
- *Configuring the MIB Profile*
- *Configuring the Routing Engine Profile*

interval (Health Monitor)

Syntax interval *seconds*;

Hierarchy Level [edit snmp health-monitor]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the interval between sampling of the object being monitored by the health monitor.

Options ***seconds***—Time between samples, in seconds.
Range: **1** through **2147483647** seconds
Default: **300** seconds

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

Related Documentation
- *Configuring Health Monitoring*

interfaces (Security Zones)

Syntax

```
interfaces interface-name {
  host-inbound-traffic {
    protocols protocol-name {
      except;
    }
    system-services service-name {
      except;
    }
  }
}
```

Hierarchy Level

```
[edit security zones functional-zone management],
[edit security zones security-zone zone-name]
```

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the set of interfaces that are part of the zone.

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

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation

- *Understanding Security Zones*

interface (Static MAC Bypass)

Syntax

```
interface [interface-names];
```

Hierarchy Level

[edit protocols dot1x authenticator authentication-profile-name static *mac-address*],
[edit ethernet-switching-options authentication-whitelist *mac-address*],
[edit switch-options authentication-whitelist *mac-address*]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement added to the **[edit ethernet-switching-options authentication-whitelist]** hierarchy in Junos OS Release 10.1 for EX Series switches.
Statement added to the **[edit switch-options authentication-whitelist]** hierarchy in Junos OS Release 13.2X50-D10 for EX Series switches (ELS).
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure interfaces on which the specified MAC addresses are allowed to bypass RADIUS authentication and allowed to connect to the LAN without authentication.

Options

interface-names—List of interfaces.

Required Privilege Level

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

Related Documentation

- **show dot1x static-mac-address on page 1811**
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 368
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

interface (VoIP)

Syntax

```
interface (all | [interface-name] | access-ports) {
  vlan vlan-name );
  forwarding-class <assured-forwarding | best-effort | expedited-forwarding |
    network-control>;
}
```

Hierarchy Level

- For platforms with ELS:

  [edit switch-options voip]

- For platforms without ELS:

  [edit ethernet-switching-options voip],

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level **[edit switch-options]** introduced in Junos OS Release 13.2X50-D10. (See *Using the Enhanced Layer 2 Software CLI* for information about ELS.)

Description

Enable voice over IP (VoIP) on interfaces.

Options

all—Enable VoIP on all interfaces.

interface-name—Enable VoIP on a specific interface.

all—(Switches without ELS only) Enable VoIP on all access ports.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication on page 426
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 421

interface-description-format

Syntax

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

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
exclude-adapter and **exclude-sub-interface** options added in Junos OS Release 10.4.
exclude-channel option added in Junos OS Release 17.3R1.

Description

Specify the information that is excluded from the interface description that the device passes to RADIUS for inclusion in the RADIUS attributes such as NAS-Port-ID (87) or Calling-Station-ID (31).

The default format for nonchannelized interfaces is as follows:

***interface-type-slot/adapter/port.subinterface*[:*svlan-vlan*]**

For example, consider physical interface ge-1/2/0, with a subinterface of 100 and SVLAN identifier of 100. The interface description used in the NAS-Port-ID is ge-1/2/0.100:100. If you exclude the subinterface, the description becomes ge-1/2/0:100.

The default format for channelized interfaces is as follows:

***interface-type-slot/adapter/channel.subinterface*[:*svlan-vlan*]**

The channel information (logical port number) is determined by this formula:

Logical port number = 100 + (*actual-port-number* x 20) + *channel-number*.

For example, consider a channelized interface 3 on port 2 where the:

- Physical interface is xe-0/1/2:3.
- Subinterface is 4.
- SVLAN is 5.
- VLAN is 6.

Using the formula, the logical port number = 100 + (2 x 20) + 3 = 143. Consequently, the default interface description is xe-0/1/143.4-5.6. If you exclude the channel information, the description becomes xe-0/1/2.4-5.6.

Options

exclude-adapter——(Optional) Exclude the adapter from the interface description.

exclude-channel—(Optional) Exclude the channel information from the interface description.

exclude-sub-interface——(Optional) Exclude the subinterface from the interface description.

Required Privilege Level

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

Related Documentation

- *Interface Text Descriptions for Inclusion in RADIUS Attributes*
- *RADIUS Servers and Parameters for Subscriber Access*

internet-options

Syntax

```
internet-options {
  (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
  icmpv4-rate-limit bucket-size bucket-size packet-rate packet-rate;
  icmpv6-rate-limit bucket-size bucket-size packet-rate packet-rate;
  (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
  ipv6-duplicate-addr-detection-transmits;
  (ipv6-reject-zero-hop-limit | no-ipv6-reject-zero-hop-limit);
  (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
  ipv6-path-mtu-discovery-timeout;
  no-tcp-reset
  no-tcp-rfc1323;
  no-tcp-rfc1323-paws;
  (path-mtu-discovery | no-path-mtu-discovery);
  source-port upper-limit <upper-limit>;
  (source-quench | no-source-quench);
  tcp-drop-synfin-set;
  tcp-mss mss-value;
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for SRX Series devices.
no-tcp-reset introduced in Junos OS Release 11.1 for SRX Series and vSRX devices.
source-port introduced in Junos OS Release 11.1 for the QFX Series and Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure system IP options to protect against certain types of DoS attacks.

Options

gre-path-mtu-discovery—(ACX Series, EX Series, Junos Fusion, OCX Series, PTX Series, QFX Series, SRX Series, T Series) Configure path MTU discovery for outgoing GRE tunnel connections. By default, path MTU discovery is enabled.

Values:

- gre-path-mtu-discovery—Path MTU discovery is enabled.
- no-gre-path-mtu-discovery—Path MTU discovery is disabled.

icmpv4-rate-limit—(EX Series, M Series, MX Series, PTX Series, SRX Series, T Series only) Configure rate-limiting parameters for ICMPv4 messages sent.

Values:

- bucket-size *seconds*—Number of seconds in the rate-limiting bucket. Range: 0 through 4294967295 seconds. Default: 5.

- packet-rate *pps*—Rate-limiting packets earned per second. Range: 0 through 4294967295 pps. Default: 1000.

icmpv6-rate-limit—(ACX Series, MX Series, SRX Series only) Configure rate-limiting parameters for ICMPv6 messages sent.

Values:

- bucket-size *seconds*—Number of seconds in the rate-limiting bucket. Range: 0 through 4294967295 seconds. Default: 5.
- packet-rate *pps*—Rate-limiting packets earned per second. Range: 0 through 4294967295 pps. Default: 1000.

ipip-path-mtu-discovery—(ACX Series, EX Series, Junos Fusion, OCX Series, PTX Series, QFX Series, SRX Series, T Series) Configure path MTU discovery for outgoing IP-IP tunnel connections. By default, path MTU discovery is enabled.

Values:

- ipip-path-mtu-discovery—Path MTU discovery is enabled.
- no-ipip-path-mtu-discovery—Path MTU discovery is disabled.

ipv6-duplicate-addr-detection-transmits—(EX Series, M Series, MX Series, PTX Series, SRX Series, T Series only) Control the number of attempts for IPv6 duplicate address detection.

Range: 0 to 20

Default: 3

ipv6-path-mtu-discovery—(ACX Series, EX Series, Junos Fusion, OCX Series, PTX Series, QFX Series, SRX Series, T Series) Configure path MTU discovery for IPv6 packets. By default, IPv6 path MTU discovery is enabled.

Values:

- ipv6-path-mtu-discovery—IPv6 path MTU discovery is enabled.
- no-ipv6-path-mtu-discovery—IPv6 path MTU discovery is disabled.

ipv6-path-mtu-discovery-timeout—(ACX Series, EX Series, Junos Fusion, OCX Series, PTX Series, QFX Series, SRX Series, T Series) Set the IPv6 path MTU discovery timeout interval.

Values: *minutes*—IPv6 path MTU discovery timeout.

Default: 10 minutes.

ipv6-reject-zero-hop-limit—(EX Series, M Series, MX Series, PTX Series, SRX Series, T Series only) Enable and disable rejecting incoming IPv6 packets with a zero hop limit value in their header.

Values:

- ipv6-reject-zero-hop-limit—Incoming IPv6 packets with a zero hop limit value in their header are rejected.
- no-ipv6-reject-zero-hop-limit—Incoming IPv6 packets with a zero hop limit value in their header are allowed.

no-tcp-reset—(SRX Series, vSRX only) When **no-tcp-reset** is enabled and non-listening ports receive TCP packets, the device does not send back RESET TCP packets. Statement introduced in Junos OS Release 11.1.

By default, a device sends a TCP packet with the RESET flag when a TCP packet is received on a non-listening port. This might lead to a security risk. Configuring this statement prevents the sending of RESET TCP packets to non-listening ports. This is accomplished through one of the following methods:

- When a TCP SYN segment is received on a port where there is no socket accepting connections, the device send back RESET segment and drops the connection. The device attempting to connect is refused connection.
- When a TCP packet with a SYN bit is received on a port, the device drops the packet and does not send back RESET segment, which makes the device appear as a black hole.
- When a TCP segment without a SYN bit received on a closed port, the device drops the packet and does not send back RESET segment. This helps to protect against stealth port scans.

Values:

- drop-all-tcp—Drop all TCP packets.
- drop-tcp-with-syn-only—Drop TCP packets with a SYN bit.

no-tcp-rfc1323—(EX Series, PTX Series, SRX Series only) Configure the Junos OS to disable RFC 1323 TCP extensions.

no-tcp-rfc1323-paws—(EX Series, M Series, MX Series, PTX Series, SRX Series, T Series only) Configure the Junos OS to disable the RFC 1323 Protection Against Wrapped Sequence (PAWS) number extension.

path-mtu-discovery—(ACX Series, EX Series, Junos Fusion, OCX Series, PTX Series, QFX Series, SRX Series, T Series) Configure path MTU discovery for outgoing Transmission Control Protocol (TCP). By default, path MTU discovery is enabled.

Values:

- path-mtu-discovery—Path MTU discovery is enabled.
- no-path-mtu-discovery—Path MTU discovery is disabled.

source-port—(SRX Series only) Configure the range of port addresses starting in Junos OS Release 11.1 for the QFX Series and Junos OS Release 14.1X53-D20 for the OCX Series.

Values:

- upper-limit *upper-limit*—(Optional) The range of port addresses can be a value from 5000 through 65,355.

source-quench—(M Series, MX Series, SRX Series, T Series only) Configure how the Junos OS handles Internet Control Message Protocol (ICMP) source quench messages. By default, the Junos OS reacts to ICMP source quench messages.

Values:

- source-quench—React to incoming ICMP source quench messages.
- no-source-quench—Do not react to incoming ICMP source quench messages.

tcp-drop-synfin-set—(EX Series, M Series, MX Series, PTX Series, SRX Series, T Series only) Configure the router or switch to drop packets that have both the SYN and FIN bits set.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Configuring Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages*
- *Configuring Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages*
- *Configuring Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections*
- *Configuring Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections*
- *Configuring Junos OS for Path MTU Discovery on Outgoing TCP Connections*
- *Configuring Junos OS for IPv6 Duplicate Address Detection Attempts*
- *Configuring Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit*
- *Configuring Junos OS to Ignore ICMP Source Quench Messages*
- *Configuring Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set*
- *Configuring Junos OS to Disable TCP RFC 1323 Extensions*
- *Configuring Junos OS to Disable the TCP RFC 1323 PAWS Extension*
- *Configuring Junos OS to Extend the Default Port Address Range*
- *Rate Limiting ICMPv4 and ICMPv6 Traffic*
- *Understanding Traffic Processing on Security Devices*
- *TCP Headers with SYN and FIN Flags Set*

interval (Access Control Service)

Syntax interval *seconds*;

Hierarchy Level [edit services unified-access-control]

Release Information Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description Configure the time between continuity check messages for the switch's connection with the Junos Pulse Access Control Service. The specified value must be less than the value specified for timeout.

Options ***seconds***—Time between continuity check messages, in seconds.

Range: 1 through 9999 seconds

Default: 30 seconds

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

Related Documentation

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 401
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 404

interval (Health Monitor)

Syntax interval *seconds*;

Hierarchy Level [edit snmp health-monitor]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the interval between sampling of the object being monitored by the health monitor.

Options ***seconds***—Time between samples, in seconds.
Range: 1 through **2147483647** seconds
Default: **300** seconds

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

Related Documentation
- *Configuring Health Monitoring*

kernel-replication (System)

Syntax kernel-replication;

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 11.1.

Description Configure kernel replication.

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

key (Authentication Keychain)

Syntax

```
key key {
  algorithm (md5 | hmac-sha-1);
  options (basic | isis-enhanced);
  key-nameauthentication-key-name;
  secret secret-data;
  start-time yyyy-mm-dd.hh:mm:ss;
}
```

Hierarchy Level

[edit security authentication-key-chains key-chain *key-chain-name*]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.4.

Description

Configure the authentication element.

Options

key—Each key within a keychain is identified by a unique integer value.

Range: 0 through 63

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols on page 226
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

key-chain (Security)

Syntax

```
key-chain key-chain-name {
  description text-string;
  key key {
    algorithm (md5 | hmac-sha-1);
    options (basic | isis-enhanced);
    key-nameauthentication-key-name;
    secret secret-data;
    start-time yyyy-mm-dd.hh:mm:ss;
  }
  tolerance seconds;
}
```

Hierarchy Level

```
[edit security authentication-key-chains]
```

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.4.

Description

Create the key-chain configuration for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol.

Options

key-chain-name—Authentication keychain name. It can be up to 126 characters. Characters can include any ASCII strings. If you include spaces, enclose all characters in quotation marks (“ ”).

Required Privilege Level

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

Related Documentation

- authentication-key-chains on page 893
- Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols on page 226
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

key-exchange

Syntax key-exchange [*algorithm1 algorithm2*...];

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 11.2. Support for curve25519-sha256 added in Junos OS Release 12.1X47-D10.

Description Specify the set of Diffie-Hellman key exchange methods that the SSH server can use.

Options One or more of the following Diffie-Hellman key exchange methods:

- **curve25519-sha256**—The EC Diffie-Hellman key exchange method on Curve25519 with SHA2-256.
- **dh-group1-sha1**—The Diffie-Hellman group1 algorithm using SHA-1.
- **dh-group14-sha1**—The Diffie-Hellman group14 algorithm using SHA-1.
- **ecdh-sha2-nistp256**—The ECDH key exchange method with ephemeral keys generated on the nistp256 curve.
- **ecdh-sha2-nistp384**—The ECDH key exchange method with ephemeral keys generated on the nistp384 curve.
- **ecdh-sha2-nistp521**—The ECDH key exchange method with ephemeral keys generated on the nistp521 curve.
- **group-exchange-sha1**—The group exchange algorithm using SHA-1.
- **group-exchange-sha2**—The group exchange algorithm using SHA-2.

NOTE: The key-exchange represents a set. To configure key-exchange:

```
user@host#set system services ssh key-exchange [ecdh-sha2-nistp256
  group-exchange-sha1]
```

NOTE: Table 58 on page 1186 shows the supportability of Diffie-Hellman key exchange methods on FIPS mode.

Table 58: Supportability of Diffie-Hellman key exchange methods on FIPS mode

Diffie-Hellman key exchange methods	Supported on FIPS mode
curve25519-sha256	No
dh-group1-sha1	No
dh-group14-sha1	Yes
ecdh-sha2-nistp256	Yes
ecdh-sha2-nistp384	Yes
ecdh-sha2-nistp521	Yes
group-exchange-sha1	No
group-exchange-sha2	No

Required Privilege Level

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

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 232
- ciphers on page 929
- macs on page 1217

layer2-liveness-detection (Send)

Syntax

```
layer2-liveness-detection {
    max-consecutive-retries number;
    transmit-interval seconds;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name
    liveness-detection method],
[edit forwarding-options dhcp-relay group group-name liveness-detection method],
[edit forwarding-options dhcp-relay liveness-detection method],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection
    method],
[edit system services dhcp-local-server dhcpv6 liveness-detection method],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name
    liveness-detection method],
[edit system services dhcp-local-server group group-name liveness-detection method],
[edit system services dhcp-local-server liveness-detection method],
```

Release Information

Statement introduced in Junos OS Release 17.4R1.

Description

Configure a router acting as a broadband network gateway (BNG) to conduct a host connectivity check on its directly connected DHCPv4 and DHCPv6 clients to determine the validity and state of the DHCP client session, and to clean up inactive sessions.

The BNG sends ARP or ND request packets to the each DHCP client at a configurable interval, then waits for a response. If it receives a response from a client before the interval times out, it sends another request to the client when the timer expires.

If the BNG does not receive a response before the interval times out, it sets the timer to 30 seconds and sends another request. This is the first retry attempt.

If it receives a response from a client before the 30-second interval times out, it sends another request to the client when the timer expires. If the 30-second timer expires before a response is received, the BNG sets the timer to 10 seconds and sends another request. This is the second retry attempt. If the BNG does not receive a response within this interval it resets the timer to 10 seconds and sends another request. The BNG continues to send requests at 10-second intervals until it either receives a response from the client before the interval times out or exhausts the number of retry attempts.

The first retry attempt uses a 30-second interval. Subsequent retries occur at 10-second intervals. The number of possible 10-second retries is therefore the total number of retries minus 1. For example, if you configure 5 retries, there is one 30-second retry and up to four 10-second retries.

If the BNG attempts all the retries and never receives a response from a client within the interval, the client session is declared to be down.

NOTE: The only option to the failure-action statement supported by Layer 2 liveness detection is clear-binding.

Options

max-consecutive-retries *number*—Maximum number of consecutive times that the router sends an ARP request packet in the absence of an ARP response packet.

Range: 3 through 6 retries

Default: 3 retries

transmit-interval *seconds*—Initial interval that the router waits for an ARP response after sending an ARP request packet to the client or waits for an ND response packet after sending an NG request packet to the client.

Range: 300 through 1800 seconds

Default: 300 seconds

Required Privilege Level

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

Related Documentation

- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets on page 686
- DHCP Liveness Detection Overview on page 674

layer2-unicast-replies

Syntax

```
layer2-unicast-replies;
```

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* interface *interface-name* overrides]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Override the setting of the broadcast bit in DHCP request packets and instead use the Layer 2 unicast transmission method to transmit DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618
- dhcp-relay on page 997

ldap-url

Syntax <ldap-url *url-name*>;

Hierarchy Level [edit security certificates certification-authority *ca-profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series,

Description (Encryption interface on M Series and T Series routers and EX Series switches only) (Optional) Specify the Lightweight Directory Access Protocol (LDAP) URL for digital certificates.

Options ***url-name***—Name of the LDAP URL.

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

Related Documentation

- *Specifying an LDAP URL*

lease-time

Syntax lease-time (*length* | infinite);

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.2 for SRX Series devices.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Request a specific lease time for the IP address. The lease time is the length of time in seconds that a client holds the lease for an IP address assigned by a DHCP server.

Default If no lease time is requested by client, then the server sends the lease time. The default lease time on a Junos OS DHCP server is one day.

Options ***seconds*** —Request a lease time of a specific duration.
Range: 60 through 2147483647 seconds

infinite—Request that the lease never expire.

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

Related Documentation

- Configuring a DHCP Client (CLI Procedure) on page 591
- *interfaces*
- *unit*
- *family*

lease-time (dhcp-client)

Syntax lease-time *seconds*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option **dhcp-clinet** at **[edit interfaces interface-name unit logical-unit-number family inet]** hierarchy is changed to **dhcp** to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option **dhcp**.

Description Specify the time to negotiate and exchange Dynamic Host Configuration Protocol (DHCP) information.

Options **seconds**— Request time to negotiate and exchange information.

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

Related Documentation
- *DHCP Server, Client, and Relay Agent Overview*

liveness-detection

Syntax

```
liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    bfd {
      version (0 | 1 | automatic);
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      detection-time {
        threshold milliseconds;
      }
      session-mode(automatic | multihop | singlehop);
      holddown-interval milliseconds;
    }
    layer2-liveness-detection {
      max-consecutive-retries number;
      transmit-interval interval;
    }
  }
}
```

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name*],
[edit forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit forwarding-options dhcp-relay group *group-name*],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group *group-name*],
[edit system services dhcp-local-server dual-stack-group *dual-stack-group-name*],
[edit system services dhcp-local-server group *group-name*]

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure bidirectional failure detection timers and authentication criteria for static routes.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- DHCP Liveness Detection Overview on page 674
- Configuring Detection of DHCP Local Server Client Connectivity with BFD on page 680
- Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD on page 675
- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677
- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets on page 686

lldp

Syntax

```
lldp {
  advertisement-interval seconds;
  disable;
  hold-multiplier number;
  interface (all | [interface-name]) {
    disable;
    power-negotiation {
      disable;
    }
  }
  lldp-configuration-notification-interval seconds;
  management-address ip-management-address;
  mau-type
  netbios-snooping;
  no-tagging;
  ptopo-configuration-maximum-hold-time seconds;
  ptopo-configuration-trap-interval seconds;
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>
      <no-stamp> <replace>;
    flag flag <disable>;
  }
  transmit-delay seconds;
  vlan-name-tlv-option (name | vlan-id);
}
```

Hierarchy Level

```
[edit protocols]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for QFX Series.

Description

Configure Link Layer Discovery Protocol (LLDP). The switch uses LLDP to advertise its identity and capabilities on a LAN, as well as to receive information about other network devices. LLDP is defined in the IEEE standard 802.1AB-2005.

The remaining statements are explained separately. See CLI Explorer.

NOTE: The **transmit-delay** and **netbios-snooping** options are not available on QFabric systems.

NOTE: On EX4300 switches, LLDP cannot be configured on the me0 or vme interface. Issuing the command **set protocols lldp interface me0** generates the following error message:

```
error: name: 'me0': Invalid interface
error: statement creation failed: interface
```

Issuing the command **set protocols lldp interface vme** generates the following error message:

```
error: name: 'vme': Invalid interface
error: statement creation failed: interface
```

Default LLDP is enabled.

The following statements have default values:

- **advertisement-interval**—The default value is 30 seconds. The allowable range is from 5 through 32768 seconds.
- **hold-multiplier**—The default values is 4. The allowable range is from 2 through 10.
- **ptopo-configuration-maximum-hold-time**—The default value is 300 seconds. The allowable range is from 1 through 2147483647 seconds.
- **transmit-delay**—The default values is 2 seconds. The allowable range is from 1 through 8192 seconds.

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

Related Documentation

- show lldp on page 1826
- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP on page 511
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

lldp-configuration-notification-interval

Syntax

```
lldp-configuration-notification-interval seconds;
```

Hierarchy Level

```
[edit protocols lldp]
[edit routing-instances routing-instance-name protocols lldp]
```

Release Information

Statement introduced in Junos OS Release 9.6 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Specify how often SNMP trap notifications are generated as a result of LLDP database changes.

Default

SNMP trap notifications of LLDP database changes are disabled.

Options

seconds—Time for the period of SNMP trap notifications about the LLDP database. This feature is disabled by default.

Range: 5 through 3600

Required Privilege Level

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

Related Documentation

- *Configuring LLDP*
- show lldp on page 1826

lldp-med (Ethernet Switching)

Syntax

```
lldp-med {
  disable;
  fast-start number;
  interface (all | interface-name) {
    disable;
    location {
      elin number;
      civic-based {
        what number;
        country-code code;
        ca-type {
          number {
            ca-value value;
          }
        }
      }
    }
  }
}
```

Hierarchy Level

[edit protocols]

Release Information

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

Description

Configure Link Layer Discovery Protocol–Media Endpoint Discovery. LLDP-MED is an extension of LLDP. The switch uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations for emergency services. LLDP-MED is defined in the standard ANSI/TIA-1057 by the Telecommunications Industry Association (TIA).

The remaining statements are explained separately. See CLI Explorer.

Default

Disabled.

Required Privilege Level

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

Related Documentation

- show lldp on page 1826
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Configuring LLDP-MED (CLI Procedure) on page 521

lldp-med-bypass

Syntax
```
lldp-med-bypass;
```

Hierarchy Level
```
[edit protocols dot1x authenticator interface (all | interface-name )]
```

Release Information
Statement introduced in Junos OS Release 12.3 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description
Bypass the 802.1X authentication procedure for connecting multiple LLDP-MED end devices. Automatically add the learned MAC addresses of the end devices to the switch's static MAC bypass list, and allow the devices to access the network. You can enable **lldp-med-bypass** only when the interface is also configured for 802.1X authentication of *multiple* supplicants.

Default
Disabled

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

Related Documentation
- supplicant on page 1514
- Understanding Authentication on Switches on page 268

lldp-priority

Syntax
```
lldp-priority;
```

Hierarchy Level
```
[edit poe],
[edit poe fpc (all | slot-number)]
```

Release Information
Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description
Configure the switch to assign interfaces the power priority provided by the powered device by using Link Layer Discovery Protocol (LLDP) power negotiation rather than the power priority configured on the switch interface.

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

Related Documentation
- *Configuring PoE on EX Series Switches (CLI Procedure)*

lldp-tx-fast-init

Syntax lldp-tx-fast-init *seconds*;

Hierarchy Level [edit protocols lldp],

Release Information Statement introduced in Junos OS Release 15.1R5 for EX Series switches.

Description Configure the interval between transmissions to be made during a fast transmission period. A device that is enabled with Link Layer Discovery Protocol (LLDP) transmits LLDP packets to neighboring nodes at a specified time interval. Fast transmission periods are initiated when a new neighbor is detected, and cause LLDP packets to be transmitted at a shorter time interval than during normal operation of the protocol. The fast transmission period ensures that more than one LLDP packet is transmitted when a new neighbor is detected. The first transmission is immediate, and the subsequent transmissions occur at the specified fast transmission (TX) interval.

Options ***seconds***—Specify the number of seconds between transmissions that occur during the fast transmission period.

Range: 1 through 8 seconds

Default: 1 second

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

Related Documentation

- show lldp on page 1826
- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518
- Understanding LLDP on page 511

load-key-file

Syntax

load-key-file *URL filename*;

Hierarchy Level

[edit system root-authentication],
[edit system login user *username* authentication]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

NOTE: ECDSA is not supported on the QFabric system.

Load RSA (SSH version 2) and DSA or ECDSA (SSH version 2) public keys from a previously-generated named file at a specified URL location or local path. The file contains one or more SSH keys that are copied into the configuration when the command is issued.

Options

URL filename—The URL filename of the key file to be loaded.

Required Privilege Level

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

Related Documentation

- Configuring the Root Password on page 140
- *Configuring the Root Password*
- Configuring Junos OS User Accounts by Using a Configuration Group on page 76

local

Syntax

```
local certificate-name {
  certificate-key-string;
  load-key-file URL filename;
}
```

Hierarchy Level

[edit security certificates]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Import a paired X.509 private key and authentication certificate, to enable Junos XML protocol client applications to establish Secure Sockets Layer (SSL) connections to the router or switch.

NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard.

Options

certificate-key-string—String of alphanumeric characters that constitute the private key and certificate.

certificate-name—Name that uniquely identifies the certificate.

load-key-file *URL filename*—File that contains the private key and certificate. It can be one of two types of values:

- Pathname of a file on the local disk (assuming you have already used another method to copy the certificate file to the router's or switch's local disk)
- URL to the certificate file location (for instance, on the computer where the Junos XML protocol client application runs)

Required Privilege Level

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

Related Documentation

- *Importing SSL Certificates for Junos XML Protocol Support*

local-certificate

Syntax

local-certificate *name*;

Hierarchy Level

[edit system services service-deployment],
[edit system services web-management https],
[edit system services xnm-ssl],
[edit system services extension-servicee request-response thrift]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced for the **[edit system services extension-service request-response thrift]** hierarchy level in Junos OS Release 16.1 for MX80, MX480, MX960, MX2010, MX2020, vMX, and PTX Series

Description

Import or reference an SSL certificate.

Specify the name of the local certificate to use. There is no default for **local-certificate**. The value for **local-certificate** should be the same as the name provided during the import of the certificate using the CLI configuration statement **local** at the **[edit security certificates]** hierarchy level.

Required Privilege Level

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

Related Documentation

- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*
- *Importing SSL Certificates for Junos XML Protocol Support*
- local on page 1202

local-server-group (DHCP Relay Agent Option)

Syntax

```
local-server-group local-server-group;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option (default-action | equals | starts-with)],
[edit forwarding-options dhcp-relay group group-name relay-option (default-action | equals
  | starts-with)],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Forward DHCP client packets to the specified group of DHCP local servers when you use the DHCP relay selective processing feature. You can configure the forwarding operation globally or for a group of interfaces.

The **local-server-group** option is not supported for DHCPv6 relay agent.

Options

local-server-group—Name of DHCP local server group.

Required Privilege Level

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

Related Documentation

- *Using DHCP Option Information to Selectively Process DHCP Client Traffic*

location

Syntax

```
location {
  altitude feet;
  building name;
  country -code code;
  floor number;
  hcoord horizontal-coordinate;
  lata service-area;
  latitude degrees;
  longitude degrees;
  npa-nxx number;
  postal-code postal-code;
  rack number;
  vcoord vertical-coordinate;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 8.5.

Description Configure the physical location of the device.

Options

- **altitude** ***feet***—Number of feet above sea level.
- **building** ***name***—Name of building. The name of the building can be 1 to 28 characters in length. If the string contains spaces, enclose it in quotation marks (" ").
- **country-code** ***code***—Two-letter country code.
- **floor** ***number***—Floor number in the building.
- **hcoord** ***horizontal-coordinate***—Bellcore Horizontal Coordinate.
- **lata** ***service-area***—Long-distance service area.
- **latitude** ***degrees***—Latitude in degree format.
- **longitude** ***degrees***—Longitude in degree format.
- **npa-nxx** ***number***—First six digits of the phone number (area code and exchange).
- **postal-code** ***postal-code***—Zip code or Postal code.
- **rack** ***number***—Rack number.
- **vcoord** ***vertical-coordinate***—Bellcore Vertical Coordinate.

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

location (SNMP)

Syntax

```
location location;
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Define the value of the MIB II **sysLocation** object, which is the physical location of the managed system.

Options

location—Location of the local system. You must enclose the name within quotation marks (" ").

Required Privilege Level

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

Related Documentation

- *Configuring the System Location for a Device Running Junos OS*

location (LLDP-MED)

Syntax

```
location {
  elin number;
  civic-based {
    what number;
    country-code code;
    ca-type{
      number {
        ca-value value;
      }
    }
  }
}
```

Hierarchy Level

[edit protocols lldp-med interface (all | *interface-name*)]

Release Information

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

Description

For Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED), configure the location information. Location information is advertised from the switch to the MED. This information is used during emergency calls to identify the location of the MED.

The remaining statements are explained separately. See CLI Explorer.

Default

Disabled.

Required Privilege Level

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

Related Documentation

- show lldp on page 1826
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Configuring LLDP-MED (CLI Procedure) on page 521

lockout-period

Syntax lockout-period *minutes*;

Hierarchy Level **[edit system login** retry-options**]**

Release Information Statement introduced in Junos OS Release 11.2.

Description Configure the amount of time before the user can attempt to log in to the router after being locked out due to the number of failed login attempts specified in the **tries-before-disconnect** statement.

Options *minutes*—Amount of time before the user can attempt to log in after being locked out.
Default: Off
Range: 1 through 43200

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

Related Documentation

- Limiting the Number of User Login Attempts for SSH and Telnet Sessions
- Login Retry Options on page 59
- Example: Configuring Login Retry Options on page 62
- **retry-options on page 1428**
- **clear system login lockout on page 1669**
- **show system login lockout on page 1967**

log

Syntax

```
log {
  session {
    client;
    all;
    dhcpv6 {
      client;
      server;
      relay;
      dynamic-server;
      all;
    }
    server;
    relay;
  }
}
```

Hierarchy Level

```
[edit system processes dhcp-service]
```

Release Information

Statement introduced in Junos OS Release 19.1R1 for SRX Series devices.

Description

Enable DHCP session log on the device. Session logs include the information on the session creation, deletion and renew events. You can use the session logs for monitoring and troubleshooting purposes.

Options

- **session**—Logs of the DHCP sessions.
- **client**—Log sessions of the DHCP client.
- **all**—Log sessions of the DHCP client, server and relay.
- **dhcpv6**—Log sessions of the DHCPv6.
- **client**—Log sessions of the DHCPv6 client.
- **dynamic-server**—Log sessions of the DHCPv6 dynamic server.
- **all**—Log sessions of the DHCPv6 client, server, relay and dynamic server.
- **server**—Log sessions of the DHCP server.
- **relay**—Log sessions of the DHCP relay.

Required Privilege Level

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

Related Documentation

- dhcp-service on page 1010

logical-system-name (DHCP Local Server)

Syntax

```
logical-system-name;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the logical system name be concatenated with the username during the subscriber authentication or DHCP client process. No logical system name is concatenated if the configuration is in the default logical system.

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651

login

Syntax

```
login {
  announcement text;
  class class-name {
    allow-commands "regular-expression";
    allow-configuration-regexps "regular expression 1" "regular expression 2";
    cli {
      prompt name;
    }
    configuration-breadcrumbs;
    deny-commands "regular-expression";
    ( deny-configuration | deny-configuration-regexps ) “regular expression 1” “regular
      expression 2 ”;
    idle-timeout minutes;
    login-script filename;
    login-tip;
    permissions [ permissions ];
  }
  message text;
  password {
    change-type (set-transitions | character-set);
    format (md5 | sha1 | des);
    maximum-length length;
    minimum-changes number;
    minimum-length length;
  }
  retry-options {
    backoff-threshold number;
    backoff-factor seconds;
    minimum-time seconds;
    tries-before-disconnect number;
  }
  user username {
    authentication {
    cli {
      prompt name;
    }
    class class-name;
    (encrypted-password "password" | plain-text-password);
    full-name complete-name;
    load-key-file URL filename;
    ssh-dsa “public-key” <from hostname>;
    ssh-rsa “public-key” <from hostname>;
    uid uid-value;
  }
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced before Junos OS Release 7.4.

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

Description Configure user access to the router or switch.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

Related Documentation
- Defining Junos OS Login Classes on page 53

login-alarms

Syntax

```
login-alarms;
```

Hierarchy Level

```
[edit system login class class-name]
```

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Show system alarms automatically when an **admin** user logs in to the router or switch.

Options ***class-name***—Login class name.

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

Related Documentation
- Configuring System Alarms to Appear Automatically Upon Login on page 56

login-script (Op Scripts)

Syntax login-script *filename*;

Hierarchy Level [edit system login class *class-name*]

Release Information Statement introduced in Junos OS Release 9.5.

Description Execute the specified op script when a user belonging to the class logs in to the CLI. The script must be enabled in the configuration.

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

Related Documentation
- *Executing an Op Script*

login-tip

Syntax login-tip;

Hierarchy Level [edit system login class *class-name*]

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

Description Enable CLI tips at login.

Default Disabled.

Options This command has no options.

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

Related Documentation
- Configuring Login Tips on page 57

log-key-changes

Syntax log-key-changes *log-key-changes*;

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 17.4R1.

Description Enable the **log-key-changes** to log the authorised SSH keys. When the **log-key-changes** configuration statement is enabled and committed, Junos OS logs the changes to the set of authorized SSH keys for each user (including the keys that were added or removed). Junos OS logs the differences since the last time the **log-key-changes** configuration statement was enabled. If the **log-key-changes** configuration statement was never enabled, then Junos OS logs all the authorized SSH keys.

Required Privilege Level admin

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 232

mac-radius

Syntax

```
mac-radius <flap-on-disconnect> <restrict>;
```

Hierarchy Level

[edit protocols dot1x authenticator interface *interface-name*]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Option **flap-on-disconnect** introduced in Junos OS Release 9.4 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure MAC RADIUS authentication for specific interfaces. MAC RADIUS authentication allows LAN access to permitted MAC addresses. When a new MAC address appears on an interface, the switch consults the RADIUS server to check whether the MAC address is a permitted address. If the MAC address is configured on the RADIUS server, the device is allowed access to the LAN.

If MAC RADIUS is configured, the switch first tries to get a response from the host for 802.1X authentication. If the host is unresponsive, the switch attempts to authenticate using MAC RADIUS.

To restrict authentication to MAC RADIUS only, use the **restrict** option. In restrictive mode, all 802.1X packets are eliminated and the attached device on the interface is considered a nonresponsive host.

Options

flap-on-disconnect—(Optional) When the RADIUS server sends a disconnect message to a supplicant, the switch resets the interface on which the supplicant is authenticated. If the interface is configured for multiple supplicant mode, the switch resets all the supplicants on the specified interface. This option takes effect only when the **restrict** option is also set.

restrict—(Optional) Restricts authentication to MAC RADIUS only. When **mac-radius restrict** is configured the switch drops all 802.1X packets. This option is useful when no other 802.1X authentication methods, such as guest VLAN, are needed on the interface, and eliminates the delay that occurs while the switch determines that a connected device is a non-802.1X-enabled host.

Required Privilege Level

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

Related Documentation

- show dot1x on page 1799
- Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 326
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Configuring MAC RADIUS Authentication (CLI Procedure) on page 325

- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- Understanding Authentication on Switches on page 268

macs

Syntax macs [*algorithm1 algorithm2*...]

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 11.2.
SHA-2 options introduced in Junos OS Release 12.1.

Description Specify the set of message authentication code (MAC) algorithms that the SSH server can use to authenticate messages.

Options Specify one or more of the following MAC algorithms to authenticate messages:

- **hmac-md5**—Hash-based MAC using Message-Digest 5 (MD5)
- **hmac-md5-96**—96-bits of hash-based MAC using MD5
- **hmac-md5-96-etm@openssh.com**—96-bits of hash-based Encrypt-then-MAC using MD5
- **hmac-md5-etm@openssh.com**—Hash-based Encrypt-then-MAC using MMD5
- **hmac-ripemd160**—Hash-based MAC using RIPEMD
- **hmac-ripemd160-etm@openssh.com**—Hash-based Encrypt-then-MAC using RIPEMD
- **hmac-sha1**—Hash-based MAC using secure hash algorithm-1 (SHA-1)
- **hmac-sha1-96**—96-bits of hash-based MAC using SHA-1
- **hmac-sha1-96-etm@openssh.com**—96-bits of hash-based Encrypt-then-MAC using SHA-1
- **hmac-sha1-etm@openssh.com**—Hash-based Encrypt-then-MAC using SHA-1
- **hmac-sha2-256**—256-bits of hash-based MAC using secure hash algorithm-2 (SHA-2)
- **hmac-sha2-256-etm@openssh.com**—Hash-based Encrypt-then-Mac using SHA-2
- **hmac-sha2-512**—512-bits of hash-based MAC using SHA-2
- **hmac-sha2-512-etm@openssh.com**—Hash-based Encrypt-then-Mac using SHA-2
- **umac-128-etm@openssh.com**—Encrypt-then-MAC using UMAC-128 algorithm specified in RFC4418
- **umac-128@openssh.com**—UMAC-128 algorithm specified in RFC4418
- **umac-64-etm@openssh.com**—Encrypt-then-MAC using UMAC-64 algorithm specified in RFC4418
- **umac-64@openssh.com**—UMAC-64 algorithm specified in RFC4418

NOTE: The *macs* configuration statement represents a set. Therefore, it must be configured as shown in the following example.

```
user@host#set system services ssh macs [hmac-md5 hmac-sha1]
```

Required Privilege Level

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

Related Documentation

- key-exchange on page 1185
- ciphers on page 929

mac-address (DHCP Local Server)

Syntax

```
mac-address;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support for DHCPv6 added in Junos OS Release 17.2 for MX Series Routers.

Description

Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process.

For DHCPv6 clients, because the DHCPv6 packet format has no specific field for the client MAC address, the MAC address is derived from among several sources with the following priority:

- Client DUID Type 1 or Type 3.
- Option 79 (client link-layer address), if present.
- The packet source address if the client is directly connected.
- The link local address.

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651

mac-address (DHCP Relay Agent)

Syntax

```
mac-address;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication
  username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support for DHCPv6 added in Junos OS Release 17.2 for MX Series Routers.

Description

Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication or client authentication process.

For DHCPv6 clients, because the DHCPv6 packet format has no specific field for the client MAC address, the MAC address is derived from among several sources with the following priority:

- Client DUID Type 1 or Type 3.
- Option 79 (client link-layer address), if present.
- The packet source address if the client is directly connected.
- The link local address.

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651

management-address

Syntax management-address *ip-management-address*;

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 9.5 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify the management address to be used in LLDP Management Address type, length, and value (TLV) messages. The Management Address TLV typically contains the IPv4 or IPv6 management addresses of the local system. Only out-of-band management addresses must be used for the management-address. Other remote managers can use this address to obtain information related to the local device.

Default The LLDP Management Address TLV uses the IP address of the switch's management Ethernet interface (**me0**), or the IP address of the virtual management Ethernet (VME) interface if the switch is a Virtual Chassis member.

Options ***ip-management-address***—You can specify either an IPv4 or an IPv6 management address for the switch.

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

Related Documentation

- show lldp on page 1826
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518
- *Interfaces Overview for Switches*
- Understanding LLDP on page 511

master-password

Syntax

```
master-password {
  plain-text-password
  iteration-count iteration-count;
  pseudorandom-function (hmac-sha1 | hmac-sha2-256 | hmac-sha2-512);
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced in Junos OS Release 16.2.

Description

Master password for 8-based password-encryption. The master password is used as input to the password based key derivation function (PBKDF2) to generate an encryption key. the key is used as input to the Advanced Encryption Standard in Galois/Counter Mode (AES256-GCM). The plain text that the user enters is processed by the encryption algorithm (with key) to produce the encrypted text (cipher text).

Options

plain-text-password—Set the master password with plain text. The password quality is evaluated for strength, and the device gives feedback if weak passwords are used.

iteration-count—The number of iterations to use for the PBKDF2 hash function. The iteration count slows the hashing count, thus slowing attacker guesses.

Default: 100

Range: 10-10000

pseudorandom-function—Choose the algorithm to use for unpredictable number generation

Values:

- **hmac-sha1**—Hash-based MAC using secure hash algorithm-1 (SHA-1)
- **hmac-sha2-256**—256-bits of hash-based MAC using SHA-2
- **hmac-sha2-512**—512-bits of hash-based MAC using SHA-2

Required Privilege Level

admin

Related Documentation

- Hardening Shared Secrets in Junos OS on page 155
- request system decrypt password on page 1694

max-outstanding-requests (Diameter Applications)

Syntax

```
max-outstanding-requests number;
```

Hierarchy Level

```
[edit access gx-plus global],
[edit access ocs partition partition-name],
[edit access pcrf partition partition-name]
```

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for OCS and PCRF partitions introduced in Junos OS Release 16.2 for MX Series routers.

Description

Limit the number of outstanding requests that the Diameter-based application (function) can retry to a remote server when the requests are improperly answered. Too many requests risks overloading the server and increases the chance of losing messages.

The **gx-plus** statement limits retries from the Gx-Plus function to the Gx-Plus server using the Gx and JSRC protocols. The **ocs** statement limits retries from the OCS function to the OCS server using the Gy protocol. The **pcrf** statement limits retries from the PCRF function to the PCRF server using the Gx protocol.

Options

number—Number of outstanding requests from the function to the server that can exist at any time.

Default: 40

Range: 2 through 40

Required Privilege Level

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

Related Documentation

- *Configuring Gx-Plus Global Attributes*
- *Configuring Gx-Plus*
- *Configuring the OCS Partition*
- *Configuring the PCRF Partition*
- *Understanding Gx Interactions Between the Router and the PCRF*
- *Understanding Gy Interactions Between the Router and the OCS*

max-pre-authentication-packets

Syntax max-pre-authentication-packets *value*;

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 12.3X48-D10.

Description Define the number of pre-authentication SSH packets that the SSH server will accept prior to user authentication.

Options ***value***—Maximum number of pre-authentication SSH packets that the server will accept.

Range: 20 through 2147483647.

Default: 128

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

Related Documentation

- The ssh Command on page 236

max-sessions-per-connection

Syntax max-sessions-per-connection *number*

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Release 11.4 of Junos OS.

Description Specify the maximum number of ssh sessions allowed per single SSH connection.

Options **Default:** 10

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

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 232
- ssh on page 1495
- *Junos OS Security Configuration Guide*

mau-type

Syntax mau-type;

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 15.1 for EX Series switches.

Description Configure the switch to advertise information about the medium attachment unit (MAU) type. The MAU is a transceiver that interconnects the attachment unit interface (AUI) port on an attached host computer to an Ethernet cable. MAU types are defined in the IEEE 802.3 standard.

The MAU type is included in the MAC/PHY Configuration Status type, length, and value (TLV) message. TLVs are used by LLDP-capable devices to transmit information to neighbor devices. The MAC/PHY Configuration Status TLV is an organizationally defined TLV that advertises information about the physical interface. In addition to the MAU type, the MAC/PHY Configuration Status TLV also includes information such as autonegotiation status, support and advertised capabilities.

The MAU type cannot be changed by configuration; however, you must configure the **mau-type** statement to include the MAU type value in the MAC/PHY Configuration Status TLV.

Default If the **mau-type** statement is not configured, the MAU type field of the MAC/PHY Configuration Status TLV contains the value **Unknown**.

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

Related Documentation

- Understanding LLDP and LLDP-MED on EX Series Switches on page 518
- *Configuring LLDP*

maximum-certificates

Syntax maximum-certificates *number*;

Hierarchy Level [edit security certificates]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the maximum number of peer digital certificates to be cached.

Options ***number***—Maximum number of peer digital certificates to be cached.

Range: 64 through 4,294,967,295 peer certificates

Default: 1024 peer certificates

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

Related Documentation

- *Configuring the Maximum Number of Peer Certificates*

maximum-hop-count

Syntax
maximum-hop-count *number*;

Hierarchy Level
[edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface (*interface-name* | *interface-group*)]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

Description
Set the maximum allowed number of hops. This value is compared against the hops field in the BOOTP request message. BOOTP request messages that have a number in the hops field that exceeds **maximum-hop-count** are not forwarded. If you omit the **maximum-hop-count** statement, the default value is four hops.

Options
number—Maximum number of hops for BOOTP request messages.
Range: 1 through 16
Default: 4

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

Related Documentation
- *Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents*

maximum-lease-time (DHCP)

Syntax maximum-lease-time *seconds*;

Hierarchy Level [edit system services dhcp],

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

Description For J Series Services Routers and EX Series switches only. Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.

An exception is that the dynamic BOOTP lease length can exceed the maximum lease length specified.

Options ***seconds***—The maximum number of seconds the lease can be held.

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

maximum-lease-time (DHCP)

Syntax maximum-lease-time *seconds*;

Hierarchy Level [edit system services dhcp],

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

Description For J Series Services Routers and EX Series switches only. Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.

An exception is that the dynamic BOOTP lease length can exceed the maximum lease length specified.

Options ***seconds***—The maximum number of seconds the lease can be held.

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

maximum-length

Syntax maximum-length *length*;

Hierarchy Level [edit system login passwords]

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

Description Specify the maximum number of characters allowed in plain-text passwords. Newly created passwords must meet this requirement.

Default For Junos-FIPS software, the maximum number of characters for plain-text passwords is 20. For Junos OS, no maximum is set.

Options **length**—The maximum number of characters the password can include.
Range: 1 to 64 characters

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

Related Documentation

- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 153
- password (Login) on page 1327

maximum-lifetime

Syntax maximum-lifetime *days*;

Hierarchy Level [edit system login passwords]

Release Information Statement introduced in Junos OS Release 18.4R1 for ACX Series, EX Series, QFX Series, MX Series, PTX Series.

Description Specify the maximum password lifetime in days. A user who has the required permissions is able to control the maximum lifetime of a password. If the age of the password reaches the maximum lifetime configured, the password expires and has to be changed. If your password has expired, you cannot commit the configuration until the password is changed. Password expiry is applicable only for local user accounts.

NOTE: You cannot configure the same password every time the password expires. Older passwords cannot be configured on password expiry. Therefore, **maximum-lifetime** can be committed only after configuring minimum-reuse, else commit fails and error is displayed on commit.

If **maximum-lifetime** is configured, password expiry validation check is performed at the time of login and at the time of commit based on the password timestamp. For passwords configured before minimum-reuse configuration is committed, the timestamp of the passwords is the time at which any configuration under system login hierarchy is committed following the commit for minimum-reuse. For passwords configured after minimum-reuse configuration is committed, the timestamp of the passwords is the time at which those passwords are committed.

Options **days**—The maximum duration of a password where the password expires after the maximum duration is reached.

Range: 30-365

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

Related Documentation

- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 153
- password (Login) on page 1327

maximum-requests

Syntax maximum-requests *number*;

Hierarchy Level [edit protocols dot1x authenticator interface (all | [*interface-names*])]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description For 802.1X authentication, configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out.

Default Two retransmission attempts

Options ***number***—Number of retransmission attempts.
Range: 1 through 10
Default: 2

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

Related Documentation
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- *Configuring 802.1X Authentication (J-Web Procedure)*

maximum-time

Syntax maximum-time *seconds*;

Hierarchy Level **[edit system login** retry-options**]**

Release Information Statement introduced in Junos OS Release 9.6.

Description Configure the maximum time available for the user to enter the username and password for logging on to a router before the connection is closed.

Options *seconds*—Maximum length of time that the connection remains open for the user to enter a username and password to log in. If the user remains idle and does not enter a username and password within the configured **maximum-time**, the connection is closed.

Range: 20 through 300

Default: 120

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

Related Documentation

- Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 60
- retry-options on page 1428

method

Syntax

```
method {
  bfd {
    version (0 | 1 | automatic);
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    transmit-interval {
      minimum-interval milliseconds;
      threshold milliseconds;
    }
    detection-time {
      threshold milliseconds;
    }
    session-mode (automatic | multihop | singlehop);
    holddown-interval milliseconds;
  }
  layer2-liveness-detection {
    max-consecutive-retries number;
    transmit-interval interval;
  }
}
```

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 group *group-name* liveness-detection],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection],
[edit forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name* liveness-detection],
[edit forwarding-options dhcp-relay group *group-name* liveness-detection],
[edit forwarding-options dhcp-relay liveness-detection],
[edit system services dhcp-local-server dhcpv6 group *group-name* liveness-detection],
[edit system services dhcp-local-server dhcpv6 liveness-detection],
[edit system services dhcp-local-server dual-stack-group *dual-stack-group-name* liveness-detection],
[edit system services dhcp-local-server group *group-name* liveness-detection],
[edit system services dhcp-local-server liveness-detection]

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the liveness detection method.

NOTE: The bfd stanza is not available at the [edit forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name* liveness-detection method] or [edit system services dhcp-local-server dual-stack-group *dual-stack-group-name* liveness-detection hierarchy levels.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

Related Documentation
- DHCP Liveness Detection Overview on page 674
- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677
- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets on page 686

message

Syntax
```
message text;
```

Hierarchy Level
```
[edit system login]
```

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 system login message. This message appears before a user logs in.

You can format the message using the following special characters:

- \n—New line
- \t—Horizontal tab
- \'—Single quotation mark
- \"—Double quotation mark
- \\—Backslash

Options
text—Text of the message.

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

Related Documentation
- *Configuring Junos OS to Display a System Login Message*
- announcement on page 875

mib-profile

Syntax

```
mib-profile profile-name {
  file filename;
  interval minutes;
  object-names {
    mib-object-name;
  }
  operation operation-name;
}
```

Hierarchy Level

```
[edit accounting-options]
```

Release Information

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Create a MIB profile to collect selected MIB statistics and write them to a file in the **/var/log** directory.

NOTE: Do not configure MIB objects related to interface octets or packets for a MIB profile, because it can cause the SNMP walk or a CLI show command to time out.

Options

profile-name—Name of the MIB statistics profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring the MIB Profile*

minimum-changes

Syntax minimum-changes *number*;

Hierarchy Level [edit system login passwords]

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

Description Specify the minimum number of character sets (or character set changes) required in plain-text passwords. Newly created passwords must meet this requirement.

This statement is used in combination with the **change-type** statement. If the change-type is **character-sets**, then the number of character sets included in the password is checked against the specified minimum. If change-type is **set-transitions**, then the number of character set changes in the password is checked against the specified minimum.

Default For Junos OS, the minimum number of changes is 1. For Junos-FIPS Software, the minimum number of changes is 3.

Options *number*—The minimum number of character sets (or character set changes) required for the password.

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

Related Documentation

- change-type on page 927

minimum-character-changes

Syntax minimum-character-changes *number*;

Hierarchy Level [edit system login passwords]

Release Information Statement introduced in Junos OS Release 18.3R1.

Description Specify the minimum number of character changes between old and new passwords. Newly created passwords must meet this requirement. A user who has the required permissions is able to configure the number of character changes between passwords. If the number of character changes between the old password and new password is greater than or equal to the configured value for minimum number of character changes, new password is accepted and if it is less, new password is rejected.

Options **number**—The minimum number of character changes between old and new passwords.
Range: 4 to 15 characters

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

Related Documentation
- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 153
- password (Login) on page 1327

minimum-interval

Syntax

```
minimum-interval milliseconds;
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd
  transmit-interval],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd
  transmit-interval],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method
  bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method
  bfd transmit-interval],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd
  transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method
  bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method
  bfd transmit-interval]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the minimum intervals at which the local routing device transmits hello packets and then expects to receive a reply from a neighbor with which it has established a BFD session. This value represents the minimum interval at which the local routing device transmits hello packets as well as the minimum interval that the routing device expects to receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can specify the minimum transmit and receive intervals separately using the **transmit-interval minimal-interval** and **minimum-receive-interval** statements.

Options

milliseconds — Specify the minimum interval value for BFD liveliness detection.

Range: 1 through 255,000

Required Privilege Level

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

Related Documentation

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677

minimum-length

Syntax

```
minimum-length length;
```

Hierarchy Level

```
[edit system login passwords]
```

Release Information

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

Description

Specify the minimum number of characters required in plain-text passwords. Newly created passwords must meet this requirement.

This statement can be used in combination with all of the other requirement options for plain-text passwords, such as **minimum-upper-cases**, **minimum-punctuations**, **minimum-lower-cases,** and so on.

Using several password minimum requirement options will cause the **minimum-length** to be reset if the total sum of the required minimums exceeds the **minimum-length** setting.

Default

For Junos OS, the minimum number of characters for plain-text passwords is six. For Junos-FIPS software, the minimum number of characters for plain-text passwords is 10.

Options

length—The minimum number of characters the password must include.

Range: 6 to 20 characters

Required Privilege Level

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

Related Documentation

- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 153
- maximum-length on page 1229

minimum-lifetime

Syntax minimum-lifetime *days*;

Hierarchy Level [edit system login passwords]

Release Information Statement introduced in Junos OS Release 18.4R1 for ACX Series, EX Series, QFX Series, MX Series, PTX Series.

Description Specify the minimum password lifetime in days. A user who has the required permissions is able to control the minimum lifetime of a password. You cannot change the password if the age of the password does not exceed the minimum lifetime value configured. When you change a password, the age of the existing password is retrieved based on the time at which the password was configured and the current time is fetched. If the age of the password is less than or equal to the configured value for **minimum-lifetime**, the new password is not accepted and error message is displayed. If the age of the password is more than the configured value for **minimum-lifetime**, the new password is accepted. .

NOTE: **minimum-lifetime** can be committed only after configuring minimum-reuse as **minimum lifetime** works in coordination with password history requirements, else commit fails and error is displayed on commit.

If **minimum-lifetime** is configured, password change for a user is accepted or rejected based on the timestamp of the current password for that user. For passwords configured before minimum-reuse configuration is committed, the timestamp of the passwords is the time at which any configuration under system login hierarchy is committed following the commit for minimum-reuse. For passwords configured after minimum-reuse configuration is committed, the timestamp of the passwords is the time at which those passwords are committed.

Options **days**—The minimum duration of a password. You cannot change the password until the minimum duration is reached.

Range: 1-30 days

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

Related Documentation

- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 153
- password (Login) on page 1327

minimum-lower-cases

Syntax minimum-lower-cases *number*;

Hierarchy Level [edit system login password]

Release Information Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify the minimum number of lower-case letters required in plain-text passwords. Newly created passwords must meet this requirement.

This statement can be used in combination with all of the other requirement options for plain-text passwords, such as **minimum-length**, **minimum-punctuations**, **minimum-upper-cases,** and so on.

Using several password minimum requirement options will cause the **minimum-length** to be reset if the total sum of the required minimums exceeds the **minimum-length** setting.

Options *number*—The minimum number of lower-case letters required for the password.

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

Related Documentation

- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 153
- password (Login) on page 1327

minimum-numerics

Syntax minimum-numerics *number*;

Hierarchy Level [edit system login password]

Release Information Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify the minimum number of numeric class characters required in plain-text passwords. Newly created passwords must meet this requirement.

This statement can be used in combination with all of the other requirement options for plain-text passwords, such as **minimum-length**, **minimum-punctuations**, **minimum-lower-cases,** and so on.

Using several password minimum requirement options will cause the **minimum-length** to be reset if the total sum of the required minimums exceeds the **minimum-length** setting.

Options *number*—The minimum number of numeric class characters required for the password.

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

Related Documentation

- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 153
- password (Login) on page 1327

minimum-reuse

Syntax minimum-reuse *number*;

Hierarchy Level [edit system login passwords]

Release Information Statement introduced in Junos OS Release 18.3R1.

Description Specify the the number of old passwords which should not match the new password. Newly created passwords must meet this requirement. A user who has the required permissions is able to control the number of old passwords that need to be compared. The number of old passwords to compare with the new password depends on the value configured. If a match is found between the new password and any of the old passwords, Junos OS device rejects the new password and aborts. If the new password is different from the configured number of old passwords, new password is accepted.

Options **number**—The minimum number of old passwords which should not match the new password.

Range: 1 to 20 passwords

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

Related Documentation

- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 153
- password (Login) on page 1327

minimum-punctuations

Syntax minimum-punctuations *number*;

Hierarchy Level [edit system login password]

Release Information Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify the minimum number of punctuation class characters required in plain-text passwords. Newly created passwords must meet this requirement.

This statement can be used in combination with all of the other requirement options for plain-text passwords, such as **minimum-length**, **minimum-upper-cases**, **minimum-lower-cases,** and so on.

Using several password minimum requirement options will cause the **minimum-length** to be reset if the total sum of the required minimums exceeds the **minimum-length** setting.

Options *number*—The minimum number of punctuation class characters required for the password.

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

Related Documentation

- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 153
- password (Login) on page 1327

minimum-receive-interval

Syntax

```
minimum-receive-interval milliseconds;
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options
  dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method
  bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method
  bfd]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the minimum interval at which the local routing device (or switch) must receive a reply from a neighbor with which it has established a BFD session.

Options

milliseconds — Specify the minimum receive interval value.

Range: 1 through 255,000

Required Privilege Level

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

Related Documentation

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677

minimum-time

Syntax minimum-time *seconds*;

Hierarchy Level [edit system login retry-options]

Release Information Statement introduced in Junos OS Release 8.0.

Description Configure the minimum time available for the user to enter a password to log on to a router before the connection is closed.

Options *seconds*—Minimum length of time that the connection remains open while the user is attempting to enter a password to log in.

Range: 20 through 60

Default: 20

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

Related Documentation

- Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 60
- retry-options on page 1428

minimum-upper-cases

Syntax minimum-upper-cases *number*;

Hierarchy Level [edit system login password]

Release Information Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify the minimum number of upper-case letters required in plain-text passwords. Newly created passwords must meet this requirement.

This statement can be used in combination with all of the other requirement options for plain-text passwords, such as **minimum-length**, **minimum-punctuations**, **minimum-lower-cases,** and so on.

Using several password minimum requirement options will cause the **minimum-length** to be reset if the total sum of the required minimums exceeds the **minimum-length** setting.

Options *number*—The minimum number of upper-case letters required for the password.

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

Related Documentation

- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 153
- password (Login) on page 1327

minimum-wait-time

Syntax

```
minimum-wait-time seconds;
```

Hierarchy Level

```
[edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface (interface-name | interface-group)]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

Description

To set the minimum allowed number of seconds in the secs field of the BOOTP message, include the minimum-wait-time statement. This setting configures a minimum number of seconds since the client sent its first BOOTP request. BOOTP messages that have a smaller number in the secs field than the allowed minimum are not forwarded. The default value for the minimum wait time is zero (0).

The default value for the minimum wait time is zero (0) seconds. If the minimum wait time is 0 and the secs field in the BOOTP request message is 0, the device forwards the packet.

Options

seconds—Minimum wait time the BOOTP client has waited before packets are forwarded.

Range: 0 to 30,000

Default: 0

Required Privilege Level

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

Related Documentation

- *Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents*

multi-domain

Syntax

```
multi-domain {
  max-data-session max-data-sessions;
  packet-action (drop-and-log | shutdown);
  recovery-timeout seconds;
}
```

Hierarchy Level

[edit protocols dot1x authenticator interface *interface-name*]

Release Information

Statement introduced in Junos OS Release 18.3R1.

Description

Configure multi-domain authentication to restrict the number of authenticated data and VoIP sessions on the port. Multi-domain authentication is an extension of multiple supplicant mode for 802.1X authentication, and is designed to support VoIP and data clients on the same interface. The interface is divided into two domains; one is the data domain and the other is the voice domain.

In multiple supplicant mode, any number of VoIP or data sessions can be authenticated; the number of sessions can be restricted using MAC limiting, but there is no way to apply the limit specifically to either data or VoIP sessions. Multi-domain authentication maintains separate session counts based on the domain type.

The data device can be authenticated using 802.1X authentication or MAC RADIUS authentication. Multi-domain authentication does not enforce the order of authentication. For best results, the VoIP device should be authenticated before the data device.

You can configure the maximum number of authenticated data sessions allowed on the interface using the **max-data-session** statement. The number of VoIP sessions is not configurable; only one authenticated VoIP session is allowed.

If a new client attempts to authenticate on the interface after the maximum session count has been reached, the default action is to drop the packet and generate an error log message. You can also configure the action to shut down the interface. The port can be manually recovered from the down state by issuing the **clear dot1x recovery-timeout** command, or can recover automatically after a recovery timeout period. To configure automatic recovery, use the **recovery-timeout** option.

Options

max-data-session *max-data-sessions*—The number of authenticated data sessions are allowed in the data domain on the 802.1X interface.

Range: 1 through 1,000 sessions

Default: 1

packet-action (drop-and-log | shutdown)—Define the action the switch should take on packets that exceed the limit of authenticated sessions allowed on the interface. The number of data sessions is configured using the **max-data-session** option. The

number of VoIP sessions is not configurable; only one authenticated VoIP session is allowed.

- **drop-and-log**—Drop the packet and generate an error syslog message.
- **shutdown**—Shut down the interface.

Default: The default packet action is to drop the packet and generate an error syslog message.

recovery-timeout *seconds*—If you configure the packet action with the shutdown option and you enable the recovery timeout, the interface is temporarily disabled when the maximum number of authenticated sessions is reached. The interface will recover automatically after the number of seconds specified.

Range: 60 through 3600 seconds

Default: none

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

Related Documentation
- authenticator on page 890
- *dot1x*
- interface (IEEE 802.1x) on page 1146

multicast-client

Syntax
```
multicast-client <address>;
```

Hierarchy Level
```
[edit system ntp]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For NTP, configure the SRX Series device to listen for multicast messages on the local network to discover other servers on the same subnet.

Options
address—(Optional) One or more IP addresses. If you specify addresses, the SRX Series device joins those multicast groups.

Default: 224.0.1.1.

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

Related Documentation
- *ntp*

multiplier

Syntax

```
multiplier number;
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method
  bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method
  bfd]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the number of hello packets not received by the neighbor before Bidirectional Forwarding Detection (BFD) declares the neighbor down.

Options

number—Maximum allowable number of hello packets missed by the neighbor.

Range: 1 through 255

Default: 3

Required Privilege Level

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

Related Documentation

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677

name

Syntax name *name*;

Hierarchy Level [edit snmp]

Release Information Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Set the system name from the command-line interface.

Options ***name***—System name override.

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

Related Documentation
- *Configuring a Different System Name*

name-server

Syntax

```
name-server {
  address {
    routing-instance routing-instance;
  }
}
```

Hierarchy Level

[edit system],
[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
routing-instance options introduced in Junos OS Release 19.2R1 under the **[edit system]** hierarchy level only.

Description

Configure one or more Domain Name System (DNS) name servers.

Options

address—Address of the name server. To configure multiple name servers, include a maximum of three ***address*** options.

routing-instance *routing-instance*—Configure name of the routing instance through which the name server is reachable.

NOTE: The only routing instance supported is mgmt_junos.

Required Privilege Level

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

Related Documentation

- *Configuring a DNS Name Server for Resolving a Hostname into Addresses*

name-server (Access)

Syntax name-server *address*

Hierarchy Level [edit access address-assignment pool <name> family (inet | inet6) xauth-attributes]

Release Information Statement introduced in Junos OS Release 10.4.

Description Specify the DNS server IP address for an address-assignment pool.

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

Related Documentation
- address-assignment (Access) on page 852

nas-ip-address

Syntax nas-ip-address *ip-address*;

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the NAS-IP address for outgoing RADIUS packets.

Options **ip-address**—IP address of the network access server (NAS) that requests user authentication.

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

Related Documentation
- Configuring RADIUS Server Authentication on page 182
- Configuring RADIUS Authentication (QFX Series or OCX Series) on page 192

nas-port-extended-format

Syntax

```
nas-port-extended-format {
  adapter-width bits;
  ae-width bits;
  atm {
    adapter-width bits;
    port-width bits;
    slot-width bits;
    vci-width bits;
    vpi-width bits;
  }
  port-width bits;
  pw-width bits;
  slot-width bits;
  stacked-vlan-width bits;
  vlan-width bits;
}
```

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.
ae-width option added in Junos OS Release 12.1.
atm option added in Junos OS Release 12.3R3 and supported in later 12.3R*x* releases.
atm option supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)
pw-width option added in Junos OS Release 15.1.

Description

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

The NAS-Port attribute specifies the physical port number of the NAS that is authenticating the user, and is formed by a combination of the physical port's slot number, port number, adapter number, VLAN ID, and S-VLAN ID. The NAS-Port extended format specifies the number of bits (bit width) for each field in the NAS-Port attribute: slot, adapter, port, aggregated, Ethernet, VLAN, and S-VLAN.

NOTE: The combined total of the widths of all fields for a subscriber 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.

Options

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

ae-width *width*—(Ethernet subscribers only) Number of bits in the aggregated Ethernet identifier field.

atm—Specify width for fields for ATM subscribers.

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

pw-width *width*—(Ethernet subscribers only) Number of bits in the pseudowire field. Appears in the Cisco NAS-Port-Info AVP (100).

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

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

vci-width *width*—(ATM subscribers only) Number of bits in the ATM virtual circuit identifier (VCI) field.

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

vpi-width *width*—(ATM subscribers only) Number of bits in the ATM virtual path identifier (VPI) field.

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

Required Privilege Level

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

Related Documentation

- *Configuring Access Profile Options for Interactions with RADIUS Servers*
- *RADIUS Servers and Parameters for Subscriber Access*

nas-port-extended-format

Syntax

```
nas-port-extended-format {
  adapter-width bits;
  ae-width bits;
  atm {
    adapter-width bits;
    port-width bits;
    slot-width bits;
    vci-width bits;
    vpi-width bits;
  }
  port-width bits;
  pw-width bits;
  slot-width bits;
  stacked-vlan-width bits;
  vlan-width bits;
}
```

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.
ae-width option added in Junos OS Release 12.1.
atm option added in Junos OS Release 12.3R3 and supported in later 12.3R*x* releases.
atm option supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)
pw-width option added in Junos OS Release 15.1.

Description

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

The NAS-Port attribute specifies the physical port number of the NAS that is authenticating the user, and is formed by a combination of the physical port's slot number, port number, adapter number, VLAN ID, and S-VLAN ID. The NAS-Port extended format specifies the number of bits (bit width) for each field in the NAS-Port attribute: slot, adapter, port, aggregated, Ethernet, VLAN, and S-VLAN.

NOTE: The combined total of the widths of all fields for a subscriber 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.

Options

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

ae-width *width*—(Ethernet subscribers only) Number of bits in the aggregated Ethernet identifier field.

atm—Specify width for fields for ATM subscribers.

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

pw-width *width*—(Ethernet subscribers only) Number of bits in the pseudowire field. Appears in the Cisco NAS-Port-Info AVP (100).

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

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

vci-width *width*—(ATM subscribers only) Number of bits in the ATM virtual circuit identifier (VCI) field.

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

vpi-width *width*—(ATM subscribers only) Number of bits in the ATM virtual path identifier (VPI) field.

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

Required Privilege Level

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

Related Documentation

- *Configuring Access Profile Options for Interactions with RADIUS Servers*
- *RADIUS Servers and Parameters for Subscriber Access*

nas-port-id-format (Subscriber Management)

Syntax

```
nas-port-id-format {
  agent-circuit-id;
  agent-remote-id;
  interface-description;
  interface-text-description;
  nas-identifier;
  order (agent-circuit-id | agent-remote-id | interface-description | interface-text-description
    | nas-identifier | postpend-vlan-tags);
  postpend-vlan-tags;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Options **interface-text-description**, **order**, and **postpend-vlan-tags** introduced in Junos OS Release 15.1.

Description

Specify the optional information that the router includes in the NAS-Port-ID (RADIUS attribute 87) that is passed to the RADIUS server during authentication and accounting. You can include any combination of the optional values.

When you specify the values for the NAS-Port-ID, you can configure the values to appear in either the default order or a custom order of your choice.

NOTE: The default and custom order methods are mutually exclusive. The configuration fails if you attempt to configure a NAS-Port-ID that includes values in both types of orders.

To specify that the optional values appear in the default order in the NAS-Port-ID, configure the values directly under the **nas-port-id-format** statement. The default order is as follows, in which the **#** character is the delimiter:

nas-identifier # interface-description # interface-text-description # agent-circuit-id # agent-remote-id # postpend-vlan-tags

To specify a custom order for the NAS-Port-ID string, you use the **order** option. Include the **order** option before each optional value you want to include in the string, in the order in which you want the options to appear. For example, the configuration, **order interface-text-description order nas-identifier order agent-remote-id** produces the following NAS-Port-ID, in which the **#** character is the delimiter:

interface-text-description # nas-identifier # agent-remote-id

Default The router includes the interface description in the NAS-Port-ID when no optional values are specified.

Options

agent-circuit-id—Include the agent circuit ID from either DHCP option 82 or the DSL forum VSAs.

agent-remote-id—Include the agent remote ID from either DHCP option 82 or the DSL forum VSAs.

interface-description—Include the interface description (interface identifier).

interface-text-description—Include the textual interface description (the text description that is statically configured in the CLI).

nas-identifier—Include the NAS identifier value (RADIUS attribute 32).

order—Specify the optional values you want to include in the NAS-Port-ID and the customized order in which you want the values to appear. You must include the **order** option before each optional value (for example, **order agent-circuit-id order interface-description**).

postpend-vlan-tags—Include the VLAN tags. The router includes the tags in the format **:<outer-tag>-<inner-tag>** for a double-tagged VLAN, or **:<outer-tag>** for a single-tagged VLAN.

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

Related Documentation

- *Configuring Access Profile Options for Interactions with RADIUS Servers*
- *Configuring a NAS-Port-ID with Additional Options*
- *RADIUS Servers and Parameters for Subscriber Access*

nas-port-type (Subscriber Management)

Syntax

```
nas-port-type {
  ethernet {
    port-type;
  }
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Specify the port type used to authenticate subscribers. The router includes the port type in RADIUS attribute 61 (NAS-Port-Type attribute).

NOTE: This statement is ignored if the **ethernet-port-type-virtual** statement is included in the same access profile.

Default

The router uses a port type of **ethernet**.

Options

port-type—One of the following port types:

- *value*—A value from 0-65535
- **adsl-cap**—Asymmetric DSL, carrierless amplitude phase (CAP) modulation
- **adsl-dmt**— Asymmetric DSL, discrete multitone (DMT)
- **async**—Asynchronous
- **cable**—Cable
- **ethernet**—Ethernet
- **fddi**—Fiber Distributed Data Interface
- **g3-fax**—G.3 Fax
- **hdlc-clear-channel**—HDLC Clear Channel
- **iapp**—Inter-Access Point Protocol (IAPP)
- **idsl**—ISDN DSL
- **isdn-sync**—ISDN Synchronous
- **isdn-v110**—ISDN Async V.110
- **isdn-v120**—ISDN Async V.120

- **piafs**—Personal Handyphone System (PHS) Internet Access Forum Standard
- **sdsl**—Symmetric DSL
- **sync**—Synchronous
- **token-ring**—Token Ring
- **virtual**—Virtual
- **wireless**—Other wireless
- **wireless-1x-ev**—Wireless 1xEV
- **wireless-cdma2000**—Wireless code division multiple access (CDMA) 2000
- **wireless-ieee80211**—Wireless 802.11
- **wireless-umts**—Wireless universal mobile telecommunications system (UMTS)
- **x25**—X.25
- **x75**—X.75
- **xdsl**—DSL of unknown type

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

Related Documentation
- *Configuring Access Profile Options for Interactions with RADIUS Servers*
- *RADIUS Servers and Parameters for Subscriber Access*

neighbor-discovery-router-advertisement (Access)

Syntax
```
neighbor-discovery-router-advertisement ndra-pool-name;
```

Hierarchy Level
```
[edit access address-assignment]
```

Release Information
Statement introduced in Junos OS Release 10.4.

Description
Configure the name of the address-assignment pool used to assign the router advertisement prefix.

Options
ndra-pool-name—Name of the address assignment pool.

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

Related Documentation

neighbor-port-info-display

Syntax

```
neighbor-port-info-display {
  port-description;
  port-id;
}
```

Hierarchy Level

```
[edit protocols lldp]
```

Release Information Statement introduced in Junos OS Release 14.1X53-D40 and Release 15.1R5 and Release 16.1R3 for EX Series switches.

Description Configure the type of Link Layer Discovery Protocol (LLDP) neighbor port information that the switch displays in the **Port info** field in the output of the show lldp neighbors CLI command.

Devices in a network use LLDP to learn about and identify neighbor devices. LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices.

The **Port info** field of the **show lldp neighbors** command displays the port information received from LLDP neighbors. This information is sent from the LLDP neighbor to the switch in a type, length, and value (TLV) message. You can use the **neighbor-port-info-display** CLI statement to configure the switch to display the information contained in either the Port Description TLV or the Port Identification TLV.

By default, the information contained in the Port Description TLV is used for the port information and is displayed in the **Port info** field. The Port Description TLV contains the textual description of the logical unit or the port. The description for the logical unit is used, if available; otherwise, the description for the physical interface (port) is used. For example, LAG member interfaces do not contain a logical unit; therefore, only the description configured on the physical interface is used.

The Port Identification TLV contains the identifier for the neighbor port. The SNMP index of the interface is used as the port identifier.

Default On EX Series switches, the **Port info** field in the output of the **show lldp neighbors** CLI command displays the Port Description TLV.

Options

port-description—Configure this option to display the Port Description TLV in the **Port info** field of the **show lldp neighbors** CLI command.

port-id—Configure this option to display the Port Identification TLV in the **Port info** field of the **show lldp neighbors** CLI command.

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

Related Documentation
- show lldp neighbors on page 1840
- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP on page 511
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

netbios-snooping

Syntax
```
netbios-snooping;
```

Hierarchy Level
```
[edit protocols lldp]
```

Release Information
Statement introduced in Junos OS Release 11.1 for EX Series switches.

Description
Enable NetBIOS snooping on the switch.

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

Related Documentation
- Configuring NetBIOS Snooping (CLI Procedure) on page 525

next-hop (Dynamic Access Routes)

Syntax

```
next-hop next-hop;
```

Hierarchy Level

```
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options
  access route prefix],
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options
  rib routing-table-name access route prefix],
[edit dynamic-profiles profile-name routing-options access route prefix]
```

Release Information

Statement introduced in Junos OS Release 9.5.
Support at the **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access route *prefix*]** and **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access route *prefix*]** hierarchy levels introduced in Junos OS Release 10.1.

Description

Dynamically configure the next-hop address for an access route. Access routes are typically unnumbered interfaces.

The next-hop gateway can be specified explicitly in the framed route, as either the subscriber's fixed address (common for business subscribers) or 0.0.0.0. Alternatively, the absence of the gateway address implies address 0.0.0.0. The address 0.0.0.0, whether implicit or explicitly configured, resolves to the subscriber's assigned address (host route).

If the RADIUS Framed-Route attribute (22) or Framed-IPv6-Route attribute [99] does not specify the next-hop gateway—as is common—the variable representing the next-hop automatically resolves to the subscriber's IP address.

Options

next-hop—Either the specific next-hop address you want to assign to the access route or one of the following next-hop address predefined variables.

- For IPv4 access routes, use the variable, **$junos-framed-route-nexthop**. The route prefix variable is dynamically replaced with the value in Framed-Route RADIUS attribute [22].
- For IPv6 access routes, use the variable, **$junos-framed-route-ipv6-nexthop**. The variable is dynamically replaced with the value in Framed-IPv6-Route RADIUS attribute [99].

Required Privilege Level

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

Related Documentation

- *Configuring Dynamic Access Routes for Subscriber Management*

next-server

Syntax

next-server *next-server*;

Hierarchy Level

[edit system services dhcp],
[edit system services dhcp pool *pool-id*],
[edit system services dhcp static-binding *mac-address*]

Release Information

Statement introduced in Junos OS Release 8.4.

Description

(J Series Services Routers only) Specify the IP address for the next DHCP server used for communication after a DHCP boot client establishes initial contact.

Options

next-server—The IP address of the DHCP server that is used as the “siaddr” in a DHCP protocol packet.

Required Privilege Level

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

Related Documentation

no-adaptation

Syntax

```
no-adaptation;
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method
  bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method
  bfd]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure Bidirectional Forwarding Detection (BFD) sessions to not adapt to changing network conditions.

Required Privilege Level

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

Related Documentation

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677

no-allow-snooped-clients

Syntax

```
no-allow-snooped-clients;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name
  overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 10.2.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Explicitly disable DHCP snooping support on DHCP relay agent.

Use the statement at the **[edit ... dhcpv6]** hierarchy levels to explicitly disable snooping support for DHCPv6 relay agent.

NOTE: In Junos OS Release 10.0 and earlier, DHCP snooping is *enabled* by default. In Release 10.1 and later, DHCP snooping is *disabled* by default.

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618
- Overriding the Default DHCP Relay Configuration Settings on page 627
- DHCP Snooping Support on page 706
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent on page 710

no-bind-on-request (DHCP Relay Agent)

Syntax

```
no-bind-on-request;
```

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name* overrides],
[edit forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 group *group-name* overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* interface *interface-name* overrides]

Release Information

Statement introduced in Junos OS Release 10.4.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Explicitly disable automatic binding of received DHCP request messages that have no entry in the database (*stray* requests). Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

M120 and M320 routers do not support DHCPv6.

NOTE: Beginning with Junos OS Release 10.4, automatic binding of stray requests is enabled by default. In Junos OS Release 10.3 and earlier releases, automatic binding of stray requests is disabled by default.

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

Related Documentation
- Extended DHCP Relay Agent Overview on page 618
- Overriding the Default DHCP Relay Configuration Settings on page 627
- Disabling Automatic Binding of Stray DHCP Requests on page 608

no-listen

Syntax
```
no-listen;
```

Hierarchy Level
[edit forwarding-options helpers bootp interface (*interface-name* | *interface-group*)],
[edit forwarding-options helpers domain interface *interface-name*],
[edit forwarding-options helpers port *port-number* interface *interface-name*],
[edit forwarding-options helpers **tftp** interface *interface-name*]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

Description
Disable recognition of DNS requests or stop packets from being forwarded on a logical interface, a group of logical interfaces, a router, or a switch.

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

Related Documentation
- *Configuring DNS and TFTP Packet Forwarding*
- *Configuring Port-based LAN Broadcast Packet Forwarding*
- *Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents*

no-mac-table-binding (802.1X)

Syntax
```
no-mac-table-binding;
```

Hierarchy Level
```
[edit protocols dot1x authenticator]
```

Release Information
Statement introduced in Junos OS Release 11.1 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description
For 802.1X authentication, disable the removal of the session from the authentication session table when the MAC address ages out of the Ethernet switching table.

Default
Not enabled

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

Related Documentation
- Controlling Authentication Session Timeouts (CLI Procedure) on page 277

no-reauthentication

Syntax
```
no-reauthentication;
```

Hierarchy Level
```
[edit protocols dot1x authenticator interface (802.1X) (all | [interface-names])]
```

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description
For 802.1X authentication, disables reauthentication.

Default
Not disabled

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

Related Documentation
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- *Configuring 802.1X Authentication (J-Web Procedure)*
- Understanding Authentication on Switches on page 268

no-vlan-interface-name

Syntax

```
no-vlan-interface-name;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id |
  relay-agent-remote-id)],
[edit forwarding-options dhcp-relay dhcpv6 group group-name (relay-agent-interface-id |
  relay-agent-remote-id)],
[edit forwarding-options dhcp-relay relay-option-82 (circuit-id | remote-id)],
[edit forwarding-options dhcp-relay group group-name relay-option-82 (circuit-id |
  remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay dhcpv6
  (relay-agent-interface-id | relay-agent-remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay ... relay-option-82
  (circuit-id | remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6
  (relay-agent-interface-id | relay-agent-remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...
  relay-option-82 (circuit-id | remote-id)],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-18],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-37]
```

Release Information

Statement introduced in Junos OS Release 14.1.

NOTE: The EX Series switches that support the **no-vlan-interface-name** statement are the EX4300, EX4600, and EX9200 switches.

Description

When you do not want bridge domain or VLAN tag information, do not include the VLAN ID nor the VLAN interface name (the default) in the circuit or remote ID value in the DHCP option 82 information.

NOTE: The **no-vlan-interface-name** statement is mutually exclusive with the **use-interface-description** and **use-vlan-id** statements.

When you configure the **no-vlan-interface-name** statement only, the format displays only the Layer 3 interface:

```
irb.subunit
```

NOTE: The *subunit* is required and used to differentiate the interface for remote systems.

When you configure the **no-vlan-interface-name** and **use-interface-description** statements, the format displays the IRB interface description:

irb_descr

If you configure the **no-vlan-interface-name** and **use-interface-description** statements, and no description for the IRB interface is found, the format displays the IRB interface name:

irb.*subunit*

When you configure the **no-vlan-interface-name** and **include-irb-and-l2** statements, the format displays the Layer 2 logical interface name and the IRB interface name:

(fe | ge)-*fpc/pic/port.subunit*+irb.*subunit*

When you configure the **no-vlan-interface-name**, **include-irb-and-l2** and **use-interface-name** statements, the format displays the Layer 2 interface description and the IRB interface name:

l2_descr+irb.*subunit*

If you configure the **no-vlan-interface-name**, **include-irb-and-l2** and **use-interface-name** statements, and no description for the Layer 2 interface is found, the format displays the Layer 2 logical interface name and the IRB interface name:

(fe | ge)-*fpc/pic/port.subunit*+irb.*subunit*

Required Privilege Level

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

Related Documentation

- *Including a Textual Description in DHCP Options*
- Using DHCP Relay Agent Option 82 Information on page 633
- *Configuring DHCPv6 Relay Agent Options*

no-passwords

Syntax no-passwords;

Hierarchy Level [edit system services ssh]

Description Disable ssh password based authentication.

NOTE: Enabling this option under **[edit system services ssh]** applies to **SSH** login service and **NETCONF** running over ssh services.

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

Related Documentation
- Configuring SSH Service for Remote Access to the Router or Switch on page 232

no-public-keys

Syntax no-public-keys;

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 15.1.

Description Disable public key authentication system wide. Another statement (**system login user *username* authentication**) is used to disable public key authentication by individual user.

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

Related Documentation
- authentication on page 883
- ssh on page 1495

no-reauthentication

Syntax no-reauthentication;

Hierarchy Level [edit protocols dot1x authenticator interface (802.1X) (all | [*interface-names*])]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description For 802.1X authentication, disables reauthentication.

Default Not disabled

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

Related Documentation

- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- *Configuring 802.1X Authentication (J-Web Procedure)*
- Understanding Authentication on Switches on page 268

no-tagging

Syntax no-tagging;

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description Configure the switch to send LLDPDUs without including VLAN tags on interfaces for which VLAN tagging in enabled (tagged interfaces).

Default Interfaces for which VLAN tagging is enabled include a VLAN tag (tag 0) in LLDPDUs if the **no-tagging** option is not configured.

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

Related Documentation

- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

no-tcp-forwarding

Syntax no-tcp-forwarding

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Release 11.4 of Junos OS.

Description Use this configuration option to prevent a user from creating an SSH tunnel over a CLI session to a Junos router via SSH. This type of tunnel could be used to forward TCP traffic, bypassing any firewall filters or ACLs, allowing access to resources beyond the router.

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

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 232
- ssh on page 1495
- *Junos OS Security Configuration Guide*

non-strict-priority-scheduling

Syntax non-strict-priority-scheduling;

Hierarchy Level [edit class-of-service non-strict-priority-scheduling]

Release Information Statement introduced in Junos OS Release 15.1X49-D80.

NOTE: This statement is supported only on SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, and vSRX2.0 devices.

Description Configure non-strict priority scheduling to avoid starvation of lower-priority queues on SRX300, SRX320, SRX340, SRX345, SRX1500, SRX550M, and vSRX 2.0 devices.

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

Related Documentation

- *Example: Configuring CoS Non-Strict Priority Scheduling*

nonvolatile

Syntax

```
nonvolatile {
  commit-delay seconds;
}
```

Hierarchy Level

[edit snmp]

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series routers and SRX firewalls.
The commit-delay statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure options for SNMP **Set** requests.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring the Commit Delay Timer*
- commit-delay on page 953

object-names

Syntax

```
object-names {
  mib-object-name;
}
```

Hierarchy Level

[edit accounting-options mib-profile *profile-name*]

Release Information

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Specify the name of each MIB object for which MIB statistics are collected for an accounting-data log file.

Options

mib-object-name—Name of a MIB object. You can specify more than one MIB object name.

Required Privilege Level

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

Related Documentation

- *Configuring the MIB Profile*

oid

Syntax oid *object-identifier* (exclude | include);

Hierarchy Level [edit snmp view *view-name*]

Release Information Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers, OCX switches and SRX devices.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify an object identifier (OID) used to represent a subtree of MIB objects.

Options

exclude—Exclude the subtree of MIB objects represented by the specified OID.

include—Include the subtree of MIB objects represented by the specified OID.

object-identifier—OID used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name.

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

Related Documentation

- *Configuring MIB Views*

operation

Syntax operation *operation-name*;

Hierarchy Level [edit accounting-options mib-profile *profile-name*]

Release Information Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the name of the operation used to collect MIB statistics for an accounting-data log file.

Options ***operation-name***—Name of the operation to use. You can specify a **get**, **get-next**, or **walk** operation.

Default: walk

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

Related Documentation

- *Configuring the MIB Profile*

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;
  }
  chap-challenge-in-request-authenticator;
  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-channel;
    exclude-sub-interface;
  }
  ip-address-change-notify message;
  juniper-access-line-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;
      pw-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;
    interface-text-description;
    nas-identifier;
    order {
      agent-circuit-id;
      agent-remote-id;
      interface-description;
      interface-text-description;
```

```
        nas-identifier;
        postpend-vlan-tags;
      }
      postpend-vlan-tags;
    }
    nas-port-type {
      ethernet {
        port-type;
      }
    }
    override {
      calling-station-id remote-circuit-id;
      nas-ip-address tunnel-client-gateway-address;
      nas-port tunnel-client-nas-port;
      nas-port-type tunnel-client-nas-port-type;
    }
    remote-circuit-id-delimiter;
    remote-circuit-id-fallback;
    remote-circuit-id-format {
      agent-circuit-id;
      agent-remote-id;
    }
    revert-interval interval;
    service-activation {
      dynamic-profile (optional-at-login | required-at-login);
      extensible-service (optional-at-login | required-at-login);
    }
    vlan-nas-port-stacked-format;
}
```

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
juniper-dsl-attributes introduced in Junos OS Release 11.4.
nas-port-id-delimiter introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
calling-station-id-delimiter introduced in Junos OS Release 13.1.
ip-address-change-notify introduced in Junos OS Release 13.1.
coa-dynamic-variable-validation, **client-authentication-algorithm**, and **client-accounting-algorithm** introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
remote-circuit-id-delimiter, **remote-circuit-id-fallback**, and **remote-circuit-id-format** introduced in Junos OS Release 13.3R1 on MX Series.
chap-challenge-in-request-authenticator introduced in Junos OS Release 15.1.
nas-identifier introduced in Junos OS Release 15.1X49-D110 for SRX300, SRX320, SRX340, SRX345, and SRX550M Series devices.
service-activation introduced in Junos OS Release 16.2.

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

Options **accounting-session-id-format**—(EX Series, MX Series only) Configure the format the router or switch uses to identify the accounting session. The default is **decimal**.

Values:

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

calling-station-id-delimiter—(MX Series, T Series only) Starting in Junos OS Release 13.1, specify the character that the router uses as a separator between the concatenated values in the Calling-Station-ID (RADIUS IETF attribute 31) string. The router uses the delimiter when you configure more than one value in the **calling-station-id-format** statement. The default is the hash (**#**) character.

Values:

- *delimiter-character*—Character to use for the delimiter. You must enclose the delimiter character in quotation marks (“ ”).

chap-challenge-in-request-authenticator—(MX Series only) Starting in Junos OS Release 15.1, configure the **authd** process to insert the random challenge generated by the NAS into the Request Authenticator field of Access-Request packets, if the challenge value is 16 bytes long. If you enable the **chap-challenge-in -request-authenticator** statement and the random challenge is not 16 bytes long, **authd** ignores the statement and uses the default behavior, which inserts the random challenge as the CHAP-Challenge attribute (RADIUS attribute 60) in Access-Request packets.

client-accounting-algorithm—(EX Series, MX Series only) Starting in Junos OS Release 13.2X50-D10 for EX Series switches, configure the access method the router uses to access RADIUS accounting servers. The default is the **direct** option.

Values:

- direct—Use the direct method.
- round-robin—Use the round-robin method.

client-authentication-algorithm—(EX Series, M Series, MX Series only) Starting in Junos OS Release 13.2X50-D10 for EX Series switches, configure the method that the authenticator uses to access RADIUS authentication servers when there are multiple servers configured. Initially, a RADIUS client sends a request to a RADIUS authentication or accounting server. The router or switch, acting as the authenticator, waits for a response from the server before sending another request.

When there are multiple RADIUS server connections configured for a client, the authenticator attempts to reach the different servers in the order that they are configured. If there is no response from the first RADIUS server, the authenticator attempts to reach the next RADIUS server. This process repeats until the client is either granted access or there are no more configured servers.

If the **direct** method is configured, the authenticator always treats the first server in the list as the primary server. The authenticator moves on to the second server only

if the attempt to reach the first server fails. If the **round-robin** method is configured, the server chosen first will be rotated based on which server was used last. The first server in the list is treated as a primary for the first authentication request, but for the second request, the second server configured is treated as primary, and so on. With this method, all of the configured servers receive roughly the same number of requests on average so that no single server has to handle all of the requests.

NOTE: The round-robin access method is not recommended for use with EX Series switches.

Default: The default is the **direct** option.

Values:

- direct—Use the direct access method. The authenticator contacts the first RADIUS server on the list for each request, the second server if the first one fails, and so on.
- round-robin—Use the round-robin method. The authenticator contacts the first RADIUS server for the first request, the second server for the second request, and so on.

coa-dynamic-variable-validation—(EX Series, M Series, MX Series only) Starting in Junos OS Release 13.2X50-D10 for EX Series switches, specify that when a CoA operation includes a change to a client profile dynamic variable that cannot be applied (such as an update to a non-existent filter), the router does not apply any changes to client profile dynamic variables in the request, and responds with a NACK message.

Default: If you do not configure this statement, the router does not apply any incorrect variable updates, but does make any other changes to the client profile dynamic variables, and responds with an ACK message.

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

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

access-loop-id-local—Specify that the Agent-Remote-Id and Agent-Circuit-Id are generated locally when these values are not present in the client database.

ip-address-change-notify—(MX Series only) Starting in Junos OS Release 13.1, for on-demand address allocation for dual-stack PPP subscribers, specify that the BNG includes the IPv4-Release-Control VSA (26–164) in the Access-Request that is sent during on-demand IP address allocation and in the Interim-Accounting messages that are sent to report an address change. The configuration of this statement has no effect when on-demand IP address allocation or deallocation is not configured.

Optionally, configure a message that is included in the VSA when it is sent to the RADIUS server.

Default: This functionality is disabled by default.

Values: ***message***—VSA message.

Range: Up to 32 characters.

juniper-access-line-attributes—Configure AAA to add Juniper Networks access line VSAs to the RADIUS authentication and accounting request messages for subscribers. If the router has not received and processed the corresponding ANCP attributes from the access node, then AAA provides only the following in these RADIUS messages:

- Downstream-Calculated-QoS-Rate (IANA 4874, 26-141)—Default configured advisory transmit speed.
- Upstream-Calculated-QoS-Rate (IANA 4874, 26-142)—Default configured advisory receive speed.

NOTE: Starting in Junos OS Release 19.2R1, the **juniper-access-line-attributes** option replaces the **juniper-dsl-attributes** option. For backward compatibility with existing scripts, the **juniper-dsl-attributes** option redirects to the new **juniper-access-line-attributes** option. We recommend that you use **juniper-access-line-attributes**.

Default: The Juniper Networks access line VSAs are not added to the RADIUS authentication and accounting request messages. However, the DSL Forum VSA—if available—is added to RADIUS messages by default.

nas-identifier—(EX Series, MX Series, SRX Series only) Configure the value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests. This statement was introduced in Junos OS Release 15.1X49-D110 for SRX300, SRX320, SRX340, SRX345, and SRX550M Series devices.

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

Range: 1 through 64 characters.

nas-port-id-delimiter—(MX Series only) Starting in Junos OS Release 11.4, specify the character that the router uses as a separator between the concatenated values in the NAS-Port-ID string. The router uses the delimiter when you configure more than one value in the **nas-port-id-format** statement. The default is the hash (**#**) character. This statement was introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Values: *delimiter-character*—Character used for the delimiter.

remote-circuit-id-delimiter—(MX Series only) Starting in Junos OS Release 13.3R1 on MX Series, configure a delimiter character for the remote circuit ID string when you use the **remote-circuit-id-format** statement to configure the string to use instead of the Calling-Station ID in L2TP Calling Number AVP 22. If more than one value is configured for the remote circuit ID format, the delimiter character is used as a separator between the concatenated values in the resulting remote circuit ID string. The default is the hash (**#**) character.

Values: *delimiter*—Delimiter character to be used between components of the remote circuit ID string.

remote-circuit-id-fallback—(MX Series only) Starting in Junos OS Release 13.3R1 on MX Series, configure the fallback value for the LAC to send in L2TP Calling Number AVP 22, either the configured Calling-Station-ID or the default underlying interface. Use of the fallback value is triggered when the components of the override string you configured with the **remote-circuit-id-format** statement—the ACI, the ARI, or both ACI and ARI—are not received by the LAC in the PPPoE Active Discovery Request (PADR) packet.

Values:

- configured-calling-station-id—Send the configured Calling-Station-ID in the Calling Number AVP.
- default—Send the underlying interface value in the Calling Number AVP.

remote-circuit-id-format—(MX Series only) Starting in Junos OS Release 13.3R1 on MX Series, configure the format of the string that overrides the Calling-Station-ID format in the Calling Number AVP 22 sent by the LAC to the LNS in the ICRQ packet when an L2TP session is being established. You can specify the ACI, the ARI, or both the ACI and ARI. This statement enables you to decouple the AVP 22 value from the RADIUS Calling-Station-ID attribute (31); the values for AVP 22 and the Calling-Station-ID attribute are the same when you use the **calling-station-id-format** statement to configure AVP 22.

NOTE: You must configure the override calling-circuit-id remote-circuit-id statement for the remote circuit ID format to be used in the calling number AVP.

Values:

- agent-circuit-id—Specifies use of the ACI string that uniquely identifies the subscriber's access node and the digital subscriber line (DSL) on the access node. For PPPoE traffic, the ACI string is in the DSL Forum Agent-Circuit-ID VSA [26-1] of PPPoE Active Discovery Initiation (PADI) and PPPoE Active Discovery Request (PADR) control packets.
- agent-remote-id—Specifies use of the ARI string that identifies the subscriber on the digital subscriber line access multiplexer (DSLAM) interface that initiated the service request. The agent remote identifier (ARI) string is stored in the DSL Forum Agent-Remote-ID VSA [26-2] for PPPoE traffic.

service-activation—(MX Series only) Starting in Junos OS Release 16.2, specify whether subscribers are allowed to log in even when service activation failures related to configuration errors occur during family activation request processing by authd for a newly authenticated subscriber. Configuration errors include missing or incorrect syntax, missing or incomplete references to dynamic profiles, and missing or incomplete variables.

NOTE: **This configuration does not apply to services activated by means of RADIUS CoA requests, JSRC Push-Profile-Request (PPR) messages, or subscriber secure policies.**

You can enable separate configurations for subscriber login services for two **service-activation** types: **dynamic-profile** and **extensible-service**. You configure the **dynamic-profile** type services in the dynamic profile at the **[edit dynamic-profiles]** hierarchy level; the profile is used to provide dynamic subscriber access and services for broadband applications. The **extensible-service** type is for business services configured in an operation script and provisioned by the Extensible Subscriber Services Manager daemon (essmd).

Default:

Default behavior depends on the service type:

- For **extensible-service** services: **optional-at-login**.
- For **dynamic-profile** services: **required-at-login**.

Values:

- optional-at-login—Service activation is optional. Failure due to configuration errors does not prevent activation of the address family; it allows subscriber access. Failure for any other reason causes network family activation to fail. If no other network family is already active for the subscriber, then the client application logs out the subscriber.
- required-at-login—Service activation is required. Failure for any reason causes the Network-Family-Activate-Request for that network family to fail. If no other network family is already active for the subscriber, then the client application logs out the subscriber.

vlan-nas-port-stacked-format—(MX Series only) Configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Configuring Access Profile Options for Interactions with RADIUS Servers*
- *RADIUS Servers and Parameters for Subscriber Access*
- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Configuring a Calling-Station-ID with Additional Options*

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;
  }
  chap-challenge-in-request-authenticator;
  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-channel;
    exclude-sub-interface;
  }
  ip-address-change-notify message;
  juniper-access-line-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;
      pw-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;
    interface-text-description;
    nas-identifier;
    order {
      agent-circuit-id;
      agent-remote-id;
      interface-description;
      interface-text-description;
```

```
        nas-identifier;
        postpend-vlan-tags;
      }
      postpend-vlan-tags;
    }
    nas-port-type {
      ethernet {
        port-type;
      }
    }
    override {
      calling-station-id remote-circuit-id;
      nas-ip-address tunnel-client-gateway-address;
      nas-port tunnel-client-nas-port;
      nas-port-type tunnel-client-nas-port-type;
    }
    remote-circuit-id-delimiter;
    remote-circuit-id-fallback;
    remote-circuit-id-format {
      agent-circuit-id;
      agent-remote-id;
    }
    revert-interval interval;
    service-activation {
      dynamic-profile (optional-at-login | required-at-login);
      extensible-service (optional-at-login | required-at-login);
    }
    vlan-nas-port-stacked-format;
}
```

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
juniper-dsl-attributes introduced in Junos OS Release 11.4.
nas-port-id-delimiter introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
calling-station-id-delimiter introduced in Junos OS Release 13.1.
ip-address-change-notify introduced in Junos OS Release 13.1.
coa-dynamic-variable-validation, **client-authentication-algorithm**, and **client-accounting-algorithm** introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
remote-circuit-id-delimiter, **remote-circuit-id-fallback**, and **remote-circuit-id-format** introduced in Junos OS Release 13.3R1 on MX Series.
chap-challenge-in-request-authenticator introduced in Junos OS Release 15.1.
nas-identifier introduced in Junos OS Release 15.1X49-D110 for SRX300, SRX320, SRX340, SRX345, and SRX550M Series devices.
service-activation introduced in Junos OS Release 16.2.

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

Options **accounting-session-id-format**—(EX Series, MX Series only) Configure the format the router or switch uses to identify the accounting session. The default is **decimal**.

Values:

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

calling-station-id-delimiter—(MX Series, T Series only) Starting in Junos OS Release 13.1, specify the character that the router uses as a separator between the concatenated values in the Calling-Station-ID (RADIUS IETF attribute 31) string. The router uses the delimiter when you configure more than one value in the **calling-station-id-format** statement. The default is the hash (**#**) character.

Values:

- *delimiter-character*—Character to use for the delimiter. You must enclose the delimiter character in quotation marks (“ ”).

chap-challenge-in-request-authenticator—(MX Series only) Starting in Junos OS Release 15.1, configure the **authd** process to insert the random challenge generated by the NAS into the Request Authenticator field of Access-Request packets, if the challenge value is 16 bytes long. If you enable the **chap-challenge-in -request-authenticator** statement and the random challenge is not 16 bytes long, **authd** ignores the statement and uses the default behavior, which inserts the random challenge as the CHAP-Challenge attribute (RADIUS attribute 60) in Access-Request packets.

client-accounting-algorithm—(EX Series, MX Series only) Starting in Junos OS Release 13.2X50-D10 for EX Series switches, configure the access method the router uses to access RADIUS accounting servers. The default is the **direct** option.

Values:

- direct—Use the direct method.
- round-robin—Use the round-robin method.

client-authentication-algorithm—(EX Series, M Series, MX Series only) Starting in Junos OS Release 13.2X50-D10 for EX Series switches, configure the method that the authenticator uses to access RADIUS authentication servers when there are multiple servers configured. Initially, a RADIUS client sends a request to a RADIUS authentication or accounting server. The router or switch, acting as the authenticator, waits for a response from the server before sending another request.

When there are multiple RADIUS server connections configured for a client, the authenticator attempts to reach the different servers in the order that they are configured. If there is no response from the first RADIUS server, the authenticator attempts to reach the next RADIUS server. This process repeats until the client is either granted access or there are no more configured servers.

If the **direct** method is configured, the authenticator always treats the first server in the list as the primary server. The authenticator moves on to the second server only

if the attempt to reach the first server fails. If the **round-robin** method is configured, the server chosen first will be rotated based on which server was used last. The first server in the list is treated as a primary for the first authentication request, but for the second request, the second server configured is treated as primary, and so on. With this method, all of the configured servers receive roughly the same number of requests on average so that no single server has to handle all of the requests.

NOTE: The round-robin access method is not recommended for use with EX Series switches.

Default: The default is the **direct** option.

Values:

- direct—Use the direct access method. The authenticator contacts the first RADIUS server on the list for each request, the second server if the first one fails, and so on.
- round-robin—Use the round-robin method. The authenticator contacts the first RADIUS server for the first request, the second server for the second request, and so on.

coa-dynamic-variable-validation—(EX Series, M Series, MX Series only) Starting in Junos OS Release 13.2X50-D10 for EX Series switches, specify that when a CoA operation includes a change to a client profile dynamic variable that cannot be applied (such as an update to a non-existent filter), the router does not apply any changes to client profile dynamic variables in the request, and responds with a NACK message.

Default: If you do not configure this statement, the router does not apply any incorrect variable updates, but does make any other changes to the client profile dynamic variables, and responds with an ACK message.

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

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

access-loop-id-local—Specify that the Agent-Remote-Id and Agent-Circuit-Id are generated locally when these values are not present in the client database.

ip-address-change-notify—(MX Series only) Starting in Junos OS Release 13.1, for on-demand address allocation for dual-stack PPP subscribers, specify that the BNG includes the IPv4-Release-Control VSA (26–164) in the Access-Request that is sent during on-demand IP address allocation and in the Interim-Accounting messages that are sent to report an address change. The configuration of this statement has no effect when on-demand IP address allocation or deallocation is not configured.

Optionally, configure a message that is included in the VSA when it is sent to the RADIUS server.

Default: This functionality is disabled by default.

Values: ***message***—VSA message.

Range: Up to 32 characters.

juniper-access-line-attributes—Configure AAA to add Juniper Networks access line VSAs to the RADIUS authentication and accounting request messages for subscribers. If the router has not received and processed the corresponding ANCP attributes from the access node, then AAA provides only the following in these RADIUS messages:

- Downstream-Calculated-QoS-Rate (IANA 4874, 26-141)—Default configured advisory transmit speed.
- Upstream-Calculated-QoS-Rate (IANA 4874, 26-142)—Default configured advisory receive speed.

NOTE: Starting in Junos OS Release 19.2R1, the **juniper-access-line-attributes** option replaces the **juniper-dsl-attributes** option. For backward compatibility with existing scripts, the **juniper-dsl-attributes** option redirects to the new **juniper-access-line-attributes** option. We recommend that you use **juniper-access-line-attributes**.

Default: The Juniper Networks access line VSAs are not added to the RADIUS authentication and accounting request messages. However, the DSL Forum VSA—if available—is added to RADIUS messages by default.

nas-identifier—(EX Series, MX Series, SRX Series only) Configure the value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests. This statement was introduced in Junos OS Release 15.1X49-D110 for SRX300, SRX320, SRX340, SRX345, and SRX550M Series devices.

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

Range: 1 through 64 characters.

nas-port-id-delimiter—(MX Series only) Starting in Junos OS Release 11.4, specify the character that the router uses as a separator between the concatenated values in the NAS-Port-ID string. The router uses the delimiter when you configure more than one value in the **nas-port-id-format** statement. The default is the hash (**#**) character. This statement was introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Values: *delimiter-character*—Character used for the delimiter.

remote-circuit-id-delimiter—(MX Series only) Starting in Junos OS Release 13.3R1 on MX Series, configure a delimiter character for the remote circuit ID string when you use the **remote-circuit-id-format** statement to configure the string to use instead of the Calling-Station ID in L2TP Calling Number AVP 22. If more than one value is configured for the remote circuit ID format, the delimiter character is used as a separator between the concatenated values in the resulting remote circuit ID string. The default is the hash (**#**) character.

Values: *delimiter*—Delimiter character to be used between components of the remote circuit ID string.

remote-circuit-id-fallback—(MX Series only) Starting in Junos OS Release 13.3R1 on MX Series, configure the fallback value for the LAC to send in L2TP Calling Number AVP 22, either the configured Calling-Station-ID or the default underlying interface. Use of the fallback value is triggered when the components of the override string you configured with the **remote-circuit-id-format** statement—the ACI, the ARI, or both ACI and ARI—are not received by the LAC in the PPPoE Active Discovery Request (PADR) packet.

Values:

- configured-calling-station-id—Send the configured Calling-Station-ID in the Calling Number AVP.
- default—Send the underlying interface value in the Calling Number AVP.

remote-circuit-id-format—(MX Series only) Starting in Junos OS Release 13.3R1 on MX Series, configure the format of the string that overrides the Calling-Station-ID format in the Calling Number AVP 22 sent by the LAC to the LNS in the ICRQ packet when an L2TP session is being established. You can specify the ACI, the ARI, or both the ACI and ARI. This statement enables you to decouple the AVP 22 value from the RADIUS Calling-Station-ID attribute (31); the values for AVP 22 and the Calling-Station-ID attribute are the same when you use the **calling-station-id-format** statement to configure AVP 22.

NOTE: You must configure the override calling-circuit-id remote-circuit-id statement for the remote circuit ID format to be used in the calling number AVP.

Values:

- agent-circuit-id—Specifies use of the ACI string that uniquely identifies the subscriber's access node and the digital subscriber line (DSL) on the access node. For PPPoE traffic, the ACI string is in the DSL Forum Agent-Circuit-ID VSA [26-1] of PPPoE Active Discovery Initiation (PADI) and PPPoE Active Discovery Request (PADR) control packets.
- agent-remote-id—Specifies use of the ARI string that identifies the subscriber on the digital subscriber line access multiplexer (DSLAM) interface that initiated the service request. The agent remote identifier (ARI) string is stored in the DSL Forum Agent-Remote-ID VSA [26-2] for PPPoE traffic.

service-activation—(MX Series only) Starting in Junos OS Release 16.2, specify whether subscribers are allowed to log in even when service activation failures related to configuration errors occur during family activation request processing by authd for a newly authenticated subscriber. Configuration errors include missing or incorrect syntax, missing or incomplete references to dynamic profiles, and missing or incomplete variables.

NOTE: This configuration does not apply to services activated by means of RADIUS CoA requests, JSRC Push-Profile-Request (PPR) messages, or subscriber secure policies.

You can enable separate configurations for subscriber login services for two **service-activation** types: **dynamic-profile** and **extensible-service**. You configure the **dynamic-profile** type services in the dynamic profile at the **[edit dynamic-profiles]** hierarchy level; the profile is used to provide dynamic subscriber access and services for broadband applications. The **extensible-service** type is for business services configured in an operation script and provisioned by the Extensible Subscriber Services Manager daemon (essmd).

Default:

Default behavior depends on the service type:

- For **extensible-service** services: **optional-at-login**.
- For **dynamic-profile** services: **required-at-login**.

Values:

- optional-at-login—Service activation is optional. Failure due to configuration errors does not prevent activation of the address family; it allows subscriber access. Failure for any other reason causes network family activation to fail. If no other network family is already active for the subscriber, then the client application logs out the subscriber.
- required-at-login—Service activation is required. Failure for any reason causes the Network-Family-Activate-Request for that network family to fail. If no other network family is already active for the subscriber, then the client application logs out the subscriber.

vlan-nas-port-stacked-format—(MX Series only) Configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Configuring Access Profile Options for Interactions with RADIUS Servers*
- *RADIUS Servers and Parameters for Subscriber Access*
- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Configuring a Calling-Station-ID with Additional Options*

option (DHCP server)

Syntax

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

Hierarchy Level

[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

Release Information

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

Description

Configure one or more user-defined options that are not included in the Junos default implementation of the DHCP server. For example, if a client requests a DHCP option that is not included in the DHCP server, you can create a user-defined option that enables the server to respond to the client's request.

Options

- ***id-number***—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.
- ***option-type***—Any of the following types: **byte**, **byte-stream**, **flag**, **integer**, **ip-address**, **short**, **string**, **unsigned-integer**, **unsigned-short**.
- **array**—An option can include an array of values.
- ***option-value***—Value associated with an option. The option value must be compatible with the option type (for example, an **On** or **Off** value for a **flag** type).

Required Privilege Level

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

Related Documentation

- Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server on page 553

option-60 (DHCP Local Server)

Syntax

```
option-60;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the payload of Option 60 (Vendor Class Identifier) from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process.

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651

option-60 (DHCP Relay Agent)

Syntax

```
option-60 {
  default-action {
    drop drop;
    forward-only forward-only;
    local-server-group local-server-group;
  }
  equals {
    ascii name {
      drop drop;
      forward-only forward-only;
      local-server-group local-server-group;
    }
    hexadecimal name {
      drop drop;
      forward-only forward-only;
      local-server-group local-server-group;
    }
  }
  not-present {
    drop drop;
    forward-only forward-only;
    local-server-group local-server-group;
  }
  equals {
    ascii name {
      drop drop;
      forward-only forward-only;
      local-server-group local-server-group;
    }
    hexadecimal name {
      drop drop;
      forward-only forward-only;
      local-server-group local-server-group;
    }
  }
}
```

Hierarchy Level

[edit bridge-domains *name* forwarding-options dhcp-relay group *name* relay-option],
[edit bridge-domains *name* forwarding-options dhcp-relay relay-option],
[edit forwarding-options dhcp-relay group *name* relay-option],
[edit forwarding-options dhcp-relay relay-option],
[edit logical-systems *name* bridge-domains *name* forwarding-options dhcp-relay group *name* relay-option],
[edit logical-systems *name* bridge-domains *name* forwarding-options dhcp-relay relay-option],
[edit logical-systems *name* forwarding-options dhcp-relay group *name* relay-option],
[edit logical-systems *name* forwarding-options dhcp-relay relay-option],
[edit logical-systems *name* routing-instances *name* bridge-domains *name* forwarding-options dhcp-relay group *name* relay-option],

[edit logical-systems *name* routing-instances *name* bridge-domains *name* forwarding-options dhcp-relay relay-option],
[edit logical-systems *name* routing-instances *name* forwarding-options dhcp-relay group *name* relay-option],
[edit logical-systems *name* routing-instances *name* forwarding-options dhcp-relay relay-option],
[edit logical-systems *name* routing-instances *name* vlans *name* forwarding-options dhcp-relay group *name* relay-option],
[edit logical-systems *name* routing-instances *name* vlans *name* forwarding-options dhcp-relay relay-option],
[edit logical-systems *name* vlans *name* forwarding-options dhcp-relay group *name* relay-option],
[edit logical-systems *name* vlans *name* forwarding-options dhcp-relay relay-option],
[edit routing-instances *name* bridge-domains *name* forwarding-options dhcp-relay group *name* relay-option],
[edit routing-instances *name* bridge-domains *name* forwarding-options dhcp-relay relay-option],
[edit routing-instances *name* forwarding-options dhcp-relay group *name* relay-option],
[edit routing-instances *name* forwarding-options dhcp-relay relay-option],
[edit routing-instances *name* vlans *name* forwarding-options dhcp-relay group *name* relay-option],
[edit routing-instances *name* vlans *name* forwarding-options dhcp-relay relay-option],
[edit vlans *name* forwarding-options dhcp-relay group *name* relay-option],
[edit vlans *name* forwarding-options dhcp-relay relay-option]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Statement updated in Junos OS Release 17.4R1 for MX Series.

Description

Specify that the payload of the Option 60 (Vendor Class Identifier) from the client PDU is concatenated with the username during the subscriber authentication or client authentication process.

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651
- *DHCPv4 and DHCPv6 Forward-Only Action for Relay Traffic with Unknown DHCP Server Address*

option-82 (DHCP Local Server Authentication)

Syntax

```
option-82 <circuit-id> <remote-id>;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the type of Option 82 information from the client PDU that is concatenated with the username during the subscriber authentication or DHCP client authentication process. You can specify either, both, or neither of the Agent Circuit ID and Agent Remote ID suboptions. If you specify both, the Agent Circuit ID is supplied first, followed by a delimiter, and then the Agent Remote ID. If you specify that neither suboption is supplied, the raw payload of Option 82 from the PDU is concatenated to the username.

Options

circuit-id—(Optional) Agent Circuit ID suboption (suboption 1).

remote-id—(Optional) Agent Remote ID suboption (suboption 2).

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651

option-82 (DHCP Local Server Pool Matching)

Syntax

```
option-82;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
  services dhcp-local-server pool-match-order],
[edit logical-systems logical-system-name system services dhcp-local-server
  pool-match-order],
[edit routing-instances routing-instance-name system services dhcp-local-server
  pool-match-order],
[edit system services dhcp-local-server pool-match-order]
```

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the extended DHCP local server to use the option 82 value in the DHCP client DHCP PDU together with the ip-address-first method to determine which address-assignment pool to use. You must configure the **ip-address-first** statement before configuring the **option-82** statement. The DHCP local server first determines which address-assignment pool to use based on the ip-address-first method. Then, the local server matches the option 82 value in the client PDU with the option 82 configuration in the address-assignment pool. This statement is supported for IPv4 address-assignment pools only.

Required Privilege Level

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

Related Documentation

- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 701
- Extended DHCP Local Server Overview on page 562
- *Address-Assignment Pools Overview*

option-82 (DHCP Relay Agent)

Syntax

```
option-82 <circuit-id> <remote-id>;
```

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* authentication username-include]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the option 82 that is concatenated with the username during the subscriber authentication or client authentication process. You can specify either, both, or neither the Agent Circuit ID and the Agent Remote ID suboptions. If you specify both, the Agent Circuit ID is supplied first, followed by a delimiter, and then the Agent Remote ID. If neither suboption is supplied, the raw payload of option 82 is concatenated to the username.

NOTE: The option 82 value used in creating the username is based on the option 82 value that is encoded in the outgoing (relayed) PDU.

Options

circuit-id—(Optional) The string for the Agent Circuit ID suboption (suboption 1).

remote-id—(Optional) The string for the Agent Remote ID suboption (suboption 2).

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651

option-number (DHCP Relay Agent Option)

Syntax

```
option-number option-number;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option],
[edit forwarding-options dhcp-relay dhcpv6 relay-option],
[edit forwarding-options dhcp-relay group group-name relay-option],
[edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Specify the DHCP option DHCP relay agent uses for selective processing of client traffic. You can configure support globally or for a named group of interfaces. You can also configure support for the extended DHCP relay agent on a per logical system and per routing instance basis.

Use the **[edit forwarding-options dhcp-relay dhcpv6]** hierarchy level to configure the DHCPv6 relay agent support.

Options

option-number—The DHCP or DHCPv6 option in the incoming traffic.

NOTE: **EX Series switches do not support the User Class Options.**

- 15 (DHCPv6 only)—Use DHCPv6 option 15 (User Class Option) in packets
- 16 (DHCPv6 only)—(MX Series routers and EX Series switches only) Use DHCPv6 option 16 (Vendor Class Option) in packets
- 60 (DHCPv4 only)—(MX Series routers and EX Series switches only) Use DHCP option 60 (Vendor Class Identifier) in DHCP packets
- 77 (DHCPv4 only)—Use DHCP option 77 (User Class Identifier) in packets

Required Privilege Level

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

Related Documentation

- *Using DHCP Option Information to Selectively Process DHCP Client Traffic*

order

Syntax order (radius | [*accounting-order-data-list*]);

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the order of authentication, authorization, and accounting (AAA) servers to use while sending accounting messages and updates.

Default No order specified

Options **radius**—RADIUS accounting for specified subscribers.

[*accounting-order-data-list*]— Set of data listing the authentication order to be used, enclosed by brackets. This can be any combination of the authentication methods, up to and including a full list of the entire authentication order.

NOTE: **The [edit access] hierarchy is not available on QFabric systems.**

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

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335

outbound-ssh

Syntax

```
[edit system services]
outbound-ssh {
  client client-id {
    address {
      port port-number;
      retry number;
      timeout seconds;
    }
    device-id device-id;
    keep-alive {
      retry number;
      timeout seconds;
    }
    reconnect-strategy (in-order | sticky);
    secret password;
    services netconf;
  }
  traceoptions {
    file filename <files number> <match regex> <size size> <world-readable |
      no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level

```
[edit system services]
```

Release Information

Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure a router or switch running the Junos OS behind a firewall to communicate with client management applications on the other side of the firewall.

Default

To configure transmission of the router's or switch's device ID to the application, include the **device-id** statement at the **[edit system services]** hierarchy level.

Options

client-id—Identifies the **outbound-ssh** configuration stanza on the router or switch. Each **outbound-ssh** stanza represents a single outbound SSH connection. This attribute is not sent to the client.

device-id—Identifies the router or switch to the client during the initiation sequence.

keep-alive—(Optional) When configured, specifies that the router or switch send keepalive messages to the management server. To configure the keepalive message, you must set both the **timeout** and **retry** attributes.

reconnect-strategy—(Optional) Specify the method the router or switch uses to reestablish a disconnected outbound SSH connection. Two methods are available:

- **in-order**—Specify that the router or switch first attempt to establish an outbound SSH session based on the management server address list. The router or switch attempts to establish a session with the first server on the list. If this connection is not available, the router or switch attempts to establish a session with the next server, and so on down the list until a connection is established.
- **sticky**—Specify that the router or switch first attempt to reconnect to the management server that it was last connected to. If the connection is unavailable, it attempts to establish a connection with the next client on the list and so forth until a connection is made.

retry—Number of keepalive messages the router or switch sends without receiving a response from the client before the current SSH connection is disconnected. The default is three messages.

secret—(Optional) Router's or switch's public SSH host key. If added to the **outbound-ssh** statement, during the initialization of the outbound SSH service, the router or switch passes its public key to the management server. This is the recommended method of maintaining a current copy of the router's or switch's public key.

timeout—Length of time that the Junos server waits for data before sending a keep alive signal. The default is 15 seconds.

When reconnecting to a client, the router or switch attempts to reconnect to the client based on the **retry** and **timeout** values for each client listed.

address—Hostname or the IPv4 address or IPv6 address of the NSM application server. You can list multiple clients by adding each client's IP address or hostname along with the following connection parameters:

- **port**—Outbound SSH port for the client. The default is port 22.
- **retry**—Number of times the router or switch attempts to establish an outbound SSH connection before giving up. The default is three tries.
- **timeout**—Length of time that the router or switch attempts to establish an outbound SSH connection before giving up. The default is fifteen seconds.

NOTE: Starting with Release 15.1, Junos OS supports outbound-SSH connections with devices having IPv6 addresses.

filename—(Optional) By default, the filename of the log file used to record the trace options is the name of the traced process (for example, **mib2d** or **snmpd**). Use this option to override the default value.

files—(Optional) Maximum number of trace files generated. By default, the maximum number of trace files is 10. Use this option to override the default value.

When a trace file reaches its maximum size, the system archives the file and starts a new file. The system archives trace files by appending a number to the filename in sequential order from 1 to the maximum value (specified by the default value or the options value set here). Once the maximum value is reached, the numbering sequence is restarted at 1, overwriting the older file.

size—(Optional) Maximum size of the trace file in kilobytes (KB). Once the maximum file size is reached, the system archives the file. The default value is 1000 KB. Use this option to override the default value.

match—(Optional) When used, the system only adds lines to the trace file that match the regular expression specified. For example, if the match value is set to **=error**, the system only records lines to the trace file that include the string **error**.

services—Services available for the session. Currently, NETCONF is the only service available.

world-readable | no-world-readable—(Optional) Whether the files are accessible by the originator of the trace operation only or by any user. By default, log files are only accessible by the user that started the trace operation (**no-world-readable**).

all | configuration | connectivity—(Optional) Type of tracing operation to perform.

all—Log all events.

configuration—Log all events pertaining to the configuration of the router or switch.

connectivity—Log all events pertaining to the establishment of a connection between the client server and the router or switch.

no-remote-trace—(Optional) Disable remote tracing.

Required Privilege Level

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

Related Documentation

- Configuring Outbound SSH Service on page 241
- *System Management Configuration Statements*

outbound-ssh

Syntax

```
outbound-ssh {
  client client-id {
    address address {
      port port-number;
      retry number;
      timeout seconds;
    }
    device-id device-id;
    keep-alive {
      retry number;
      timeout seconds;
    }
    reconnect-strategy (in-order | sticky);
    secret password;
    services netconf;
  }
  traceoptions {
    file filename <files number> <match regex> <size size> <world-readable |
      no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level

```
[edit system services]
```

Release Information

Statement introduced in Junos OS Release 10.4.
Support for IPv6 address added in Junos OS Release 12.1X47-D15.

Description

Initiate outbound SSH connections.

Options

client *client-id*—Defines a device-initiated connection. This value serves to uniquely identify the outbound-ssh configuration stanza. Each outbound-ssh stanza represents a single outbound SSH connection. Thus, the administrator is free to assign the client-id any meaningful unique value.

address *address*—Specifies the IPv4 or IPv6 address or hostname of the client.

port *port-number*—Specifies the port at which a server listens for outbound SSH connection requests.

retry *number*—Specifies the maximum number of connection attempts a device can make to the specified IP address. The default is three attempts.

timeout *seconds*—Specifies how long the application waits between attempts to reconnect to the specified IP address, in seconds. The default is 15 seconds.

device *device-id*—Identifies the device to the management client. Each time the device establishes an outbound SSH connection, it first sends an initiation sequence (device-id) to the management client.

keep-alive—Enables the device to send SSH protocol keepalive messages to the client application. The **timeout** statement specifies how long the device waits to receive data before sending a request for acknowledgment from the application. The default is 15 seconds. The **retry** statement specifies how many keepalive messages the router sends without receiving a response from the client. When that number is exceeded, the device disconnects from the application, ending the outbound SSH connection. The default is three retries.

reconnect-strategy (in-order|sticky)—Specifies how the device reconnects to the server after a connection is dropped.

in-order—Configures the device to reconnect to the first configured server. If this server is unavailable, the device tries to connect to the next configured server. This process repeats until a connection is completed.

sticky—Configures the device to reconnect to the server from which it disconnected.

secret *password*—Sends the device's public SSH host key when the device connects to the client.

services *netconf*—Configures the application to accept NETCONF as an available service.

Required Privilege Level

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

Related Documentation

- traceoptions (Outbound SSH) on page 1563
- Configuring Outbound SSH Service on page 241

overrides (DHCP Local Server)

Syntax

```
asymmetric-lease-time seconds;
  asymmetric-prefix-lease-time seconds;
  client-discover-match <option60-and-option82 | incoming-interface>;
  client-negotiation-match incoming-interface;
  delay-advertise {
    based-on (option-15 | option-16 | option-18 | option-37) {
      equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      not-equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      starts-with {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
    }
    delay-time seconds;
  }
  delay-offer {
    based-on (option-60 | option-77 | option-82) {
      equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      not-equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      starts-with {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
    }
    delay-time seconds;
  }
  delegated-pool;
  delete-binding-on-renegotiation;
  dual-stack dual-stack-group-name;
  include-option-82 {
    forcerenew;
    nak;
  }
  interface-client-limit number;
  multi-address-embedded-option-response;
  process-inform {
    pool pool-name;
  }
  protocol-attributes attribute-set-name;
```

```
  rapid-commit;
}
```

Hierarchy Level

[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group *group-name*],
[edit system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name*],
[edit system services dhcp-local-server group *group-name*],
[edit system services dhcp-local-server group *group-name* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server ...],
[edit logical-systems *logical-system-name* system services dhcp-local-server ...],
[edit routing-instances *routing-instance-name* system services dhcp-local-server ...]

Release Information

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Support for the **allow-no-end** option introduced in Junos OS Release 14.1X53-D15 for EX Series switches.
Statement introduced in Junos OS Release 12.3X48-D10 for SRX Series devices.

Description Override the default configuration settings for the extended DHCP local server. Specifying the **overrides** statement with no subordinate statements removes all DHCP local server overrides at that hierarchy level.

- To override global DHCP local server configuration options, include the **overrides** statement and its subordinate statements at the **[edit system services dhcp-local-server]** hierarchy level.
- To override configuration options for a named group of interfaces, include the statements at the **[edit system services dhcp-local-server group *group-name*]** hierarchy level.
- To override configuration options for a specific interface within a named group of interfaces, include the statements at the **[edit system services dhcp-local-server group *group-name* interface *interface-name*]** hierarchy level.
- Use the **[edit system services dhcp-local-server dhcpv6]** hierarchy level to override DHCPv6 configuration options.

NOTE: By default, jdhcp does not process DHCPINFORM message. Only after you enable the overrides command using the **set system services dhcp-local-server overrides process-inform** statement, jdhcp starts processing the DHCPINFORM message.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

The interface-client-limit statement is not supported in the **[edit system services dhcp-local-server dhcpv6]** hierarchy level.

The **asymmetric-prefix-lease-time**, delegated-pool, **multi-address-embedded-option-response**, and rapid-commit statements are supported in the **[edit system services dhcp-local-server dhcpv6 ...]** hierarchy level only.

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

Related Documentation

- Extended DHCP Local Server Overview on page 562
- Overriding the Default DHCP Local Server Configuration Settings Overview on page 630
- Configuring a DHCP Server on Switches (CLI Procedure) on page 588

overrides (DHCP Relay Agent)

Syntax

```
overrides {
  allow-no-end-option;
  allow-snooped-clients;
  always-write-giaddr;
  always-write-option-82;
  asymmetric-lease-time seconds;
  asymmetric-prefix-lease-time seconds;
  client-discover-match <option60-and-option82 | incoming-interface>;
  client-negotiation-match incoming-interface;
  delay-authentication;
  delete-binding-on-renegotiation;
  disable-relay;
  dual-stack dual-stack-group-name;
  interface-client-limit number;
  layer2-unicast-replies;
  no-allow-snooped-clients;
  no-bind-on-request;
  proxy-mode;
  relay-source
  replace-ip-source-with;
  send-release-on-delete;
  trust-option-82;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay group group-name interface interface-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 8.3.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Override the default configuration settings for the extended DHCP relay agent. Specifying the **overrides** statement with no subordinate statements removes all DHCP relay agent overrides at that hierarchy level. Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

M120 and M320 routers do not support DHCPv6.

The following statements are supported at both the **[edit ... dhcp-relay]** and **[edit ... dhcpv6]** hierarchy levels.

- **allow-snooped-clients**
- **asymmetric-lease-time**
- **delete-binding-on-renegotiation**
- **dual-stack**
- **interface-client-limit**
- **no-allow-snooped-clients**
- **no-bind-on-request**
- **relay-source**
- **send-release-on-delete**

The following statements are supported at the **[edit ... dhcpv6]** hierarchy levels only.

- **asymmetric-prefix-lease-time**

All other statements are supported at the **[edit ... dhcp-relay]** hierarchy levels only.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618
- Overriding the Default DHCP Relay Configuration Settings on page 627

overrides (New Relay Options)

Syntax

```
overrides {
  allow-no-end-option;
  always-write-option-82;
  asymmetric-lease-time;
  bootp-support;
  delete-binding-on-renegotiation;
  disable-relay;
  dual-stack;
  no-bind-on-request;
  relay-source;
  replace-ip-source-with;
  send-release-on-delete;
  trust-option-82;
  user-defined-option-82;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay]
```

Release Information Statement introduced in Junos OS Release 15.1X49-D100.

Description Override the default configuration settings for the extended DHCP relay agent. Specifying the **overrides** statement with no subordinate statements removes all DHCP relay agent overrides at that hierarchy level.

Options

allow-no-end-option—Accept packets without end-of-option.

asymmetric-lease-time—Provides a way to send the DHCP client a lease that is shorter than the actual lease granted by the DHCP local server.

Range: 600 through 86,400 seconds.

bootp-support—Allows send bootp request from a remote client to a DHCP server for an IP address.

delete-binding-on-renegotiation—Allows DHCP relay agent to delete binding information for a specific client when a DHCP DISCOVER packet is received from the client.

disable-relay—Disable DHCP relay processing.

dual-stack—Specify the dual stack group to use.

no-bind-on-request—Explicitly disable automatic binding of received DHCP request messages that have no entry in the database (stray requests).

relay-source—Specify the interface for relay source.

send-release-on-delete—Always send RELEASE to the server when a binding is deleted.

trust-option-82—Allow processing of DHCP client packets that have a gateway IP address giaddr of 0 and contain option 82 information.

user-defined-option-82—Specify user defined description for option-82.

The remaining statements are explained separately. see CLI Explorer.

Required Privilege Level

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

Related Documentation

- replace-ip-source-with (Before Forwarding Packet) on page 1414
- always-write-option-82 on page 845

overrides (System Services DHCP)

Syntax

```
overrides {
  interface-client-limit number;
}
```

Hierarchy Level

```
[edit system services dhcp-local-server dhcpv6]
[edit system services dhcp-local-server dhcpv6 group group-name]
[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name]
```

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Override the default configuration settings for the extended DHCP local server. Specifying the **overrides** statement with no subordinate statements removes all DHCP local server overrides at that hierarchy level.

- To override global DHCP local server configuration options, include the **overrides** statement and its subordinate statements at the **[edit system services dhcp-local-server]** hierarchy level.
- To override configuration options for a named group of interfaces, include the statements at the **[edit system services dhcp-local-server dhcpv6 group *group-name*]** hierarchy level.
- To override configuration options for a specific interface within a named group of interfaces, include the statements at the **[edit system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name*]** hierarchy level.
- Use the DHCPv6 hierarchy levels to override DHCPv6 configuration options.

Options

interface-client-limit *number*—Sets the maximum number of DHCP clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group.

Range: 1 through 500,000

Default: No limit

Required Privilege Level

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*

password (Login)

Syntax

```
password {
  change-type (set-transitions | character-set);
  format (sha1 | sha256 | sha512);
  maximum-length length;
  minimum-changes number;
  minimum-length length;
}
```

Hierarchy Level

```
[edit system login]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure special requirements such as character length and encryption format for plain-text passwords. Newly created passwords must meet these requirements.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

password (Access Control Service)

Syntax password *password*;

Hierarchy Level [edit services unified-access-control infranet-controller *hostname*]

Release Information Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description Configure the password to connect the switch to the Junos Pulse Access Control Service network access control (NAC) device. This password must match the password specified on the Access Control Service though its administrative interface.

Options ***password***—A string of up to 200 alphanumeric characters bounded by quotation marks. Spaces are allowed, but special characters, such as **?**, are not allowed.

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

Related Documentation

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 401
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 404

password (DHCP Local Server)

Syntax

password *password-string*;

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the password that is sent to the external AAA authentication server for subscriber authentication or DHCP client authentication.

Options

password-string—Authentication password.

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

Related Documentation
- Using External AAA Authentication Services with DHCP on page 651

password (DHCP Relay Agent)

Syntax

password *password-string*;

Hierarchy Level

[edit forwarding-options dhcp-relay authentication],
[edit forwarding-options dhcp-relay dhcpv6 authentication],
[edit forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name* authentication],
[edit forwarding-options dhcp-relay group *group-name* authentication],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name* authentication],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay authentication],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 authentication],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* authentication],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay authentication],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 authentication],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* authentication],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Support at the **[edit ... dual-stack-group *dual-stack-group-name* authentication]** hierarchy level introduced in Junos OS Release 15.1.

Description

Configure the password that is sent to the external AAA authentication server for subscriber authentication or client authentication. Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

Options

password-string—Authentication password.

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651
- *Configuring Passwords for Usernames*

password (DHCP Local Server)

Syntax

password *password-string*;

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the password that is sent to the external AAA authentication server for subscriber authentication or DHCP client authentication.

Options

password-string—Authentication password.

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

Related Documentation
- Using External AAA Authentication Services with DHCP on page 651

password (Login)

Syntax

```
password {
  change-type (set-transitions | character-set);
  format (sha1 | sha256 | sha512);
  minimum-character-changesnumber
  maximum-length length;
  maximum-lifetime days
  minimum-changes number;
  minimum-length length;
  minimum-lifetime days
  minimum-lower-cases number;
  minimum-numerics number;
  minimum-punctuations number;
  minimum-reuse number;
  minimum-upper-cases number;
}
```

Hierarchy Level
[edit system login]

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

Description
Configure special requirements such as character length and encryption format for plain-text passwords. Newly created passwords must meet these requirements.

Using several password minimum requirement options will cause the **minimum-length** to be reset if the total sum of the required minimums exceeds the **minimum-length** setting.

The individual statements are explained separately.

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

Related Documentation
- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 153

path-length

Syntax path-length *certificate-path-length*;

Hierarchy Level [edit security certificates]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the digital certificate path length.

Options ***certificate-path-length***—Digital certificate path length.

Range: 2 through 15 certificates

Default: 15 certificates

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

Related Documentation

- *Configuring the Path Length for the Certificate Hierarchy*

partition (Gx-Plus)

Syntax

```
partition partition-name {
  diameter-instance instance-name;
  destination-host hostname;
  destination-realm realm;
}
```

Hierarchy Level

[edit access gx-plus]

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure a Gx-Plus partition.

Options

partition-name—Name of the Gx-Plus partition.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Configuring Gx-Plus*
- *Configuring the Gx-Plus Partition*

peer (NTP)

Syntax peer *address* <key *key-number*> <version *value*> <prefer>;

Hierarchy Level [edit system *ntp*]

Release Information Statement introduced before Junos OS Release 7.4.

Description For NTP, configure the SRX Series device to operate in symmetric active mode with the remote system at the specified address. In this mode, the SRX Series device and the remote system can synchronize with each other. This configuration is useful in a network in which either the SRX Series device or the remote system might be a better source of time.

Options

address—Address of the remote system. You must specify an address, not a hostname.

key *key-number*—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.

Range: Any unsigned 32-bit integer

prefer—(Optional) Mark the remote system as the preferred host, which means that if all other factors are equal, this remote system is chosen for synchronization among a set of correctly operating systems.

version *value*—(Optional) Specify the NTP version number to be used in outgoing NTP packets.

Range: 1 through 4

Default: 4

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

Related Documentation

- *ntp*

permissions

Syntax

```
permissions [ permissions ];
```

Hierarchy Level

```
[edit system login class]
```

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 login access privileges to be provided on the router or switch.

Options

permissions—Privilege type. For a list of permission flag types, see "Login Class Permission Flags" on page 91.

Required Privilege Level

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

Related Documentation

- Example: Configuring User Permissions with Access Privilege Levels on page 95
- user on page 1597

pool (DHCP Local Server Overrides)

Syntax

pool *pool-name*;

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server overrides process-inform],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 overrides process-inform],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* overrides process-inform],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides process-inform],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides process-inform],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* interface *interface-name* overrides process-inform],
[edit logical-systems *logical-system-name* system services dhcp-local-server overrides process-inform],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 overrides process-inform],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* overrides process-inform],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides process-inform],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* overrides process-inform],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* interface *interface-name* overrides process-inform],
[edit routing-instances *routing-instance-name* system services dhcp-local-server overrides process-inform],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 overrides process-inform],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* overrides process-inform],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides process-inform],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides process-inform],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* interface *interface-name* overrides process-inform],
[edit system services dhcp-local-server overrides process-inform],
[edit system services dhcp-local-server dhcpv6 overrides process-inform],
[edit system services dhcp-local-server dhcpv6 group *group-name* overrides process-inform],
[edit system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides process-inform],
[edit system services dhcp-local-server group *group-name* overrides process-inform],
[edit system services dhcp-local-server group *group-name* interface *interface-name* overrides process-inform]

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure DHCP or DHCPv6 local server to reply to DHCP information request messages (DHCPINFORM for DHCPv4 and INFORMATION-REQUEST for DHCPv6) with information taken from the specified pool without interacting with AAA.

Options

pool-name—Name of the address pool, which must be configured within **family inet** for DHCP local server and within **family inet6** for DHCPv6 local server.

Required Privilege Level

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

Related Documentation

- Enabling Processing of Client Information Requests on page 658
- Overriding the Default DHCP Local Server Configuration Settings Overview on page 630

pool (System)

Syntax

```
pool address/prefix-length {
  address-range {
    low address;
    high address;
  }
  exclude-address {
    address;
  }
}
```

Hierarchy Level

```
[edit system services dhcp],
```

Release Information

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

Description

For J Series Services Routers and EX Series switches only. Configure a pool of IP addresses for DHCP clients on a subnet. When a client joins the network, the DHCP server dynamically allocates an IP address from this pool.

Options

address-range—Lowest and highest IP addresses in the pool that are available for dynamic address assignment. If no range is specified, the pool will use all available addresses within the subnet specified. (Broadcast addresses, interface addresses, and excluded addresses are not available.)

exclude-address—Addresses within the range that are not used for dynamic address assignment. You can exclude one or more addresses within the range.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- address-assignment (Address-Assignment Pools) on page 855

pool-match-order

Syntax

```
pool-match-order {
  external-authority;
  ip-address-first;
  option-82;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
[edit logical-systems *logical-system-name* system services dhcp-local-server],
[edit routing-instances *routing-instance-name* system services dhcp-local-server],
[edit system services dhcp-local-server]

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1.

Description

Configure the order in which the DHCP local server uses information in the DHCP client PDU to determine how to obtain an address for the client.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Default

DHCP local server uses the **ip-address-first** method to determine which address pool to use.

Required Privilege Level

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

Related Documentation

- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 701
- Extended DHCP Local Server Overview on page 562

port (Access Control Service)

Syntax port *port-number*;

Hierarchy Level [edit services unified-access-control infranet-controller]

Release Information Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description Configure the switch's connection to the security port on the Junos Pulse Access Control Service network access control (NAC) device.

NOTE: Do not change this port setting.

Options *port-number*—11123

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

Related Documentation

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 401
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 404

port (HTTP/HTTPS)

Syntax port *port-number*;

Hierarchy Level [edit system services web-management]

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 on which the HTTP or HTTPS service is connected.

Options ***port-number***—The TCP port number on which the specified service listens.

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

Related Documentation

- *Secure Management Access Configuration Summary*
- *J-Web Interface User Guide*
- http on page 1128
- https on page 1129
- web-management on page 1622

port (NETCONF)

Syntax port *port-number*;

Hierarchy Level [edit system services netconf]

Release Information Statement introduced in Junos OS Release 10.0.

Description Configure the TCP port used for NETCONF-over-SSH connections.

NOTE:

- The configured port accepts only NETCONF-over-SSH connections. Regular SSH session requests for this port are rejected.
- The default SSH port (22) continues to accept NETCONF sessions even with a configured NETCONF server port. To disable the SSH port from accepting NETCONF sessions, you can specify this in the login event script.
- We do not recommend configuring the default ports for FTP (21) and Telnet (23) services for configuring NETCONF-over-SSH connections.

Options port *port-number*—Port number on which to enable incoming NETCONF connections over SSH.

Default: 830 (as specified in RFC 4742, *Using the NETCONF Configuration Protocol over Secure Shell (SSH)*)

Range: 1 through 65535

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

Related Documentation

- *NETCONF XML Management Protocol Guide*
- Configuring NETCONF-Over-SSH Connections on a Specified TCP Port on page 244

port (RADIUS Server)

Syntax port *port-number*;

Hierarchy Level [edit system radius-server *address*],
[edit system accounting destination radius server *address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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

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

Default: 1812 (as specified in RFC 2865)

NOTE: The **[edit system accounting]** hierarchy is not available on QFabric systems.

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

Related Documentation

- Configuring RADIUS Server Authentication on page 182

port (SRC Server)

Syntax port *port-number*;

Hierarchy Level [edit system services service-deployment servers *server-address*]

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

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

Options ***port-number***—(Optional) The TCP port number for the SRC server.
Default: 3333

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

Related Documentation
- *Configuring the Junos OS to Work with SRC Software*

port (TACACS+ Server)

Syntax port *port-number*;

Hierarchy Level [edit system accounting destination tacplus server *server-address*]

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

Description Configure the port number on which to contact the TACACS+ server.

Options ***number***—Port number on which to contact the TACACS+ server.
Default: 49

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

Related Documentation
- Configuring TACACS+ System Accounting on page 219

power-negotiation

Syntax

```
power-negotiation {
  disable;
}
```

Hierarchy Level

[edit protocols lldp interface (all | *interface-name*)]

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Configure Link Layer Discovery Protocol (LLDP) power negotiation, which negotiates with Power over Ethernet (PoE) powered devices to allocate power.

LLDP power negotiation requires the PoE **management** option to be set to **class**.

The remaining statement is explained separately. See CLI Explorer.

Default

LLDP power negotiation is enabled by default when the PoE **management** option is set to **class**.

Required Privilege Level

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

Related Documentation

- Configuring LLDP (CLI Procedure) on page 512
- *Configuring PoE on EX Series Switches (CLI Procedure)*

preference (Subscriber Management)

Syntax

```
preference route-distance
```

Hierarchy Level

```
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options
  access route prefix],
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options
  rib routing-table-name access route prefix],
[edit dynamic-profiles profile-name routing-options access route prefix]
```

Release Information

Statement introduced in Junos OS Release 9.5.
Support at **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access route *prefix*]** and **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access route *prefix*]** hierarchy levels introduced in Junos OS Release 10.1.

Description

Dynamically configure the distance for an access route.

Options

route-distance—Either the specific distance you want to assign to the access route or either of the following distance variables:

- **$junos-framed-route-distance**—Distance of an IPv4 access route; the variable is dynamically replaced with the preference value (Subattribute 5) from the RADIUS Framed-Route attribute [22].
- **$junos-framed-route-ipv6-distance**—Distance of an IPv6 access route; the variable is dynamically replaced with the preference value (Subattribute 5) from the RADIUS Framed-IPv6-Route attribute [99].

Required Privilege Level

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

Related Documentation

- *Configuring Dynamic Access Routes for Subscriber Management*

prefix

Syntax

```
prefix {
  host-name;
  logical-system-name;
  routing-instance-name;
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client
  client-identifier]
```

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Specify a prefix as a client identifier.

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

Related Documentation

prefix (DHCP Relay Agent)

Syntax

```
prefix prefix;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id |
  relay-agent-remote-id)],
[edit forwarding-options dhcp-relay dhcpv6 group group-name (relay-agent-interface-id |
  relay-agent-remote-id)],
[edit forwarding-options dhcp-relay relay-option-82 (circuit-id | remote-id)],
[edit forwarding-options dhcp-relay group group-name relay-option-82 (circuit-id |
  remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay dhcpv6
  (relay-agent-interface-id | relay-agent-remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay ... relay-option-82
  (circuit-id | remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6
  (relay-agent-interface-id | relay-agent-remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...
  relay-option-82 (circuit-id | remote-id)]
```

Release Information

Statement introduced in Junos OS Release 8.3.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.
Support at the **[edit ... relay-agent-remote-id]** and **[edit ... remote-id]** hierarchy levels introduced in Junos OS Release 14.1.

Description

Add a prefix to the DHCP base option 82 Agent Circuit ID (suboption 1) or Agent Remote ID (suboption 2) information, or to the DHCPv6 option 18 (Relay Agent Interface-ID) or option 37 (Relay Agent Remote-ID) information in DHCP packets that DHCP relay agent sends to a DHCP server. The prefix can consist of any combination of the hostname, logical system name, and routing instance name.

Options

prefix—Any of the following:

- **host-name**—Prepend the hostname of the router configured with the **host-name** statement at the **[edit system]** hierarchy level to the DHCP option information.
- **logical-system-name**—Prepend the name of the logical system to the option information.
- **routing-instance-name**—Prepend the name of the routing instance to the option information.

Required Privilege Level

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

Related Documentation

- *Including a Prefix in DHCP Options*
- Using DHCP Relay Agent Option 82 Information on page 633

- *Configuring DHCPv6 Relay Agent Options*

preferred-prefix-length

Syntax

```
preferred-prefix-length preferred-prefix-length;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client
  prefix-delegating]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
  family inet6 dhcpv6-client prefix-delegating]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6
  dhcpv6-client prefix-delegating]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30 and in Junos OS Release 15.1X49-D100.
The **logical-systems** and **tenants** options are introduced in Junos OS Release 18.4R1.

Description

Allows you to configure DHCPv6 client preferred prefix length. If preferred-prefix-length is configured, the DHCPv6 client checks the prefix length in the ADVERTISE packet and if the check fails, a sysolg is created.

Required Privilege Level

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

Related Documentation

- sub-prefix-length on page 1512

process-inform

Syntax

```
process-inform {
    pool pool-name;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* interface *interface-name* overrides],
[edit logical-systems *logical-system-name* system services dhcp-local-server overrides],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 overrides],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* overrides],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* overrides],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* interface *interface-name* overrides],
[edit routing-instances *routing-instance-name* system services dhcp-local-server overrides],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 overrides],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* overrides],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* interface *interface-name* overrides],
[edit system services dhcp-local-server overrides],
[edit system services dhcp-local-server dhcpv6 overrides],
[edit system services dhcp-local-server dhcpv6 group *group-name* overrides],
[edit system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides],
[edit system services dhcp-local-server group *group-name* overrides],
[edit system services dhcp-local-server group *group-name* interface *interface-name* overrides]

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Enable the processing of DHCP information request messages (DHCPINFORM for DHCPv4 and INFORMATION-REQUEST for DHCPv6) sent from the client to request DHCP options. For DHCP local servers, the messages are also passed to the configured server list.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Default Information request messages are not processed.

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

Related Documentation

- Enabling Processing of Client Information Requests on page 658
- Overriding the Default DHCP Local Server Configuration Settings Overview on page 630

profile

Syntax

```
profile profile-name {
  accounting (Access Profile) {
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    order (radius | [ accounting-order-data-list ];
  }
  authentication-order [authentication-method];
  radius {
    accounting-server [server-addresses];
    authentication-server [server-addresses];
  }
}
```

Hierarchy Level

```
[edit access]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure an access profile. The access profile contains the entire authentication, authorization, and accounting (AAA) configuration that aids in handling AAA requests, including the authentication method and order, AAA server addresses, and AAA accounting.

Default

Not enabled.

Options

profile-name—Profile name of up to 32 characters.

The remaining statements are explained separately. See CLI Explorer.

NOTE: **The [edit access] hierarchy is not available on QFabric systems.**

Required Privilege Level

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

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335

profilerd

Syntax

```
profilerd {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the profiler process.

Options

- **command** ***binary-file-path***—Path to binary for process.
- **disable**—Disable the profiler process.
- **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
  - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
  - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

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

protocols

Syntax

```
protocols {
  bgp {
    disable;
    accept-remote-nexthop;
    advertise-external <conditional>;
    advertise-inactive;
    (advertise-peer-as | no-advertise-peer-as);
    authentication-algorithm (aes-128-cmac-96 | hmac-sha-1-96 | md5);
    authentication-key key;
    authentication-key-chain key-chain;
    bfd-liveness-detection {
      authentication {
        algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
          meticulous-keyed-sha-1 | simple-password);
        key-chain key-chain-name;
        loose-check;
      }
      detection-time {
        threshold milliseconds;
      }
      hold-down-interval milliseconds;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      session-mode (automatic | multihop | single-hop);
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (1 | automatic);
    }
    cluster cluster-identifier;
    damping;
    description text-description;
    export [ policy-names ];
    family family-name {
      ... the family subhierarchies appear after the main [edit protocols bgp] hierarchy ...
    }
    graceful-restart {
      disable;
      restart-time seconds;
      stale-routes-time seconds;
    }
    group group-name {
      ... the group subhierarchy appears after the main [edit protocols bgp] hierarchy ...
    }
    hold-time seconds;
    import [ policy-names ];
    include-mp-next-hop;
    keep (all | none);
```

```
    local-address address;
    local-as autonomous-system <loops number> < alias> <private>;
    local-preference local-preference;
    log-updown;
    metric-out (metric | igp (delay-med-update | offset) | minimum-igp offset);
    mtu-discovery;
    multihop {
      no-nexthop-change;
      ttl ttl-value;
    }
    no-aggregator-id;
    no-client-reflect;
    out-delay seconds;
    outbound-route-filter {
      bgp-orf-cisco-mode;
      prefix-based {
        accept {
          inet;
          inet6;
        }
      }
    }
    passive;
    path-selection {
      always-compare-med;
      as-path-ignore;
      cisco-non-deterministic;
      external-router-id;
      med-plus-igp {
        igp-multiplier number;
        med-multiplier number;
      }
    }
    peer-as autonomous-system;
    preference preference;
    remove-private;
    tcp-mss segment-size;
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
}
dcbx {
    disable;
    interface (interface-name | all) {
      disable;
      application-map application-map-name;
      applications {
        no-auto-negotiation;
      }
      enhanced-transmission-selection {
        no-auto-negotiation;
        no-recommendation-tlv;
        recommendation-tlv {
```

```
            no-auto-negotiation;
          }
        }
        dcbx-version (auto-negotiate | ieee-dcbx | dcbx-version-1.01);
        priority-flow-control {
          no-auto-negotiation;
        }
      }
    }
    iccp {
      authentication-key string;
      local-ip-addr local-ip-addr;
      peer ip-address{
        authentication-key string;
        backup-liveness-detection {
          backup-peer-ip ip-address;
        }
        liveness-detection {
          detection-time {
            threshold milliseconds;
          }
          minimum-intervalmilliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
          version (Liveness Detection) (1 | automatic);
        }
        local-ip-addr ipv4-address;
        session-establishment-hold-time seconds;
      }
      session-establishment-hold-time seconds;
      traceoptions {
        file <filename> <files number> <match regular-expression> <microsecond-stamp>
          <size size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
      }
    }
    igmp-snooping {
      traceoptions {
        file filename <files number> <size size> <world-readable | no-world-readable> <match
          regex>;
        flag flag (detail | disable | receive | send);
      }
      vlan vlan-name {
        disable;
        }
        interface interface-name {
          group-limit limit;
          multicast-router-interface;
          static {
```

```
            group ip-address;
          }
        }
        robust-count number;
      }
    }
    isis {
      disable;
      export [ policy-names ];
      ignore-attached-bit;
      interface interface-name {
        bfd-liveness-detection {
          authentication {
            algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
              meticulous-keyed-sha-1 | simple-password);
            key-chain key-chain-name;
            loose-check;
          }
          detection-time {
            threshold milliseconds;
          }
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
          version (1 | automatic);
        }
        checksum;
        csnp-interval (seconds | disable);
        disable;
        hello-padding (adaptive | loose | strict);
        level (1 | 2) {
          disable;
          hello-authentication-key key;
          hello-authentication-type authentication;
          hello-interval seconds;
          hold-time seconds;
          ipv4-multicast-metric number;
          metric metric;
          passive;
          priority number;
        }
        lsp-interval milliseconds;
        mesh-group (value | blocked);
        no-ipv4-multicast;
        no-unicast-topology;
        passive;
        point-to-point;
      }
      level (1 | 2) {
        disable;
```

```
      authentication-key key;
      authentication-type authentication;
      external-preference preference;
      no-csnp-authentication;
      no-hello-authentication;
      no-psnp-authentication;
      preference preference;
      prefix-export-limit number;
      wide-metrics-only;
    }
    loose-authentication-check;
    lsp-lifetime seconds;
    max-areas number;
    no-adjacency-holddown;
    no-authentication-check;
    no-ipv4-routing;
    overload {
      advertise-high-metrics;
      timeout seconds;
    }
    reference-bandwidth reference-bandwidth;
    rib-group {
      inet group-name;
    }
    topologies {
      ipv4-multicast;
    }
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    traffic-engineering {
      disable;
      family inet {
        shortcuts {
          multicast-rpf-routes:
        }
      }
    }
  }
  lldp {
    disable;
    advertisement-interval seconds;
    hold-multiplier number;
    interface (LLDP) (all | interface-name) {
      disable;
    }
    traceoptions {
      file filename <files number> <size size> <world-readable | no-world-readable> <match
        regex>;
      flag flag (detail | disable | receive | send);
    }
  }
  mstp {
```

```
    disable;
    bpdu-timeout-action;
    bridge-priority priority;
    configuration-name name;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
      disable;
      bpdu-timeout-action {
        block;
        alarm;
      }
      cost  cost;
      edge;
      mode mode;
      no-root-port;
      priority priority;
    }
    max-age seconds;
    max-hops hops;
    msti msti-id {
      vlan (vlan-id | vlan-name);
      interface interface-name {
        disable;
        cost  cost;
        edge;
        mode mode;
        priority priority;
      }
    }
    revision-level revision-level;
    traceoptions {
      file filename <files number > <size size> <no-stamp | world-readable |
        no-world-readable>;
      flag flag;
    }
}
ospf {
    disable;
    area area-id {
      area-range ip-prefix</prefix-length> <exact> <override-metric metric> <restrict>;
      context-identifier identifier
      interface interface-name {
        disable;
        authentication {
          md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
          simple-password key-string;
        }
        bandwidth-based-metrics {
          bandwidth value metric number;
        }
        bfd-liveness-detection {
          authentication {
            algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
              meticulous-keyed-sha-1 | simple-password);
```

```
            key-chain key-chain-name;
            loose-check;
          }
          detection-time {
            threshold milliseconds;
          }
          full-neighbors-only;
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
          version (1 | automatic);
        }
        dead-interval seconds;
        dynamic-neighbors;
        flood-reduction;
        hello-interval seconds;
        interface-type (nbma | p2mp | p2p);
        metric metric;
        neighbor address <eligible>;
        no-eligible-backup;
        no-interface-state-traps;
        no-neighbor-down-notification;
        passive {
          traffic-engineering {
            remote-node-id address;
          }
        }
        poll-interval seconds;
        priority number;
        retransmit-interval seconds;
        secondary;
        te-metric metric;
        topology (name | default | ipv4-multicast) {
          disable;
          bandwidth-based-metrics {
            bandwidth value;
            metric number;
          }
          metric metric;
        }
        transit-delay seconds;
      }
      network-summary-export [ policy-names ];
      network-summary-import [ policy-names ];
      nssa {
        area-range ip-prefix</prefix-length> <exact> <override-metric metric> <restrict>;
        default-lsa {
          default-metric metric;
          metric-type type;
          type-7;
```

```
      }
      (summaries | no-summaries);
    }
    stub <default-metric metric> <summaries | no-summaries>;
    virtual-link neighbor-id router-id transit-area area-id {
      disable;
      authentication {
        md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
        simple-password key-string;
      }
      dead-interval seconds;
      demand-circuit;
      flood-reduction;
      hello-interval seconds;
      ipsec-sa sa-name;
      no-neighbor-down-notification;
      retransmit-interval seconds;
      topology (name | default | ipv4-multicast) {
        disable;
        metric metric;
      }
      transit-delay seconds;
    }
  }
  database-protection {
    ignore-count number;
    ignore-time seconds;
    maximum-lsa number;
    reset-time seconds;
    warning-only;
    warning-threshold percent;
  }
  export [ policy-names ];
  external-preference preference;
  graceful-restart {
    disable;
    helper-disable <both | restart-signaling | standard>;
    no-strict-lsa-checking;
    notify-duration seconds;
    restart-duration seconds;
  }
  import [ policy-names ];
  no-nssa-abr;
  no-rfc-1583;
  overload <timeout seconds>;
  preference preference;
  prefix-export-limit number;
  reference-bandwidth reference-bandwidth;
  rib-group group-name;
  topology (default | ipv4-multicast | name) {
    overload;
    prefix-export-limit number;
    topology-id number;
  }
  traceoptions {
```

```
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    traffic-engineering {
      advertise-unnumbered-interfaces;
      credibiliity-protocol-preference;
      ignore-lsp-metrics;
      multicast-rpf-routes;
      no-topology;
      shortcuts <lsp-metric-into-summary>;
    }
}
pim {
    disable;
    assert-timeout seconds;
    dense-groups {
      addresses;
    }
    dr-election-on-p2p;
    export;
    family (inet | inet6) {
      disable;
    }
    graceful-restart {
      disable;
      restart-duration seconds;
    }
    import [ policy-names ];
    interface interface-name {
      accept-remote-source;
      disable;
      family (inet | inet6) {
        disable;
      }
      hello-interval seconds;
      mode (dense | sparse | sparse-dense);
      neighbor-policy [ policy-names ];
      override-interval milliseconds;
      priority number;
      propagation-delay milliseconds;
      reset-tracking-bit;
      version version;
    }
    join-load-balance;
    join-prune-timeout;
    nonstop-routing;
    override-interval milliseconds;
    propagation-delay milliseconds;
    reset-tracking-bit;
    rib-group group-name;
    rp {
      auto-rp {
        (announce | discovery | mapping);
        (mapping-agent-election | no-mapping-agent-election);
```

```
    }
    bootstrap {
      family (inet | inet6) {
        export [ policy-names ];
        import [ policy-names ];
        priority number;
      }
    }
    bootstrap-import [ policy-names ];
    bootstrap-export [ policy-names ];
    bootstrap-priority number;
    dr-register-policy [ policy-names ];
    embedded-rp {
      group-ranges {
        destination-ip-prefix</prefix-length>;
      }
      maximum-rps limit;
    }
    local {
      family (inet | inet6) {
        address address;
        anycast-pim {
          disable;
            rp-set {
            address address <forward-msdp-sa>;
          }
          local-address address;
        }
        group-ranges {
          destination-ip-prefix</prefix-length>;
        }
        hold-time seconds;
        priority number;
      }
    }
    rp-register-policy [ policy-names ];
    spt-threshold {
      infinity [ policy-names ];
    }
    static {
      address address {
        group-ranges {
        version version;
        destination-ip-prefix</prefix-length>;
        }
      }
    }
  }
  rpf-selection {
    group group-address{
      source source-address{
        next-hop next-hop-address;
      }
      wildcard-source {
        next-hop next-hop-address;
```

```
        }
      }
      prefix-list prefix-list-addresses {
        source source-address {
          next-hop next-hop-address;
        }
        wildcard-source {
          next-hop next-hop-address;
        }
      }
    traceoptions {
      file filename <files number> <size size> <world-readable | no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    tunnel-devices [ mt-fpc/pic/port ];
}
rip {
    authentication-key password;
    authentication-type type;
    (check-zero | no-check-zero);
    group group-name {
      bfd-liveness-detection {
        authentication {
          algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
            meticulous-keyed-sha-1 | simple-password);
          key-chain key-chain-name;
          loose-check;
        }
        detection-time {
          threshold milliseconds;
        }
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        version (1 | automatic);
      }
      export [ policy-names ];
      import [ policy-names ];
      metric-out metric;
        neighbor neighbor-name {
          any-sender;
          authentication-key password;
          authentication-type type;
          bfd-liveness-detection {
            ... same statements as at the [edit protocols rip group group-name
              bfd-liveness-detection] hierarchy level ...
          }
          (check-zero | no-check-zero);
          import [ policy-names ];
          message-size number;
```

```
            metric-in metric;
            receive (both | none | version-1 | version-2);
            route-timeout seconds;
            send (broadcast | multicast | none | version-1);
            update-interval seconds;
          }
        preference preference;
        route-timeout seconds;
        update-interval seconds;
    }
    holddown seconds;
    import [ policy-names ];
    message-size number;
    metric-in metric;
    receive (both | none | version-1 | version-2);
    rib-group group-name;
    route-timeout seconds;
    send (broadcast | multicast | none | version-1);
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    update-interval seconds;
}
rstp {
    disable;
    bpdu-block-on-edge;
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
      disable;
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost  cost;
      edge;
      mode mode;
      no-root-port;
      priority priority;
    }
    max-age seconds;
    }
    traceoptions {
      file filename <files number > <size size> <no-stamp> <world-readable |
        no-world-readable>;
      flag flag;
    }
}
stp {
    disable;
    bridge-priority priority;
    forward-delay seconds;
```

```
    hello-time seconds;
    interface (all | interface-name) {
      disable;
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost  cost;
      edge;
      mode mode;
      no-root-port;
      priority priority;
    }
    max-age seconds;
  }
    traceoptions {
      file filename <files number > <size size> <no-stamp | world-readable |
        no-world-readable>;
      flag flag;
    }
  uplink-failure-detection {
    group group-name {
      link-to-monitor interface-name;
      link-to-disable interface-name;
    }
  }
  vstp {
    bpdu-block-on-edge;
    disable;
    force-version stp;
    vlan vlan-id {
      bridge-priority priority;
      forward-delay seconds;
      hello-time seconds;
      interface (all | interface-name) {
        bpdu-timeout-action (Spanning Trees) {
          block;
          log;
        }
        cost  cost;
        disable;
        edge (Spanning Trees);
        mode mode;
        no-root;
        priority priority;
      }
      max-age seconds;
      traceoptions {
        file filename <files number > <size size> <no-stamp | world-readable |
          no-world-readable>;
        flag flag;
      }
    }
  }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure protocols.

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation
- *Junos OS Routing Protocols Configuration Guide*

protocol-version

Syntax protocol-version [v2];

Hierarchy Level [edit system services ssh]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Specify the Secure Shell (SSH) protocol version.

Default **v2**—SSH protocol version 2 is the default, introduced in Junos OS Release 11.4.

Options SSH protocol version **v2**.

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

Related Documentation
- Configuring SSH Service for Remote Access to the Router or Switch on page 232

provisioning-order (Diameter Applications)

Syntax

```
provisioning-order (gx-plus | jsrc | pcrf);
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.6.
Support for Gx-Plus introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
pcrf option added in Junos OS Release 16.2.

Description

Configure AAA to use the specified application for subscriber service provisioning.

Options

gx-plus—Specify Gx-Plus as the application used to communicate with a PCRF server for subscriber service provisioning. Sets the Subscription-Id-Type Diameter AVP sub-attribute (450) to 4 (END_USER_PRIVATE) and sets the Subscription-Id-Data Diameter AVP sub-attribute (444) to **reserved**. Both of these sub-attributes are conveyed in the Diameter AVP Subscription-ID (443) by a CCR-I message.

jsrc—Specify JSRC as the application used to communicate with the SAE for subscriber service provisioning. JSRC is used in an SRC environment to request services from the SAE for an authenticated subscriber. JSRC attempts to activate these services. If successful, JSRC returns an ACK message. If unsuccessful, the subscriber is denied access.

pcrf—Specify Policy Control and Charging Rules Function (PCRF) as the application used to request provisioning from the PCRF server over the Gx protocol. If you change this configuration, any existing subscriber sessions are unaffected.

Required Privilege Level

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

Related Documentation

- *JSRC Configuration Overview*
- *Provisioning Subscribers with JSRC*
- *Configuring Gx-Plus*
- *Provisioning Subscribers with Gx-Plus*
- *Understanding Gx Interactions Between the Router and the PCRF*
- *Understanding Interactions Between the PCRF, PCEF, and OCS*

proxy

Syntax

```
proxy {
   password password;
   port port-number;
   server url;
   username user-name;
}
```

Hierarchy Level

```
[edit system]
```

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the proxy information for the router.

Options

- **password *password***—Password configured in the proxy server.
- **port *port number***—Proxy server port number.

  Range: 0 through 65,535
- **server *url***—URL or IP address of the proxy server host.
- **username *username***—Username configured in the proxy server.

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

proxy-mode

Syntax

```
proxy-mode;
```

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* interface *interface-name* overrides]

Release Information

Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Enable DHCP relay proxy mode on the extended DHCP relay. Proxy mode supports all extended DHCP relay functionality.

You cannot configure both the DHCP relay proxy and the extended DHCP local server on the same interface.

Required Privilege Level

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

Related Documentation

- DHCP Relay Proxy Overview on page 646
- Extended DHCP Relay Agent Overview on page 618
- Enabling DHCP Relay Proxy Mode on page 647

ptopo-configuration-maximum-hold-time

Syntax ptopo-configuration-maximum-hold-time *seconds*;

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 9.6 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure how long to maintain the physical topology database entries. The physical topology identifies the devices on the network and their physical interconnections.

Options *seconds*—Time to maintain physical topology database entries.

Default: 300

Range: 1 through 2147483647

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

Related Documentation

- show lldp on page 1826
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518
- Understanding LLDP on page 511

ptopo-configuration-trap-interval

Syntax ptopo-configuration-trap-interval *seconds*;

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 9.6 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify how often SNMP trap notifications are sent regarding changes in physical topology global statistics.

Default SNMP trap notifications of changes in physical topology global statistics are disabled.

Options ***seconds***—Interval between SNMP trap notifications about physical topology global statistics.

Range: 0 through 3600

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

quiet-period

Syntax quiet-period *seconds*;

Hierarchy Level [edit protocols dot1x authenticator interface (802.1X) (all | [*interface-names*])]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description For 802.1X authentication, configure the number of seconds the interface remains in the wait state following a failed authentication attempt by a supplicant before reattempting authentication.

Default 60 seconds

Options ***seconds***—Number of seconds the interface remains in the wait state.

Range: 0 through 65,535 seconds

Default: 60 seconds

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

Related Documentation

- show network-access aaa statistics authentication on page 1855
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302

quiet-period (Captive Portal)

Syntax

```
quiet-period seconds;
```

Hierarchy Level

```
[edit services captive-portal interface (all | interface-names)]
```

Release Information Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description Configure time, in seconds, after a user exceeds the maximum number of retries before they can attempt to authenticate.

Options *seconds*—Number of seconds.

Range: 1–65535

Default: 60

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

Related Documentation

- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

radius

Syntax

```
radius {
  accounting-server [server-addresses];
  authentication-server [server-addresses];
}
```

Hierarchy Level

[edit access profile *profile-name*]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure the RADIUS servers for authentication and for accounting. To configure multiple RADIUS servers, include multiple **radius** 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.

The remaining statements are explained separately. See CLI Explorer.

NOTE: The **[edit access]** hierarchy is not available on QFabric systems.

Required Privilege Level

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

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 297

radius (System)

Syntax

```
radius {
  server {
    server-address {
      accounting-port port-number;
      secret password;
      source-address address;
      retry number;
      timeout seconds;
    }
  }
}
```

Hierarchy Level

[edit system accounting destination]

Release Information

Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the RADIUS accounting server.

Options

server-address—Address of the RADIUS accounting server.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Configuring RADIUS System Accounting on page 200

radius (Access Profile)

Syntax

```
radius {
  accounting-server [ ip-address ];
  attributes {
    exclude
      attribute-name packet-type;
      standard-attribute number {
        packet-type [ access-request | accounting-off | accounting-on | accounting-start |
          accounting-stop ];
      }
      vendor-id id-number {
        vendor-attribute vsa-number {
          packet-type [ access-request | accounting-off | accounting-on | accounting-start
            | accounting-stop ];
        }
      }
    }
    ignore {
      dynamic-iflset-name;
      framed-ip-netmask;
      idle-timeout;
      input-filter;
      logical-system-routing-instance;
      output-filter;
      session-timeout;
      standard-attribute number;
      vendor-id id-number {
        vendor-attribute vsa-number;
      }
    }
  }
  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;
    }
    chap-challenge-in-request-authenticator;
    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-channel;
      exclude-sub-interface;
    }
    ip-address-change-notify message;
```

```
juniper-access-line-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;
   interface-text-description;
   nas-identifier;
   order {
      agent-circuit-id;
      agent-remote-id;
      interface-description;
      interface-text-description;
      nas-identifier;
      postpend-vlan-tags;
   }
   postpend-vlan-tags;
}
nas-port-type {
   ethernet {
      port-type;
   }
}
override {
   calling-station-id remote-circuit-id;
   nas-ip-address tunnel-client-gateway-address;
   nas-port tunnel-client-nas-port;
   nas-port-type tunnel-client-nas-port-type;
}
remote-circuit-id-delimiter;
remote-circuit-id-fallback;
remote-circuit-id-format {
   agent-circuit-id;
   agent-remote-id;
}
revert-interval interval;
service-activation {
   dynamic-profile (optional-at-login | required-at-login);
   extensible-service (optional-at-login | required-at-login);
```

```
    }
    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.

Options

accounting-server—(MX Series only) Specify a list of the RADIUS accounting servers used for accounting for DHCP, L2TP, and PPP clients.

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

authentication-server—(SRX Series only) 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.

Values: *ip-address*—IPv4 address.

preauthentication-server—(MX Series only) Starting in Junos OS Release 13.3, specify the RADIUS preauthentication server, which is used for the LLID service.

NOTE: You cannot configure this statement if the Calling-Station-ID attribute is excluded from RADIUS Access-Request messages by the exclude statement.

Values: *ip-address*—IPv4 address.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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*
- *RADIUS Logical Line Identifier (LLID) Overview*
- *Configuring Logical Line Identification (LLID) Preauthentication*

radius (System)

Syntax

```
radius {
  server {
    server-address {
      accounting-port port-number;
      secret password;
      source-address address;
      retry number;
      timeout seconds;
    }
  }
}
```

Hierarchy Level

[edit system accounting destination]

Release Information

Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the RADIUS accounting server.

Options

server-address—Address of the RADIUS accounting server.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Configuring RADIUS System Accounting on page 200

radius-disconnect (DHCP Local Server)

Syntax

```
radius-disconnect;
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server reconfigure trigger],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure trigger],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* reconfigure trigger],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure trigger],
[edit logical-systems *logical-system-name* system services dhcp-local-server reconfigure trigger],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 reconfigure trigger],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* reconfigure trigger],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure trigger],
[edit routing-instances *routing-instance-name* system services dhcp-local-server reconfigure trigger],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure trigger],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* reconfigure trigger],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure trigger],
[edit system services dhcp-local-server reconfigure trigger],
[edit system services dhcp-local-server dhcpv6 reconfigure trigger],
[edit system services dhcp-local-server group *group-name* reconfigure trigger],
[edit system services dhcp-local-server dhcpv6 group *group-name* reconfigure trigger]

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6 ...]** hierarchy levels introduced in Junos OS Release 10.4.

Description

Configure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces to be reconfigured when a RADIUS-initiated disconnect is received by the DHCP client or group of clients. A group configuration takes precedence over a DHCP local server configuration.

Default

The client is deleted when a RADIUS-initiated disconnect is received.

Required Privilege Level

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

Related Documentation

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview on page 662
- Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 666

radius-options (edit system)

Syntax

```
radius-options {
  attributes {
    nas-ip-address ip-address;
  }
  enhanced-accounting;
  password-protocol mschap-v2;
}
```

Hierarchy Level

[edit system]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2.
MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

NOTE: The **radius-options** statement is not available on QFabric systems.

enhanced-accounting statement introduced in Junos OS Release 14.1.

Description

Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.

Options

enhanced-accounting—View the attribute values of a logged in user.

nas-ip-address ***ip-address***—IP address of the network access server (NAS) that requests user authentication.

password-protocol ***mschap-v2***—Protocol MS-CHAPv2, used for password authentication and password changing.

Required Privilege Level

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

Related Documentation

- Configuring MS-CHAPv2 for Password-Change Support on page 285
- Configuring RADIUS System Accounting on page 200
- **enhanced-accounting on page 1076**

radius-options (Protocols 802.1X)

Syntax

```
radius-options {
  use-vlan-id;
  use-vlan-name;
}
```

Hierarchy Level

[edit protocols dot1x authenticator]

Release Information

Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure 802.1X authenticator so that the VLAN ID or VLAN name is included in the packet sent to the RADIUS server to request authentication.

Options

use-vlan-id—Include the VLAN ID in the packet sent to the RADIUS server to request authentication.

use-vlan-name—Include the VLAN name in the packet sent to the RADIUS server to request authentication. The VLAN name is sent even if the 802.1X interface is configured with the VLAN ID.

Required Privilege Level

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

Related Documentation

- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- Specifying RADIUS Server Connections on Switches (CLI Procedure) on page 283
- authenticator on page 903

radius-options

Syntax

```
radius-options {
  attributes {
    nas-ip-address nas-ip-address;
  }
  password-protocol mschap-v2;
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced in Junos OS Release 8.5. Support for network access server (NAS) IPv6 address added in Junos OS Release 12.1X47-D15 for SRX1500, SRX5400, SRX5600, and SRX5800 devices.

Description

Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.

Options

- **attributes**—Configure RADIUS attributes.
  - **nas-ip-address *nas-ip-address***—Valid IPv4 or IPv6 address of the NAS requesting user authentication.
- **password-protocol mschap-v2**—Protocol MS-CHAPv2, used for password authentication and password changing.

Required Privilege Level

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

Related Documentation

- radius-server on page 1392

radius-options (Access)

Syntax

```
radius-options {
  revert-interval seconds;
}
```

Hierarchy Level

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

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure RADIUS options.

Options The remaining statement is explained separately.

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

Related Documentation

- *Junos OS Security Configuration Guide*

radius-options (edit system)

Syntax

```
radius-options {
  attributes {
    nas-ip-address ip-address;
  }
  enhanced-accounting;
  password-protocol mschap-v2;
}
```

Hierarchy Level

[edit system]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2.
MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

NOTE: The **radius-options** statement is not available on QFabric systems.

enhanced-accounting statement introduced in Junos OS Release 14.1.

Description

Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.

Options

enhanced-accounting—View the attribute values of a logged in user.

nas-ip-address ***ip-address***—IP address of the network access server (NAS) that requests user authentication.

password-protocol ***mschap-v2***—Protocol MS-CHAPv2, used for password authentication and password changing.

Required Privilege Level

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

Related Documentation

- Configuring MS-CHAPv2 for Password-Change Support on page 285
- Configuring RADIUS System Accounting on page 200
- **enhanced-accounting on page 1076**

radius-options (Protocols 802.1X)

Syntax

```
radius-options {
  use-vlan-id;
  use-vlan-name;
}
```

Hierarchy Level

[edit protocols dot1x authenticator]

Release Information

Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure 802.1X authenticator so that the VLAN ID or VLAN name is included in the packet sent to the RADIUS server to request authentication.

Options

use-vlan-id—Include the VLAN ID in the packet sent to the RADIUS server to request authentication.

use-vlan-name—Include the VLAN name in the packet sent to the RADIUS server to request authentication. The VLAN name is sent even if the 802.1X interface is configured with the VLAN ID.

Required Privilege Level

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

Related Documentation

- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- Specifying RADIUS Server Connections on Switches (CLI Procedure) on page 283
- authenticator on page 903

radius-server

Syntax

```
radius-server server-address {
  accounting-port port-number;
  port number;
  retry number;
  secret password;
  source-address source-address;
  timeout seconds;
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure a RADIUS server for Point-to-Point Protocol (PPP).

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

Options

server-address—Address of the RADIUS authentication server.

The remaining statements are explained separately. See CLI Explorer.

NOTE: The **accounting-port** and **source-address** options are not available on QFabric systems.

Required Privilege Level

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

Related Documentation

- Configuring RADIUS Authentication (QFX Series or OCX Series) on page 192
- *accounting-port*
- port on page 1339
- retry on page 1426
- *secret*
- *source-address*
- *timeout*

radius-server

Syntax

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

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
max-outstanding-requests introduced in Junos OS Release 11.4.
accounting-retry and **accounting-timeout** introduced in Junos OS Release 14.1.
dynamic-request-port option added in Junos OS Release 14.2R1 for MX Series routers.
preauthentication-port and **preauthentication-secret** options added in Junos OS Release 15.1 for MX Series routers.
accounting-port introduced in Junos OS Release 13.2X50-D10 for EX Series switches with support for Enhanced Layer 2 software (ELS). It was introduced in Junos OS without ELS in the following releases: Junos OS Releases 12.3R10, 14.1X53-D25, and 15.1R4 for EX Series switches.
Support for IPv6 ***server-address*** introduced in Junos OS Release 16.1.

Description

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

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

Options

server-address—IPv4 or IPv6 address of the RADIUS server.

accounting-port—(EX Series, M Series, MX Series, PTX Series, T Series only) Configure the port number on which to contact the RADIUS accounting server. This statement was introduced in Junos OS Release 13.2X50-D10 for EX Series switches with support for Enhanced Layer 2 software (ELS). It was introduced in Junos OS without ELS in the following releases: Junos OS Releases 12.3R10, 14.1X53-D25, and 15.1R4 for EX Series switches.

NOTE: Specifying the accounting port is optional, and port 1813 is the default. However, we recommend that you configure it in order to avoid confusion, as some RADIUS servers might refer to an older default.

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

Default: 1813

accounting-retry—(MX Series, T Series only) Starting in Junos OS Release 14.1, configure the number of times the device retransmits RADIUS accounting messages when no response is received from the server. When you do not configure this statement, the number of retry attempts is determined by the **retry** statement.

NOTE: To successfully set a retry limit for the accounting servers different from the authentication servers, you must configure both the **accounting-retry** and **accounting-timeout** statements . If you configure only one of these statements, then the value you configure is ignored in favor of the values configured with the **retry** and **timeout** statements.

NOTE: The maximum retry duration (the number of retries times the length of the timeout) cannot exceed 2700 seconds. An error message is displayed if you configure a longer duration.

Values: *number*—Number of retry attempts.

Range: 0 through 100

Default: 0 (disabled)

accounting-timeout—(MX Series, T Series only) Starting in Junos OS Release 14.1, configure how long the local device waits to receive a response from a RADIUS accounting server before retransmitting the message. When you do not configure this statement, the length of the timeout is determined by the **timeout** statement.

NOTE: To successfully set a timeout value for the accounting servers different from the authentication servers, you must configure both the **accounting-retry** and **accounting-timeout** statements . If you configure only one of these statements, then the value you configure is ignored in favor of the values configured with the **retry** and **timeout** statements.

NOTE: The maximum retry duration (the number of retries times the length of the timeout) cannot exceed 2700 seconds. An error message is displayed if you configure a longer duration.

Values: *seconds*—Duration of timeout period.

Range: 0 through 1000 seconds

Default: 0 (disabled)

dynamic-request-port—(MX Series only) Starting in Junos OS Release 14.2R1, specify the port that the router monitors for dynamic (CoA) requests from the specified RADIUS servers. You can configure a port globally or for a specific access profile.

You must either use the default port for all RADIUS servers or configure the same nondefault port for all RADIUS servers. This rule applies at both the global access and access profile levels.

NOTE: Any other configuration results in a commit check failure. Multiple port numbers—that is, different port numbers for different servers—are not supported.

Values: *port-number*—Number of the monitored port.

Default: 3799 (as specified in RFC 5176)

max-outstanding-requests—(MX Series only) Starting in Junos OS Release 11.4, configure the maximum number of outstanding requests for this RADIUS server. An increase in this value is immediate while a decrease is more gradual if the current number of outstanding requests exceeds the new value.

Values: *requests*—Maximum number of outstanding requests for this RADIUS server.

Range: 0 through 2000 outstanding requests per server

Default: 1000 outstanding requests per server

port—(EX Series, M Series, MX Series, SRX Series, T Series only) Configure the port number on which to contact the RADIUS server.

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

Default: 1812 (as specified in RFC 2865)

preauthentication-port—(MX Series only) Starting in Junos OS Release 15.1 for MX Series routers, configure the port number on which to contact the RADIUS server for logical line identification (LLID) preauthentication requests. If you do not configure a separate UDP port for preauthentication purposes, the same UDP port that you configure for authentication messages by including the **port *port-number*** statement is used.

Values: *port-number*—Port number used for preauthentication requests to contact the RADIUS server.

preauthentication-secret—(MX Series only) Starting in Junos OS Release 15.1 for MX Series routers, configure the password to use with the RADIUS server for LLID preauthentication requests. If you do not configure a separate UDP password for preauthentication purposes, the same password that you configure for authentication messages by including the **secret *password*** statement is used. The secret password used by the local router must match that used by the server.

Values: *password*—Password to use. To include spaces enclose the character string in quotation marks.

retry—(EX Series, M Series, MX Series, PTX Series, T Series only) Specify the number of times that the device is allowed to attempt to contact a RADIUS authentication or accounting server. You can override the retry limit for accounting servers with the **accounting-retry** statement.

NOTE: To successfully set a retry limit for the accounting servers different from the authentication servers, you must configure both the **accounting-retry** and **accounting-timeout** statements . If you configure only one of these statements, then the value you configure is ignored in favor of the values configured with the **retry** and **timeout** statements.

NOTE: The maximum retry duration (the number of retries times the length of the timeout) cannot exceed 2700 seconds. An error message is displayed if you configure a longer duration.

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

Range: 1 through 100

Default: 3

routing-instance—(SRX Series, vSRX only) Configure the routing instance used to send RADIUS packets to the RADIUS server.

Values: *routing-instance-name*—Routing instance name.

source-address—(SRX Series, vSRX only) Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. Support for IPv6 ***source-address*** was introduced in Junos OS Release 16.1.

Values: *source-address*—Valid IPv4 or IPv6 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.

timeout—(SRX Series, vSRX only) Configure the amount of time that the local device waits to receive a response from RADIUS authentication and accounting servers. You can override the timeout value for accounting servers with the **accounting-timeout** statement.

NOTE: To successfully set a timeout value for the accounting servers different from the authentication servers, you must configure both the **accounting-retry** and **accounting-timeout** statements . If you configure only one of these statements, then the value you configure is ignored in favor of the values configured with the **retry** and **timeout** statements.

NOTE: The maximum retry duration (the number of retries times the length of the timeout) cannot exceed 2700 seconds. An error message is displayed if you configure a longer duration.

Values: *seconds*—Amount of time to wait.

Range: 1 through 1000 seconds

Default: 3 seconds

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Configuring the PPP Authentication Protocol*
- *Configuring RADIUS Authentication for L2TP*
- Configuring RADIUS System Accounting on page 200
- *Configuring RADIUS-Initiated Dynamic Request Support*
- *RADIUS Logical Line Identifier (LLID) Overview*
- *RADIUS Attributes for LLID Preauthentication Requests*
- *show network-access aaa statistics*
- *clear network-access aaa statistics*

radius-server

Syntax

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

Hierarchy Level

```
[edit system]
```

Release Information Statement introduced in Junos OS Release 8.5. Support for IPv6 source address added in Junos OS Release 12.1X47-D15 for SRX1500, SRX5400, SRX5600, and SRX5800 devices.

Description Configure RADIUS server address for subscriber access management, Layer 2 Tunnelling Protocol (L2TP), or (Point-to-Point Protocol (PPP).

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

Options

- *server-address*—Address of the RADIUS server.
- **accounting-port** ***port-number***—RADIUS server accounting port number.

  Range: 1 through 65,335 files

  Default: 1813
- **port** ***port-number***—RADIUS server authentication port number.

  Range: 1 through 65,335 files

  Default: 1812
- **retry** ***value***—Number of times that the router is allowed to attempt to contact a RADIUS server.

  Range: 1 through 10

  Default: 3
- **secret** ***password***—Password to use; it can include spaces if the character string is enclosed in quotation marks.
- **max-outstanding-requests** ***value***—Maximum number of outstanding requests in flight to server.

  Range: 1 through 65,335 files

- **source-address** ***source-address***—Valid IPv4 or IPv6 address configured on one of the router or switch interfaces.
- **timeout** ***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.

radius-server (System)

Syntax

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

Hierarchy Level

```
[edit system]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure a RADIUS server for Point-to-Point Protocol (PPP).

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

Options
server-address—Address of the RADIUS authentication server.

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation
- Configuring RADIUS Server Authentication on page 182

radsec

Syntax

```
radsec {
  destination id-number {
    address ip-address;
    max-tx-buffers number;
    id-reuse-timeout seconds;
    port port-number;
    source-address ip-address;
    tls-certificate certificate-name;
    tls-force-ciphers [medium | low];
    tls-min-version [v1.1 | v1.2];
    tls-peer-name x0.radsec.com;
    tls-timeout seconds;
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 19.1R1.

Description Configure RADIUS over TLS, also known as RADSEC, to redirect regular RADIUS traffic to remote RADIUS servers connected over TLS. The TLS connection provides encryption, authentication, and data integrity for the exchange of RADIUS messages.

TLS relies on certificates and private-public key exchange pairs to secure the transmission of data between the RADSEC client and server. The RADSEC destination uses local certificates that are dynamically acquired from the Junos PKI infrastructure.

To enable RADSEC, you must specify the name of the local certificate. If a certificate is not available, or if the certificate was revoked, the RADSEC destination attempts to retrieve it every 300 seconds.

Default RADSEC is not enabled by default.

Options

source-address *ip-address*—Source IP address of the dynamic request.

id-reuse-timeout *seconds*—Response timeout after which the RADIUS ID field value can be reused.

Default: 120 seconds

port *port-number*—(Optional) Port number of the RADSEC server.

Default: 2083

source-port *port-number*—(Optional) Source port to include in RADIUS messages.

tls-certificate—Provide the name of the local certificate.

tls-force-ciphers [low | medium]—(Optional) Allow lower-grade ciphers than the default.

tls-min-version [v1.1 | v1.2]—(Optional) Configure TLS version to limit the lowest supported versions of TLS that are enabled for SSL connections.

Default: v1.2

tls-peer-name *name*—Certified name of the RADSEC server.

tls-timeout *seconds*—Timeout for TLS negotiation.

Default: 5 seconds

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

Related Documentation
- RADIUS over TLS (RADSEC) on page 203

radsec-destination

Syntax

```
radsec-destination id-number;
```

Hierarchy Level

```
[edit access radius-server server-address],
[edit access profile profile-name radius-server server-address]
```

Release Information
Statement introduced in Junos OS Release 19.1R1 for EX Series switches.

Description
Configure a RADIUS over TLS (RADSEC) server as the destination for RADIUS traffic. The RADIUS traffic is redirected from the RADIUS server to the RADSEC destination. You can redirect more than one RADIUS server to the same RADSEC destination.

Options
id-number—The unique ID number for the RADSEC destination.

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

Related Documentation
- RADIUS over TLS (RADSEC) on page 203

rapid-commit

Syntax

```
rapid-commit;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
  family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6
  dhcpv6-client]
```

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.
The **logical-systems** and **tenants** options are introduced in Junos OS Release 18.4R1.

Description

Used to signal the use of the two-message exchange for address assignment.

Required Privilege Level

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

Related Documentation

- DHCPv6 Client Overview on page 787
- Understanding DHCPv6 Client and Server Identification on page 793

rapid-commit (DHCPv6 Local Server)

Syntax

```
rapid-commit;
```

Hierarchy Level

```
[edit system services dhcp-local-server dhcpv6 overrides],
[edit system services dhcp-local-server dhcpv6 group group-name overrides],
[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name
  overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
  services dhcp-local-server dhcpv6 ...],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 ...],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
  ...]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure DHCPv6 local server to recognize the Rapid Commit option (DHCPv6 option 14) in DHCPv6 solicit messages sent from the DHCPv6 client. When rapid commit is enabled for both DHCPv6 local server and the DHCPv6 client, a two-message handshake is used instead of the standard four-message handshake. You can enable rapid commit support on DHCPv6 local server globally, for a named group, or for a specific interface.

Default

Rapid commit support is not enabled.

Required Privilege Level

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

Related Documentation

- Configuring DHCPv6 Rapid Commit (MX, EX) on page 615
- Overriding the Default DHCP Local Server Configuration Settings Overview on page 630

rate-limit

Syntax

rate-limit *limit*;

Hierarchy Level

[edit system services finger],
[edit system services ftp],
[edit system services netconf ssh],
[edit system services ssh],
[edit system services telnet],
[edit system services tftp-server],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure the maximum number of connections attempts per minute, per protocol (either IPv6 or IPv4) on an access service. For example, a rate limit of 10 allows 10 IPv6 telnet session connection attempts per minute and 10 IPv4 telnet session connection attempts per minute.

Default

150 connections

Options

rate-limit *limit*—(Optional) Maximum number of connection attempts allowed per minute, per IP protocol (either IPv4 or IPv6).

Range: 1 through 250

Default: 150

Required Privilege Level

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

Related Documentation

- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*

reauthentication

Syntax reauthentication *interval*;

Hierarchy Level [edit protocols dot1x authenticator interface (all | [*interface-names*])]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description The **reauthentication** statement is used to locally configure the number of seconds before the 802.1X authentication session times out and the client must reattempt authentication.

NOTE: If the authentication server sends an authentication session timeout to the client, this takes priority over the value configured locally using the **reauthentication** statement. The session timeout value is sent from the server to the client as an attribute of the RADIUS Access-Accept message.

Options *interval*—Sets the periodic reauthentication time interval in seconds.
Range: 1 through 4,294,967,296 seconds
Default: 3600 seconds

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

Related Documentation
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292

reconfigure (DHCP Local Server)

Syntax

```
reconfigure {
  attempts attempt-count;
  clear-on-abort;
  strict;
  support-option-pd-exclude;
  timeout timeout-value;
  token token-value;
  trigger {
    radius-disconnect;
  }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name*],
[edit logical-systems *logical-system-name* system services dhcp-local-server],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name*],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name*],
[edit routing-instances *routing-instance-name* system services dhcp-local-server],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name*],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server group *group-name*],
[edit system services dhcp-local-server dhcpv6 group *group-name*]

Release Information

Statement introduced in Junos OS Release 10.0.
Support at the **[edit ... dhcpv6 ...]** hierarchy levels introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
support-option-pd-exclude statement introduced in Junos OS Release 17.3 for the MX Series.

Description

Enable dynamic reconfiguration triggered by the DHCP local server of all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. A group configuration takes precedence over a DHCP local server configuration. The **strict** statement is available only for DHCPv6.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Options **support-option-pd-exclude**—Request to exclude prefix option in the reconfigure message.

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

Related Documentation

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview on page 662
- *DHCPv6 Prefix Exclusion*
- *dhcp-attributes*
- reconfigure on page 1400

reconfigure (System Services DHCP)

Syntax

```
reconfigure {
  attempts number;
  clear-on-abort;
  strict;
  timeout number;
  token token-name;
  trigger {
    radius-disconnect;
  }
}
```

Hierarchy Level

```
[edit system services dhcp-local-server dhcpv6]
[edit system services dhcp-local-server group group-name]
[edit system services dhcp-local-server dhcpv6 group group-name]
```

Release Information Statement introduced in Junos OS Release 10.4.

Description Enable dynamic reconfiguration triggered by the DHCP local server of all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. A group configuration takes precedence over a DHCP local server configuration.

Options

attempts *number*—Configure maximum number of attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces before reconfiguration is considered to have failed. A group configuration takes precedence over a DHCP local server configuration.

Range: 1 through 10 attempts

Default: 8 attempts

clear-on-abort —Delete all DHCP clients or only the DHCP clients serviced by the specified group of interfaces when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success. A group configuration takes precedence over a DHCP local server configuration.

strict —Configure the system to only allow packets that contain the reconfigure accept option.

timeout *seconds*—Configure the initial value in seconds between attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. Each successive attempts doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.

Range: 1 through 10 seconds

Default: 2 seconds

token *token-name*—Configure a plain-text token for all DHCP clients or only the clients specified by the specified group of interfaces. The default is null (empty string).

trigger — Specify DHCP reconfigure trigger.

Required Privilege Level

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*
- DHCP Server Configuration Overview on page 719

req-option

Syntax

```
req-option (dns-server | domain | fqdn | nis-domain | nis-server | ntp-server | sip-domain |
  sip-server | time-zone | vendor-spec);
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
  family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6
  dhcpv6-client]
```

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.
The **logical-systems** and **tenants** options are introduced in Junos OS Release 18.4R1.

Description

The configuration options requested by the DHCPv6 client.

Options

dns-server—Specify a DNS server.

domain—Specify a domain name.

fqdn—Specify a fully qualified domain name.

nis-domain—Specify a Network Information Service (NIS) domain.

nis-server—Specify a Network Information Service (NIS) server.

ntp-server—Specify a Network Time Protocol (NTP) server.

sip-domain—Specify a Session Initiation Protocol (SIP) domain.

sip-server—Specify a Session Initiation Protocol (SIP) server.

time-zone—Specify a time zone.

vendor-spec—Specify vendor specification.

Required Privilege Level

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

regex-additive-logic

Syntax

```
regex-additive-logic;
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced in Junos OS Release 16.1.

Description

Enable additive logic (that is, deny all by default / allow some as specified) to be used in regular expressions.

This statement changes the behavior of existing regular expressions so that all configuration hierarchies are denied by default and must be explicitly allowed using the **allow-configuration-regexps** statement.

For example, to grant users in a named user class access to a specific configuration hierarchy, but deny access to all other configuration hierarchies, enable the **regex-additive-logic** statement and configure an **allow-configuration-regexps** statement that includes the specific configuration hierarchy to which you want to allow access. When a user logs in, only the specified configuration hierarchy is visible.

Default

By default, this statement is disabled; configuration hierarchies not explicitly denied with a **deny-configuration-regexps** statement are visible to the user.

Required Privilege Level

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

Related Documentation

- Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies on page 125
- Example: Using Additive Logic With Regular Expressions to Specify Access Privileges on page 110
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 99
- **allow-configuration-regexps on page 869**
- **deny-configuration-regexps on page 973**
- **user on page 1597**

redirect-url

Syntax redirect-url *url*;

Hierarchy Level [edit protocols dot1x authenticator interface *interface-name*]

Release Information Statement introduced in Junos OS Release 15.1R3 for EX Series switches.

Description Configure a URL that redirects unauthenticated hosts to a central Web authentication (CWA) server. The CWA server provides a web portal where the user can enter a username and password. If these credentials are validated by the CWA server, the user is authenticated and is allowed access to the network.

The redirect URL for central Web authentication can be configured centrally on the AAA server or locally on the switch. Use the **redirect-url** statement to configure the redirect URL locally on the interface connecting the host to the switch.

The redirect URL and a dynamic firewall filter must both be present for the central Web authentication process to be triggered. For more information about configuring the redirect URL and the dynamic firewall filter for central Web authentication, see "Configuring Central Web Authentication" on page 396.

Default Disabled. The redirect URL is not enabled for central Web authentication by default.

Options *url*—The URL that redirects the host to the server that will handle central web authentication. The redirect URL must use the HTTP or HTTPS protocol and include an IP address or website name. The following are examples of valid redirect URL formats:

- http://www.example.com
- https://www.example.com
- http://10.10.10.10
- https://10.10.10.10
- http://www.example.com/login.html
- https://www.example.com/login.html
- http://10.10.10.10/login.html
- https://10.10.10.10/login.html

NOTE: When the dynamic firewall filter is configured using the special Filter-ID attribute JNPR_RSVD_FILTER_CWA, the CWA redirect URL must include the IP address of the AAA server, for example, https://10.10.10.10.

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

Related Documentation
- Configuring Central Web Authentication on page 396

relay-agent-interface-id (DHCP Local Server)

Syntax
```
relay-agent-interface-id;
```

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

Release Information
Statement introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Specify that the DHCPv6 Relay Agent Interface-ID option (option 18) in the client PDU name is concatenated with the username during the subscriber authentication or DHCP client authentication process.

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

Related Documentation
- Creating Unique Usernames for DHCP Clients on page 653

relay-agent-interface-id (DHCPv6 Relay Agent)

Syntax

```
relay-agent-interface-id {
  include-irb-and-l2;
  keep-incoming-interface-id ;
  no-vlan-interface-name;
  prefix prefix;
  use-interface-description (logical | device);
  use-option-82 <strict>;
  use-vlan-id;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dual-stack-group
  dual-stack-group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay
  dual-stack-group ],
```

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.
Support at the **[edit ... dual-stack-group *dual-stack-group-name*]** hierarchy level introduced in Junos OS Release 15.1.

Description

Insert the DHCPv6 Relay Agent Interface-ID option (option 18) in DHCPv6 packets destined for the DHCPv6 server.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- dhcp-relay on page 997
- Extended DHCP Relay Agent Overview on page 618
- DHCPv6 Relay Agent Overview on page 648
- Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets on page 649

relay-agent-remote-id (DHCP Local Server)

Syntax

```
relay-agent-remote-id;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
For MX Series routers only, **enterprise-id** and **remote-id** options introduced in Junos OS Release 12.3R3.
For MX Series routers only, the **enterprise-id** and **remote-id** options are obsoleted starting in Junos OS Releases 12.3R7, 13.2R4, 13.3R2, and 14.1R1.

Description

Specify that the DHCPv6 Relay Agent Remote-ID option (option 37) in the client PDU name is concatenated with the username during the subscriber authentication or DHCP client authentication process. In order to generate an ASCII version of the username, the router concatenates only the remote-id portion of option 37 to the username, and ignores the enterprise number.

Required Privilege Level

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

Related Documentation

- Creating Unique Usernames for DHCP Clients on page 653

relay-agent-remote-id (DHCPv6 Relay Agent Username)

Syntax

```
relay-agent-remote-id;
```

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include]

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
For MX Series routers only, **enterprise-id** and **remote-id** options introduced in Junos OS Release 12.3R3.
For MX Series routers only, the **enterprise-id** and **remote-id** options are obsoleted starting in Junos OS Releases 12.3R7, 13.2R4, 13.3R2, and 14.1R1.
Support at the **[edit ... dual-stack-group *dual-stack-group-name*]** hierarchy level introduced in Junos OS Release 15.1.

Description

Specify that the DHCPv6 Relay Agent Remote-ID option (option 37) in the client PDU name is concatenated with the username during the subscriber authentication or client authentication process. In order to generate an ASCII version of the username, the router concatenates only the remote-id portion of option 37 to the username, and ignores the enterprise number.

Required Privilege Level

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

Related Documentation

- DHCPv6 Relay Agent Overview on page 648
- Creating Unique Usernames for DHCP Clients on page 653

relay-option (DHCP Relay Agent)

Syntax

```
relay-option {
  option-number option-number;
  default-action {
    drop;
    forward-only;
    local-server-group local-server-group;
    relay-server-group relay-server-group;
  }
  equals (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    local-server-group local-server-group;
    relay-server-group relay-server-group;
  }
  starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    local-server-group local-server-group;
    relay-server-group relay-server-group;
  }
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Configure the extended DHCP relay agent selective processing that is based on DHCP options in DHCP client packets and specify the action to perform on client traffic. You can configure support globally or for a named group of interfaces, and for either DHCP or DHCPv6 relay agent.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Using DHCP Option Information to Selectively Process DHCP Client Traffic*

relay-option-82

Syntax

```
relay-option-82 {
  circuit-id {
    include-irb-and-l2;
    keep-incoming-circuit-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-vlan-id;
  }
  remote-id {
    include-irb-and-l2;
    keep-incoming-remote-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-vlan-id;
  }
  server-id-override
  vendor-specific{
    host-name;
    location;
  }
}
```

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay group *group-name*],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name*],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name*]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Enable or disable the insertion of the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.

To enable insertion of option 82 information in DHCP packets, you must specify at least one of the **circuit-id** or **remote-id** statements.

You can use the **relay-option-82** statement and its subordinate statements at the **[edit forwarding-options dhcp-relay]** hierarchy level to control insertion of option 82 information

globally, or at the **[edit forwarding-options dhcp-relay** group ***group-name*]** hierarchy level to control insertion of option 82 information for a named group of interfaces.

To restore the default behavior (option 82 information is not inserted into DHCP packets), use the **delete relay-option-82** statement.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

Related Documentation
- Using DHCP Relay Agent Option 82 Information on page 633
- dhcp-relay on page 997

relay-server-group (DHCP Relay Agent Option)

Syntax

```
relay-server-group relay-server-group;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option (default-action | equals | starts-with),
[edit forwarding-options dhcp-relay dhcpv6 relay-option (default-action | equals |
  starts-with),
[edit forwarding-options dhcp-relay group group-name relay-option (default-action | equals
  | starts-with),
[edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option (default-action
  | equals | starts-with),
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information
Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Relay DHCP client packets to the specified group of DHCP servers when you use the DHCP relay selective processing feature. You can configure the relay operation globally or for a group of interfaces, and for either DHCP or DHCPv6 relay agent.

Options
relay-server-group—Name of DHCP server group.

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

Related Documentation
- *Using DHCP Option Information to Selectively Process DHCP Client Traffic*

replace-ip-source-with (Before Forwarding Packet)

Syntax replace-ip-source-with giaddr;

Hierarchy Level [edit forwarding-options dhcp-relay overrides]

Release Information Statement introduced in Junos OS Release 15.1X49-D100.

Description Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr) before forwarding the packet to the DHCP server.

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

Related Documentation

- overrides (New Relay Options) on page 1317

replace-ip-source-with

Syntax

```
replace-ip-source-with giaddr;
```

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* interface *interface-name* overrides]

Release Information

Statement introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618
- Replacing the DHCP Relay Request and Release Packet Source Address on page 621

remote-debug-permission

Syntax

```
remote-debug-permission (qfabric-admin | qfabric-operator | qfabric-user);
```

Hierarchy Level

```
[edit system login user username authentication]
[edit system root-authentication]
```

Release Information

Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

(QFabric systems only) Configure authentication classes that permit or deny user access to individual components of the QFabric system.

Default

qfabric-user

Options

qfabric-admin—Permits a user to log in to individual QFabric system components, view operations, and change component configurations.

qfabric-operator—Permits a user to log in to individual QFabric system components and view component operations.

qfabric-user—Prevents a user from logging in to individual QFabric system components.

Required Privilege Level

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

Related Documentation

- *Example: Configuring QFabric System Login Classes*
- request component login on page 1673
- *Understanding QFabric System Login Classes*

restart (Reset)

Syntax

```
restart
<application-identification |application-security |audit-process |commitd-service
  |chassis-control | class-of-service |database-replication |datapath-trace-service |ddns
  |dhcp |dhcp-service |dynamic-flow-capture |disk-monitoring |event-processing |
  ethernet-connectivity-fault-management |ethernet-link-fault-management
  |extensible-subscriber-services |fipsd |firewall |firewall-authentication-service
  |general-authentication-service |gracefully |gprs-process |idp-policy |immediately
  |interface-control | ipmi |ipsec-key-management |jflow-service |jnu-management
  |jnx-wmicd-service |jsrp-service |kernel-replication |l2-learning |l2cpd-service |lacp
  |license-service |logical-system-service |mib-process |mountd-service |named-service
  |network-security |network-security-trace |nfsd-service |ntpd-service |pgm
  |pic-services-logging |profilerd |pki-service |remote-operations |rest-api |routing |sampling
  |sampling-route-record |scc-chassisd |secure-neighbor-discovery |security-intelligence
  |security-log |services |service-deployment |simple-mail-client-service |soft |snmp
  |static-routed |statistics-service |subscriber-management |subscriber-management-helper
  |system-log-vital |tunnel-oamd |uac-service |user-ad-authentication |vrrp
  |web-management >
```

Release Information Command introduced before Junos OS Release 9.2

Description Restart a Junos OS process.

CAUTION: Never restart a software process unless instructed to do so by a customer support engineer. A restart might cause the router to drop calls and interrupt transmission, resulting in possible loss of data.

Options

- application-identification—(Optional) Restart the process that identifies an application using intrusion detection and prevention (IDP) to allow or deny traffic based on applications running on standard or nonstandard ports.
- application-security—(Optional) Restart the application security process.
- audit-process—(Optional) Restart the RADIUS accounting process that gathers statistical data that can be used for general network monitoring, for analyzing and tracking usage patterns, and for billing a user based upon the amount of time used or the type of services accessed.
- chassis-control—(Optional) Restart the chassis management process.
- class-of-service—(Optional) Restart the class-of-service (CoS) process, which controls the router's or switch's CoS configuration.
- commitd-service—(Optional) Restart the committed services.
- database-replication—(Optional) Restart the database replication process.
- datapath-trace-service—(Optional) Restart the Restart the packet path tracing process.

- ddns—(Optional) Restart the dynamic domain name system, which dynamically updates IP addresses for registered domain names.
- dhcp—(Optional) Restart the software process for a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server allocates network IP addresses and delivers configuration settings to client hosts without user intervention.
- dhcp-service—(Optional) Restart the Dynamic Host Configuration Protocol process.
- disk-monitoring—(Optional) Restart disk monitoring, which checks the health of the hard disk drive on the Routing Engine.
- dynamic-flow-capture—(Optional) Restart the dynamic flow capture (DFC) process, which controls DFC configurations on PIC3 monitoring services cards.
- ethernet-connectivity-fault-management—(Optional) Restart the process that provides IEEE 802.1ag Operation, Administration, and Maintenance (OAM) connectivity fault management (CFM) database information for CFM maintenance association end points (MEPs) in a CFM session.
- ethernet-link-fault-management—(Optional) Restart the process that provides the OAM link fault management (LFM) information for Ethernet interfaces.
- event-processing—(Optional) Restart the event process (eventd).
- extensible-subscriber-services—(Optional) Restart the extensible subscriber services process.
- fipsd—(Optional) Restart the fipsd services.
- firewall—(Optional) Restart the firewall management process, which manages the firewall configuration and accepts or rejects packets that are transiting an interface on a router or switch.
- firewall-authentication-service—(Optional) Restart the firewall authentication service process.
- general-authentication-service—(Optional) Restart the general authentication process.
- gprs-process—(Optional) Restart the General Packet Radio Service (GPRS) process.
- gracefully—(Optional) Restart the software process.
- idp-policy—(Optional) Restart the intrusion detection and prevention (IDP) protocol process.
- immediately—(Optional) Immediately restart the software process.
- interface-control—(Optional) Restart the interface process, which controls the router's or switch's physical interface devices and logical interfaces.
- ipmi—(Optional) Restart the intelligent platform management interface process.
- ipsec-key-management—(Optional) Restart the IPsec key management process.
- jflow-service—(Optional) Restart jflow service process.
- jnu-management—(Optional) Restart jnu management process.
- jnx-wmicd-service—(Optional) Restart jnx wmicd service process.

- jsrp-service—(Optional) Restart the Juniper Services Redundancy Protocol (jsrdp) process, which controls chassis clustering.
- kernel-replication—(Optional) Restart the kernel replication process, which replicates the state of the backup Routing Engine when graceful Routing Engine switchover (GRES) is configured.
- lacp—(Optional) Restart the Link Aggregation Control Protocol (LACP) process. LACP provides a standardized means for exchanging information between partner systems on a link. The LACP process allows link aggregation control instances to reach agreement on the identity of the LAG to which a link belongs, moves the link to that LAG, and enables the transmission and reception processes for the link to function in an orderly manner.
- l2cpd-service—(SRX5400, SRX5600, and SRX5800 devices only) (Optional) Restart the Layer 2 Control Protocol (L2CP) process, which enables features such as L2 protocol tunneling and nonstop bridging.
- l2-learning—(Optional) Restart the Layer 2 (L2) address flooding and learning process.
- license-service—(Optional) Restart the feature license management process.
- logical-system-service—(Optional) Restart the logical system service process.
- mib-process—(Optional) Restart the MIB version II process, which provides the router's MIB II agent.
- mountd-service—(Optional) Restart the service for Network File System (NFS) mount requests.
- named-service—(Optional) Restart the DNS Server process, which is used by a router or a switch to resolve hostnames into addresses.
- network-security—(Optional) Restart the network security process.
- network-security-trace—(Optional) Restart the network security trace process.
- nfsd-service—(Optional) Restart the remote NFS server process, which provides remote file access for applications that need NFS-based transport.
- ntpd-service—(Optional) Restart the Network Time Protocol (NTP) process.
- pgm—(Optional) Restart the process that implements the Pragmatic General Multicast (PGM) protocol for assisting in the reliable delivery of multicast packets.
- pic-services-logging—(Optional) Restart the logging process for some PICs. With this process, also known as fsad (the file system access daemon), PICs send special logging information to the Routing Engine for archiving on the hard disk.
- pki-service—(Optional) Restart the public key infrastructure (PKI) service process.
- profilerd—(Optional) Restart the profiler process.
- remote-operations—(Optional) Restart the remote operations process, which provides the ping and traceroute MIBs.
- rest-api—(Optional) Restart the rest api process.
- routing—(Optional) Restart the routing protocol process (rpd).

- sampling—(Optional) Restart the sampling process, which performs packet sampling based on particular input interfaces and various fields in the packet header.
- sampling-route-record—(Optional) Restart the sampling route record process.
- scc-chassisd—(Optional) Restart the scc chassisd process.
- secure-neighbor-discovery—(Optional) Restart the secure Neighbor Discovery Protocol (NDP) process, which provides support for protecting NDP messages.
- security-intelligence—(Optional) Restart security intelligence process.
- security-log—(Optional) Restart the security log process.
- service-deployment—(Optional) Restart the service deployment process, which enables Junos OS to work with the Session and Resource Control (SRC) software.
- services—(Optional) Restart a service.
- simple-mail-client-service—(Optional) Restart the simple mail client service process.
- snmp—(Optional) Restart the SNMP process, which enables the monitoring of network devices from a central location and provides the router's or switch's SNMP master agent.
- static-routed—(Optional) Restart the static routed process.
- soft—(Optional) Reread and reactivate the configuration without completely restarting the software processes. For example, BGP peers stay up and the routing table stays constant. Omitting this option results in a graceful restart of the software process.
- statistics-service—(Optional) Restart the process that manages the Packet Forwarding Engine statistics.
- subscriber-management—(Optional) Restart the subscriber management process.
- subscriber-management-helper—(Optional) Restart the subscriber management helper process.
- system-log-vital—(Optional) Restart system log vital process.
- tunnel-oamd—(Optional) Restart the tunnel OAM process for L2 tunneled networks.
- uac-service—(Optional) Restart the Unified Access Control (UAC) process.
- user-ad-authentication—(Optional) Restart User ad Authentication process
- vrrp—(Optional) Restart the Virtual Router Redundancy Protocol (VRRP) process, which enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts.
- web-management—(Optional) Restart the Web management process.

Required Privilege Level reset

Related Documentation
- *Restart Commands Overview*

List of Sample Output restart interfaces on page 1421

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

Sample Output

restart interfaces

```
user@host> restart interfaces
interfaces process terminated
interfaces process restarted
```

retransmission-attempt

Syntax
```
retransmission-attempt number;
```

Hierarchy Level
```
[edit interfaces interface-name unit logical-unit-number family inet dhcp]
```

Release Information
Statement introduced in Junos OS Release 8.5 for J Series devices.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.2 for SRX Series devices.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify the number of times the device retransmits a Dynamic Host Control Protocol (DHCP) packet if a DHCP server fails to respond. After the specified number of attempts, no further attempts at reaching a server are made.

Options ***number***—Number of retransmit attempts.
Range: 0 through 6
Default: 4

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

Related Documentation
- Configuring a DHCP Client (CLI Procedure) on page 591
- *interfaces*
- *unit*
- *family*

retransmission-attempt (dhcp-client)

Syntax retransmission-attempts *number*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option **dhcp-clinet** at **[edit interfaces interface-name unit logical-unit-number family inet]** hierarchy is changed to **dhcp** to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option **dhcp**.

Description Specify the number of times the device attempts to retransmit a Dynamic Host Control Protocol (DHCP) packet fallback.

Options **number**—Number of attempts to retransmit the packet.

Range: 0 through 6

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

Related Documentation

- Understanding DHCP Client Operation on page 733
- Minimum DHCP Client Configuration on page 734

retransmission-attempt (dhcpv6-client)

Syntax

```
retransmission-attempt number;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
  family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6
  dhcpv6-client]
```

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.
The **logical-systems** and **tenants** options are introduced in Junos OS Release 18.4R1.

Description

Specify the number of times the device retransmits a DHCPv6 client packet if a DHCPv6 server fails to respond. After the specified number of attempts, no further attempts at reaching a server are made.

Options

number—Number of retransmit attempts

Required Privilege Level

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

Related Documentation

retransmission-interval

Syntax retransmission-interval *seconds*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify the time between successive retransmissions of the client DHCP request if a DHCP server fails to respond.

Options ***seconds***—Number of seconds between successive retransmissions.

Range: 4 through 64 seconds

Default: 4 seconds

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

Related Documentation

- Configuring a DHCP Client (CLI Procedure) on page 591

retransmission-interval (dhcp-client)

Syntax retransmission-interval *seconds*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option **dhcp-clinet** at **[edit interfaces interface-name unit logical-unit-number family inet]** hierarchy is changed to **dhcp** to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option **dhcp**.

Description Specify the initial retransmission interval. Successive retransmission intervals are doubled as per RFC2131.

NOTE: Though the SRX series devices implement the exponential backoff, as described in RFC 2131, the retransmit attempt does not stop when the retransmission interval reaches 64 seconds. The packet is transmitted till the retransmission attempt is reached. For example, if you configure the **retransmission-attempt** to 5 and the **retransmission-interval** to 20, the sequence of retransmission-interval is 20, 40, 80, 160, 320.

Options **seconds**—Number of seconds before initial retransmission.

Range: The range is 4 through 64. The default is 4 seconds.

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

Related Documentation

- Understanding DHCPv6 Client and Server Identification on page 793

retry

Syntax retry *number*;

Hierarchy Level [edit system radius server *server-address*],
[edit system accounting destination radius server *server-address*]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Number of times the router or switch is allowed to try to contact a RADIUS authentication or accounting server.

Options *number*—Number of retries allowed for contacting a RADIUS server.

Range: 1 through 10

Default: 3

NOTE: The **[edit system accounting]** hierarchy is not available on QFabric systems.

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

Related Documentation

- Configuring RADIUS Authentication (QFX Series or OCX Series) on page 192
- *timeout*

retry (RADIUS)

Syntax

```
retry number;
```

Hierarchy Level

```
[edit system radius-server server-address],
[edit system accounting destination radius server server-address]
```

Release Information

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

Description

Number of times the router or switch is allowed to try to contact a RADIUS authentication or accounting server.

Options

number—Number of retries allowed for contacting a RADIUS server.

Range: 1 through 10

Default: 3

Required Privilege Level

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

Related Documentation

- Configuring RADIUS Server Authentication on page 182
- Configuring RADIUS System Accounting on page 200
- timeout on page 1536

retry-options

Syntax

```
retry-options {
  backoff-factor seconds;
  backoff-threshold number;
  maximum-time seconds;
  minimum-time seconds;
  tries-before-disconnect number;
}
```

Hierarchy Level [edit system login]

Release Information

Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
maximum-time option introduced in Junos OS Release 9.6.
maximum-time option introduced in Junos OS Release 9.6 for EX Series switches.

Description Maximum number of times a user can attempt to enter a password while logging in through SSH or Telnet before being disconnected.

Required Privilege Level

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

Related Documentation

- Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 60
- rate-limit on page 1398
- lockout-period on page 1208

retries

Syntax retries *number*;

Hierarchy Level [edit protocols dot1x authenticator interface (802.1X) (all | [*interface-names*])]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description For 802.1X authentication, configure the number of times the switch attempts to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt.

Options *number*—Number of retries.

Default: 3 retries

Range: 1 through 10

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

Related Documentation

- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- *Configuring 802.1X Authentication (J-Web Procedure)*
- Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 315

retries (Captive Portal)

Syntax retries *number-of-tries*;

Hierarchy Level [edit services captive-portal interface (all | *interface-names*)]]

Release Information Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description Configure the number of times the user can attempt to submit authentication information.

Options ***number-of-tries***—Number of authentication attempts by user.
Range: 1–65535
Default: 3

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

Related Documentation
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

revert-interval (Access)

Syntax

```
revert-interval interval;
```

Hierarchy Level

```
[edit access profile profile-name 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

interval—Amount of time to wait.

Range: 0 through 604,800 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

- *RADIUS Servers and Parameters for Subscriber Access*
- *Configuring Authentication and Accounting Parameters for Subscriber Access*

rising-threshold (Health Monitor)

Syntax rising-threshold *percentage*;

Hierarchy Level [edit snmp health-monitor]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Set the upper threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored object, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options ***percentage***—Upper threshold for the alarm entry.

Range: 1 through 100

Default: 80 percent of the maximum possible value

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

Related Documentation

- *Configuring Health Monitoring*
- falling-threshold on page 1097

root-authentication

Syntax

```
root-authentication {
  encrypted-password password;
  load-key-file URL;
  plain-text-password;
  ssh-dsa public-key {
  <from pattern-list>;
  }
  ssh-rsa public-key {
  <from pattern-list>;
  }
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify authentication information for the root login.

Options

- **encrypted-password *password***—Specify the encrypted authentication password. You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.
- **plain-text-password**—The CLI prompts you for a password encrypts it, and stores the encrypted version in its user database.
- **load-key-file*URL***—File URL containing one or more SSH keys.
- **ssh-dsa *public-key***—SSH DSA public key string.
  - **from *pattern-list***—Pattern list of allowed hosts.
- **ssh-rsa *public-key***—SSH RSA public key string.
  - **from *pattern-list***—Pattern list of allowed hosts.

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

root-authentication

Syntax

```
root-authentication {
  (encrypted-password "password";
  no-public-keys
  ssh-ecdsa name {
    from from;
  }
  ssh-ed25519 name {
    from from;
  }
  ssh-rsa name {
    from from;
  }
}
```

Hierarchy Level

```
[edit system]
```

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 authentication methods for the root-level user, whose username is **root**.

You can use the **ssh-ecdsa**, **ssh-ed25519**, or **ssh-rsa** statements to directly configure SSH ECDSA, ED25519, or RSA keys to authenticate root logins. You can configure more than one public key for SSH authentication of root logins as well as for user accounts. When a user logs in as root, the public keys are referenced to determine whether the private key matches any of them.

Options

encrypted-password "*password*"—Specify the MD5 or other password. You can specify only one encrypted password. You cannot configure a blank password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

no-public-keys—Disable SSH public key-based authentication.

ssh-ecdsa *name* from *from*—Use an SSH ECDSA public key. You can specify one or more public keys.

ssh-ed25519 *name* from *from*—Use an SSH ED25519 public key. You can specify one or more public keys.

ssh-rsa *name* from *from*—Use an SSH RSA public key. You can specify one or more public keys.

Required Privilege Level

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

Related Documentation

- Junos OS User Accounts Overview on page 67
- *Protecting Network Security by Configuring the Root Password*
- Recovering the Root Password on page 144
- **authentication on page 883**

root-login

Syntax

```
root-login (allow | deny | deny-password);
```

Hierarchy Level

```
[edit system services ssh]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Control user access through SSH.

Default

root-login deny-password is the default for most systems.

Starting in Junos release 17.4R1 for MX Series routers, the default for root-login is **deny**. In previous Junos releases, the default setting for the MX240, MX480, MX960, MX2010 and MX2020 was **allow.**

Options

allow—Allow users to log in to the router or switch as root through SSH.

deny—Disable users from logging in to the router or switch as root through SSH.

deny-password—Allow users to log in to the router or switch as root through SSH when the authentication method (for example, RSA authentication) does not require a password.

Required Privilege Level

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

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 232

route-suppression (DHCP Local Server and Relay Agent)

Syntax

```
route-suppression (access | access-internal | destination);
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit logical-systems logical-system-name ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name...],
[edit routing-instances routing-instance-name ...],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name]
```

Release Information Statement introduced in Junos OS Release 13.2.

Description Configure the jdhcpd process to suppress the installation of access, access-internal, or destination routes during client binding.

NOTE: You cannot suppress access-internal routes when the subscriber is configured with both IA_NA and IA_PD addresses over IP demux interfaces—the IA_PD route relies on the IA_NA route for next hop connectivity.

Options

access—(DHCPv6 only) Suppress installation of access routes. You can use the **access** and **access-internal** options in the same statement for DHCPv6.

access-internal—In a DHCPv4 hierarchy, suppress installation of both access-internal and destination routes. In a DHCPv6 hierarchy, suppress access-internal routes only. Can be configured in the same statement with the **access** option.

destination—(DHCPv4 only) Suppress installation of destination routes. This option and the **access-internal** option are mutually exclusive; however, the **access-internal** option also suppresses destination routes.

Required Privilege Level

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

Related Documentation

- Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default on page 705

routing-engine-profile

Syntax

```
routing-engine-profile profile-name {
  fields {
    field-name;
  }
  file filename;
  interval minutes;
}
```

Hierarchy Level

```
[edit accounting-options]
```

Release Information

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

Description

Create a Routing Engine profile to collect selected Routing Engine statistics and write them to a file in the **/var/log** directory.

Options

profile-name—Name of the Routing Engine statistics profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring the Routing Engine Profile*

routing-instance

Syntax

```
routing-instance {
  instance-name {
    bridge-domain bridge-domain-name;
  }
  vlan (vlan-id | vlan-name);
}
```

Hierarchy Level

[edit forwarding-options ananlyzer *analyzer-name* input egress],
[edit forwarding-options ananlyzer *analyzer-name* input ingress],
[edit forwarding-options ananlyzer *analyzer-name* output]

Release Information

Statement introduced in Junos OS Release 14.1.

Description

Configure routing instance.

Options

instance-name—Name of the routing instance.

Required Privilege Level

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

Related Documentation

routing-instance-name (DHCP Local Server)

Syntax

```
routing-instance-name;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the routing instance name be concatenated with the username during the subscriber authentication or DHCP client authentication process. No routing instance name is concatenated if the configuration is in the default routing instance.

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651

routing-instance-name (DHCP Relay Agent)

Syntax

```
routing-instance-name;
```

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name* authentication username-include],
[edit forwarding-options dhcp-relay group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* authentication username-include],
[edit tenants *tenant-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include]
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* authentication username-include]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Support at the **[edit ... dual-stack-group *dual-stack-group-name*]** hierarchy level introduced in Junos OS Release 15.1.
The **tenants** option is introduced in Junos OS Release 18.4R1.

Description

Specify that the routing instance name is concatenated with the username during the subscriber authentication or client authentication process. No routing instance name is concatenated if the configuration is in the default routing instance. Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

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

Related Documentation
- Using External AAA Authentication Services with DHCP on page 651
- Creating Unique Usernames for DHCP Clients on page 653

scp

Syntax
```
scp (recursive | source-path | destination-path | source-address | routing-instance);
```

Release Information
Statement introduced in Junos OS Release 15.1X49-D110 for SRX300, SRX320, SRX340, and SRX345 devices.
Statement introduced in Junos OS Release 18.4R1 for MX240, MX480, MX960, MX2010, MX2020, and vMX routers.
Options **source-address** and **routing-instance** added in Junos OS Release 18.4R1.

Description
Initiates a secure copy (**scp**) connection from the Junos CLI shell.

Options
- recursive—Copy files recursively.
- source-path— (Mandatory) Specify the source file location.
- destination-path—(Mandatory) Specify the destination file location.
- source-address—(Optional) Specify the local address to use in originating the secure copy connection.
- routing-instance—(Optional) Specify the name of the routing instance for the secure copy session. Default is inet.0.

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

Related Documentation
- The ssh Command on page 236

security

Syntax

```
security {
  authentication-key-chains {
    key-chain key-chain-name {
      key key {
        secret secret-data;
        start-time yyyy-mm-dd.hh:mm:ss;
      }
    }
  certificates {
    cache-size bytes;
    cache-timeout-negative seconds;
    certification-authority ca-profile-name {
      ca-name ca-identity;
      crl file-name;
      encoding (binary | pem);
      enrollment-url url-name;
      file certificate-filename;
      ldap-url url-name;
    }
    enrollment-retry attempts;
    local certificate-filename {
      certificate-key-string;
      load-key-file key-file-name;
    }
    maximum-certificates number;
    path-length certificate-path-length;
  }
  ssh-known-hosts {
    host {
      fetch-from-server host-name;
      load-key-file file-name;
    }
  }
  traceoptions {
    file filename <files number> <size size>;
    flag flag;
    level level;
    no-remote-trace
  }
}
```

Hierarchy Level

```
[edit]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure security services. Most of the configuration statements do not have default values. If you do not specify an identifier for a statement that does not have a default value, you cannot commit the configuration.

Required Privilege Level

Related Documentation

secret

Syntax

```
secret password;
```

Hierarchy Level

```
[edit system accounting destination radius server server-address],
[edit system accounting destination tacplus server server-address],
[edit system radius-server server-address],
[edit system tacplus-server server-address]
```

Release Information

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

Description

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

NOTE: To ensure better security, we recommend you to configure TACACS+ secret password with a minimum of 14 characters.

Options

password—Password to use; can include spaces included in quotation marks.

Required Privilege Level

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

Related Documentation

- Configuring RADIUS Server Authentication on page 182
- Configuring TACACS+ Authentication on page 207
- Configuring TACACS+ System Accounting on page 219
- Configuring RADIUS System Accounting on page 200

secret

Syntax

```
secret password;
```

Hierarchy Level

```
[edit access profile profile-name radius-server server-address],
[edit access radius-disconnect client-address],
[edit access radius-server server-address]
```

Release Information

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

Description

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

Options

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

Required Privilege Level

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

Related Documentation

- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *RADIUS Authentication and Accounting Server Definition*
- *Example: Configuring CHAP Authentication with RADIUS*
- *Configuring RADIUS Authentication for L2TP*
- *Configuring the RADIUS Disconnect Server for L2TP*

secret

Syntax secret *secret-data*;

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

Release Information
Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify a password in encrypted text or plain text format. The secret password always appears in encrypted format.

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

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

Related Documentation

- Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols on page 226
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

secure-authentication

Syntax secure-authentication (http | https);

Hierarchy Level [edit services captive-portal]

Release Information Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description Enable HTTP or HTTPS access on the captive portal interface.

Default http

Options **http**—Enables HTTP access on the captive portal interface.

https—Enables HTTPS access on the captive portal interface. HTTPS is recommended.

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

Related Documentation

- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

send-acct-status-on-config-change (Access Profile)

Syntax

```
send-acct-status-on-config-change;
```

Hierarchy Level

[edit access profile *profile-name* accounting]

Release Information

Statement introduced in Junos OS Release 13.1.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure the router's authd process to send accounting messages when the RADIUS server status changes for an access profile. When you include this statement, authd sends an Acct-On message when the first RADIUS server is added to an access profile, and to send an Acct-Off message when the last RADIUS server is removed from an access profile.

Required Privilege Level

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

Related Documentation

- *Configuring Per-Subscriber Session Accounting*
- *RADIUS Servers and Parameters for Subscriber Access*

send-release-on-delete (DHCP Relay Agent)

Syntax

```
send-release-on-delete;
```

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name* overrides],
[edit forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 group *group-name* overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* interface *interface-name* overrides]

Release Information

Statement introduced in Junos OS Release 10.2.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Send a release message to the DHCP (or DHCPv6) server whenever DHCP relay or relay proxy deletes a client. Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

M120 and M320 routers do not support DHCPv6.

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618
- Overriding the Default DHCP Relay Configuration Settings on page 627
- Sending Release Messages When Clients Are Deleted on page 659

server (NTP)

Syntax server *address* <key *key-number*> <version *value*> <prefer>;

Hierarchy Level [edit system *ntp*]

Release Information Statement introduced before Junos OS Release 7.4.

Description For NTP, configure the SRX Series device to operate in client mode with the remote system at the specified address. In this mode, the SRX Series device can be synchronized with the remote system, but the remote system can never be synchronized with the SRX Series device.

If the NTP client time drifts so that the difference in time from the NTP server exceeds 128 milliseconds, the client is automatically stepped back into synchronization. If the offset between the NTP client and server exceeds the 1000-second threshold, the client still synchronizes with the server, but it also generates a system log message noting that the threshold was exceeded.

Options ***address***—Address of the remote system. You must specify an address, not a hostname.

key *key-number*—(Optional) Use the specified key number to encrypt authentication fields in all packets sent to the specified address.

Range: Any unsigned 32-bit integer

prefer—(Optional) Mark the remote system as the preferred host, which means that if all other things are equal, this remote system is chosen for synchronization among a set of correctly operating systems.

version *value*—(Optional) Specify the version number to be used in outgoing NTP packets.

Range: 1 through 4

Default: 4

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

Related Documentation

- *ntp*

server (DNS, Port, and TFTP Service)

Syntax

```
server address <logical-system logical-system-name> <routing-instance
  routing-instance-name>;
```

Hierarchy Level

```
[edit forwarding-options helpers domain],
[edit forwarding-options helpers domain interface interface-name],
[edit forwarding-options helpers port port-number],
[edit forwarding-options helpers port port-number interface interface-name],
[edit forwarding-options helpers tftp],
[edit forwarding-options helpers tftp interface interface-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced for port helpers in Junos OS Release 17.2R1 for EX4300 switches.
Support for multiple server instances for a given port introduced in Junos OS Release 17.2 for MX Series routers.
Support for multiple server instances for a given port introduced in Junos OS Release 17.3R1 for EX9200 switches.

Description

Specify the DNS or TFTP server for forwarding DNS or TFTP requests, or specify a destination server address for forwarding LAN broadcast packets as unicast traffic for a custom-configured UDP port.

When configuring port helpers, in releases prior to Junos OS Release 17.2, only one server can be specified for a given port. For Junos OS Release 17.2 and later, multiple servers can be specified for a given port at the global or interface-specific level. When multiple servers are specified, the same packet, with the originator IP address and port requests, is forwarded to the different configured servers; the payload of the UDP packet is not modified.

Options

address—IP address of the server.

logical-system *logical-system-name*—(Optional) Logical system name of the server.

routing-instance [*routing-instance-names*]—(Optional) Set the routing instance name or names that belong to the DNS server or TFTP server.

Required Privilege Level

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

Related Documentation

- *Configuring DNS and TFTP Packet Forwarding*
- *Configuring Port-based LAN Broadcast Packet Forwarding*

server (RADIUS Accounting)

Syntax

```
server {
  server-address {
    accounting-port port-number;
    retry number;
    routing-instance routing-instance;
    secret password;
    source-address address;
    timeout seconds;
  }
}
```

Hierarchy Level

```
[edit system accounting destination radius]
```

Release Information

Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **source-address-inet6** statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description

Configure RADIUS logging.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring RADIUS System Accounting on page 200

server (TACACS+ Accounting)

Syntax

```
server {
  server-address {
    port port-number;
    routing-instance (Accounting and Authentication) routing-instance;
    secret password;
    single-connection;
    timeout seconds;
  }
}
```

Hierarchy Level

```
[edit system accounting destination tacplus]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
routing-instance option introduced in Junos OS Release 17.4R1.

Description

Configure TACACS+ logging.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring TACACS+ System Accounting on page 219

server-address

Syntax server-address *ip-address*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

Release Information Statement introduced in Junos OS Release 8.5 for J Series devices.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.2 for SRX Series devices.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify the address of the DHCP server that the client should accept DHCP offers from. If this option is included in the DHCP configuration, the client accepts offers only from this server and ignores all other offers.

Default The client accepts the first offer it receives from any DHCP server.

Options ***ip-address***—DHCP server address.

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

Related Documentation

- Configuring a DHCP Client (CLI Procedure) on page 591
- *interfaces*
- *unit*
- *family*

server-address (dhcp-client)

Syntax server address *ip-address*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option **dhcp-clinet** at **[edit interfaces interface-name unit logical-unit-number family inet]** hierarchy is changed to **dhcp** to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option **dhcp**.

Description Specify the preferred DHCP server address that is sent to DHCP clients.

Options **ip-address**—DHCP server address.

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

Related Documentation

server-fail

Syntax server-fail (deny | permit | use-cache | *vlan-id* | *vlan-name*);

Hierarchy Level [edit protocols dot1x authenticator interface (all | [*interface-names*])]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description Configure authentication fallback options to specify how end devices connected to a switch are supported if the RADIUS authentication server becomes unavailable. Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by a supplicant's initial attempt at authentication through the RADIUS server.

When you configure the server fail fallback feature you must specify an action that the switch applies to end devices when the authentication servers are unavailable. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN. The VLAN must already be configured on the switch.

NOTE: The server-fail statement is specifically for data traffic. For VoIP tagged traffic, use the server-fail-voip statement. The same interface can have a server-fail VLAN and a server-fail-voip VLAN configured.

Default If the **server-fail** statement is not configured, in the event that the RADIUS authentication server becomes unavailable, the end device is not authenticated and is denied access to the network.

Options **deny**—Force fail the supplicant authentication. No traffic will flow through the interface.

permit—Force succeed the supplicant authentication. Traffic will flow through the interface as if it were successfully authenticated by the RADIUS server.

use-cache—Force succeed the supplicant authentication only if it was previously authenticated successfully. This action ensures that already authenticated supplicants are not affected.

vlan-id—Move supplicant on the interface to the VLAN specified by this numeric identifier. This action is allowed only if it is the first supplicant connecting to the interface. If an authenticated supplicant is already connected, then the supplicant is not moved

to the VLAN and is not authenticated. The VLAN must already be configured on the switch.

vlan-name—Move supplicant on the interface to the VLAN specified by this name. This action is allowed only if it is the first supplicant connecting to an interface. If an authenticated supplicant is already connected, then the supplicant is not moved to the VLAN and is not authenticated. The VLAN must already be configured on the switch.

Required Privilege Level

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

Related Documentation

- show dot1x on page 1799
- Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 309
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Configuring RADIUS Server Fail Fallback (CLI Procedure) on page 287
- Understanding Server Fail Fallback and Authentication on Switches on page 286

server-fail-voip

Syntax server-fail (deny | permit | use-cache | vlan-name);

Hierarchy Level [edit protocols dot1x authenticator interface (all | [*interface-names*])]

Release Information Statement introduced in Junos OS Releases 14.1X53-D40 and 15.1R4 for EX Series switches.

Description Configure authentication fallback options to specify how VoIP clients sending voice traffic are supported if the RADIUS authentication server becomes unavailable. Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by a supplicant's initial attempt at authentication through the RADIUS server.

When you configure the server fail fallback feature you must specify an action that the switch applies to end devices when the authentication servers are unavailable. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN. The VLAN must already be configured on the switch.

The **server-fail-voip** statement is specific to the VoIP-tagged traffic sent by clients. VoIP clients still require that the **server-fail** statement be configured for the un-tagged traffic that they generate. Therefore, when you configure the **server-fail-voip** statement you must also configure the **server-fail** statement.

NOTE: **An option other than server-fail deny must be configured for server-fail-voip to successfully commit.**

Default If the **server-fail-voip** statement is not configured, in the event that the RADIUS authentication server becomes unavailable, a VoIP client that begins authentication by sending voice traffic is not authenticated, and the voice traffic is dropped.

Options **deny**—Force fail the supplicant authentication. No traffic will flow through the interface.

permit—Force succeed the supplicant authentication. Traffic will flow through the interface as if it were successfully authenticated by the RADIUS server.

use-cache—Force succeed the supplicant authentication only if it was previously authenticated successfully. This action ensures that already authenticated supplicants are not affected. This option can be used only for reauthentication.

vlan-name—Move supplicant on the interface to the VLAN specified by this name. This action is allowed only if it is the first supplicant connecting to an interface. If an authenticated supplicant is already connected, then the supplicant is not moved to the VLAN and is not authenticated. The VLAN must already be configured on the switch.

Required Privilege Level

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

Related Documentation

- show dot1x on page 1799
- Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 309
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Configuring RADIUS Server Fail Fallback (CLI Procedure) on page 287
- Understanding Server Fail Fallback and Authentication on Switches on page 286

server-group

Syntax

```
server-group {
  server-group-name {
    server-ip-address;
  }
}
```

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6]

Release Information

Statement introduced in Junos OS Release 8.3.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Specify the name of a group of DHCP server addresses for use by the extended DHCP relay agent. Apply the group with the active-server-group statement globally for all interfaces or for a named group of interfaces configured with the group statement. This mechanism enables you to apply different DHCP relay configurations for different groups of servers, with a common configuration for the servers within a server group.

Options

server-group-name—Name of the group of DHCP or DHCPv6 server addresses.

server-ip-address—IP address of the DHCP server belonging to this named server group. Use IPv6 addresses when configuring DHCPv6 support. Starting in Junos OS Release 18.4R1, you can configure up to 32 server IP addresses per group for DHCPv4 servers. In earlier releases, you can configure only up to 5 server IP addresses for DHCPv4 servers. For DHCPv6 servers, you can configure only up to 32 addresses in all releases. The configuration fails commit check if you configure more than the maximum number of server addresses.

Required Privilege Level

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

Related Documentation

- Extended DHCP Relay Agent Overview on page 618
- Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups on page 667

server-identifier

Syntax server-identifier *address*;

Hierarchy Level [edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

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 server identifier. The identifier can be used to identify a DHCP server in a DHCP message. It can also be used as a destination address from clients to servers (for example, when the boot file is set, but not the boot server).

Servers include the server identifier in **DHCPOFFER** messages so that clients can distinguish between multiple lease offers. Clients include the server identifier in **DHCPREQUEST** messages to select a lease and indicate which offer is accepted from multiple lease offers. Also, clients can use the server identifier to send unicast request messages to specific DHCP servers to renew a current lease.

This address must be a manually assigned, static IP address. The server cannot send a request and receive an IP address from itself or another DHCP server.

Default If no server identifier is set, the DHCP server sets the server identifier based on the primary interface address used by the server to receive a client request. For example, if the client sends a DHCP request and the server receives it on **fe-0/0/0** and the primary interface address is **1.1.1.1**, then the server identifier is set to **1.1.1.1**.

Options ***address***—IPv4 address of the server. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).

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

Related Documentation

server-reject-vlan

Syntax

```
server-reject-vlan (vlan-id | vlan-name) {
  eapol-block;
   block-interval block-interval;
}
```

Hierarchy Level

[edit protocols dot1x authenticator interface (802.1X) (all | [*interface-names*])]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.

Description

For EX Series switches configured for 802.1X authentication, specify that when the switch receives an Extensible Authentication Protocol Over LAN (EAPoL) Access-Reject message during the authentication process between the switch and the RADIUS authentication server, supplicants attempting access to the LAN are granted access and moved to a specific VLAN. Any VLAN name or VLAN ID sent by a RADIUS server as part of the EAPoL Access-Reject message is ignored.

When you specify the VLAN ID or VLAN name, the VLAN must already be configured on the switch.

The remaining statements are explained separately. See CLI Explorer.

Default

None

Options

vlan-id—Numeric identifier of the VLAN to which the supplicant is moved.

vlan-name—Name of the VLAN to which the supplicant is moved.

Required Privilege Level

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

Related Documentation

- show dot1x on page 1799
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 315
- Configuring RADIUS Server Fail Fallback (CLI Procedure) on page 287
- Understanding Server Fail Fallback and Authentication on Switches on page 286

server-timeout

Syntax server-timeout *seconds*;

Hierarchy Level [edit protocols dot1x authenticator interface (802.1X) (all | [*interface-name*])

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description For 802.1X authentication, configure the amount of time a port will wait for a reply when relaying a response from the supplicant to the authentication server before timing out and invoking the server-fail action.

Default 30 seconds

Options ***seconds*** —Number of seconds.
Range: 1 through 60 seconds
Default: 30 seconds

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

Related Documentation

- show dot1x on page 1799
- clear dot1x on page 1659
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302
- 802.1X for Switches Overview on page 289

server-timeout (Captive Portal)

Syntax server-timeout *seconds*;

Hierarchy Level [edit services captive-portal interface (all | *interface-names*)]]

Release Information Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description Configure the time in seconds an interface will wait for a reply when relaying a response from the client to the authentication server before timing out and invoking the server-fail action.

Options ***seconds***—Number of seconds.
Range: 1–65535
Default: 20

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

Related Documentation
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

servers

Syntax

```
servers server-address {
  port port-number;
}
```

Hierarchy Level

[edit system services service-deployment]

Release Information

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

Description

Configure an IPv4 address for the Session and Resource Control (SRC) server.

Options

server-address—The TCP port number.

Default: 3333

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Configuring the Junos OS to Work with SRC Software*

service (Service Accounting)

Syntax

```
service {
  accounting-order (activation-protocol | local | radius);
  accounting {
    statistics (time | volume-time);
    update-interval minutes;
  }
}
```

Hierarchy Level

[edit access profile *profile-name*]

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
accounting, **update-interval**, and **statistics** options added in Junos OS Release 14.2R1 for MX Series routers.

Description

Define the subscriber service accounting configuration.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Configuring Service Accounting with JSRC*
- *Service Accounting with JSRC*
- *Configuring Service Accounting in Local Flat Files*
- *Configuring Service Accounting*
- *Configuring Per-Subscriber Session Accounting*

service-deployment

Syntax

```
service-deployment {
  servers server-address {
    port port-number;
  }
  source-address source-address;
}
```

Hierarchy Level

[edit system services]

Release Information

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

Description

Enable Junos OS to work with the Session and Resource Control (SRC) software.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Configuring the Junos OS to Work with SRC Software*

service-profile (DHCP Local Server)

Syntax

```
service-profile dynamic-profile-name;
```

Hierarchy Level

```
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name],
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server group group-name interface interface-name],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
  services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]
```

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the default subscriber service or DHCP client management service, which is activated when the subscriber or client logs in and no other service is activated by a RADIUS server or a provisioning server.

- To specify the default service for all DHCP local server clients, include the **service-profile** statement at the **[edit system services dhcp-local-server]** hierarchy level.
- To specify the default service for a named group of interfaces, include the **service-profile** statement at the **[edit system services dhcp-local-server group *group-name*]** hierarchy level.
- To specify the default service for a particular interface within a named group of interfaces, include the **service-profile** statement at the **[edit system services dhcp-local-server group *group-name* interface *interface-name*]** hierarchy level.
- For DHCPv6 clients, use the **service-profile** statement at the **[edit system services dhcp-local-server dhcpv6]** hierarchy level.

Options

dynamic-profile-name—Name of the dynamic profile that defines the service.

Required Privilege Level

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

Related Documentation

- Extended DHCP Local Server Overview on page 562
- *Default Subscriber Service Overview*
- *Configuring a Default Subscriber Service*

service-profile (DHCP Relay Agent)

Syntax

```
service-profile dynamic-profile-name;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay group group-name interface interface-name],
[edit forwarding-options dhcp-relay dhcpv6 groupgroup-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6 ...]** hierarchy levels introduced in Junos OS Release 11.4.
Support at the **[edit ... dual-stack-group *dual-stack-group-name*]** hierarchy level introduced in Junos OS Release 15.1.

Description

Specify the default subscriber service (or the default DHCP client management service), which is activated when the subscriber (or client) logs in and no other service is activated by a RADIUS server or a provisioning server.

- To specify the default service for all DHCP relay agent clients, include the **service-profile** statement at the **[edit forwarding-options dhcp relay]** hierarchy level.
- To specify the default service for a named group of interfaces, include the **service-profile** statement at the **[edit forwarding-options dhcp relay group *group-name*]** hierarchy level.
- To specify the default service for a particular interface within a named group of interfaces, include the **service-profile** statement at the **[edit forwarding-options dhcp relay group *group-name* interface *interface-name*]** hierarchy level.

Options

dynamic-profile-name—Name of the dynamic service profile.

Required Privilege Level

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

Related Documentation

- dhcp-relay on page 997
- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
- Grouping Interfaces with Common DHCP Configurations on page 670
- *Default Subscriber Service Overview*

- *Configuring a Default Subscriber Service*

services (System Services)

Syntax

```
services {
  dhcp { # DHCP is not supported on a DCF
    dhcp_services;
  }
  dtcp-only
  flow-tap-dtcp {
    ssh {
      connection-limit limit;
      rate-limit limit;
    }
  }
  extension-service {
    request-response{
      grpc {
        ssl{
          address ip-address;
          local-certificate local-certificate;
          port port;
        }
        max-connections max-connections;
      }
    }
    notification {
      port port;
      max-connections max-connections;
      allow-clients {
        address ip-address;
      }
    }
    traceoptions {
      file <filename> <files number> <match regex> <size size> <world-readable |
        no-world-readable>;
      flag flag;
      no-remote-trace;
    }
  }
  finger {
    connection-limit limit;
    rate-limit limit;
  }
  ftp {
    authentication-order [authentication-methods];
    connection-limit limit;
    rate-limit limit;
  }
  service-deployment {
    servers address {
      port-number port-number;
    }
    source-address address;
  }
```

```
ssh {
  authentication-order [authentication-methods];
  ciphers [ cipher-1 cipher-2 cipher-3 ...];
  client-alive-count-max seconds;
  client-alive-interval seconds;
  connection-limit limit;
  fingerprint-hash (md5 | sha2-256);
  hostkey-algorithm (algorithm | no-algorithm);
  key-exchange [algorithm];
  macs [algorithm];
  max-sessions-per-connection <number>;
  no-passwords;
  no-public-keys;
  no-tcp-forwarding;
  protocol-version [v1 v2];
  rate-limit limit;
  root-login (allow | deny | deny-password);
  sftp-server;
}
resource-monitor {
  free-fw-memory-watermark number;
  free-heap-memory-watermark number;
  free-nh-memory-watermark number;
  high-threshold number;
  no-logging;
  no-throttle;
  resource-category jtree {
    resource-type (continguous-pages | free-dwords | free-pages) {
      low-watermark number;
      high-watermark number;
    }
  }
  subscribers-limit {
    client-type (any | dhcp | l2tp | pppoe) {
      chassis {
        limit limit;
      }
      fpc slot-number {
        limit limit;
        pic number {
          limit limit;
          port number {
            limit limit;
          }
        }
      }
    }
  }
  traceoptions {
    file filename <files number> <match regular-expression> <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

```
subscriber-management {
  enable;
  enforce-strict-scale-limit-license;
  gres-route-flush-delay;
  }
  overrides {
    event {
      catastrophic-failure {
        reboot (master | standby);
      }
    }
    interfaces {
      family (inet | inet6) {
        layer2-liveness-detection;
      }
    }
    no-unsolicited-ra;
    ra-initial-interval-max seconds;
    ra-initial-interval-min seconds;
    shmlog {
      disable;
      file filename <files maximum-no-files> <size maximum-file-size>;
      filtering enable;
      log-name {
        all;
        logname {
          <brief | detail | extensive | none | terse>;
          <file-logging |no-file-logging>;
        }
        }
      log-type (debug | info | notice);
    |
  }
  redundancy {
    interface name {
      virtual-inet-address virtual-v4-address;
      virtual-inet6-address virtual-v6-address;
    }
    no-advertise-routes-on-backup;
    protocol vrrp;
  }
  traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
  }
}
telnet {
  authentication-order [authentication-methods];
  connection-limit limit;
  rate-limit limit;
}
web-management {
  http {
    interfaces [ names ];
```

```
      port port;
    }
    https {
      interfaces [ names ];
      local-certificate name;
      port port;
    }
    session {
      idle-timeout [ minutes ];
      session-limit [ limit ];
    }
  }
  xnm-ssl {
    connection-limit limit;
    local-certificate name;
    rate-limit limit;
    ssl-renegotiation;
  }
}
```

Hierarchy Level

[edit system]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
extension-service option added in Junos OS Release 16.1 for MX80, MX104, MX240, MX480, MX960, MX2010, MX2020, vMX Series.
grpc option added in Junos OS Release 16.2 for MX80, MX104, MX240, MX480, MX960, MX2010, MX2020, vMX Series.

Description

Configure the router or switch so that users on remote systems can access the local router or switch through the DHCP server, DTCP over SSH, finger, rlogin, SSH, telnet, Web management, Junos XML protocol SSL, and network utilities, or enable Junos OS to work with the Session and Resource Control (SRC) software. Also, enable configuration of third-party applications developed using the Juniper Extension Toolkit (JET) to run on Junos OS.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Configuring the Junos OS to Work with SRC Software*
- *Understanding JET Interaction with Junos OS*
- *Configuring Junos OS Enhanced Subscriber Management*
- *How to Configure M:N Subscriber Redundancy with DHCP Binding Synchronization*

services (Switches)

Syntax

```
services {
  service-deployment {
    servers address {
      port-number port-number;
    }
    source-address address;
  }
  ssh {
    connection-limit limit;
    protocol-version [v1 v2];
    rate-limit limit;
    root-login (allow | deny | deny-password);
  }
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure the switch so that users on remote systems can access the local switch through SSH.

The remaining statements are explained separately.

Required Privilege Level

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

services (System Services)

Syntax

```
services {
  dhcp { # DHCP is not supported on a DCF
    dhcp_services;
  }
  dtcp-only
  flow-tap-dtcp {
    ssh {
      connection-limit limit;
      rate-limit limit;
    }
  }
  extension-service {
    request-response{
      grpc {
        ssl{
          address ip-address;
          local-certificate local-certificate;
          port port;
        }
        max-connections max-connections;
      }
    }
    notification {
      port port;
      max-connections max-connections;
      allow-clients {
        address ip-address;
      }
    }
    traceoptions {
      file <filename> <files number> <match regex> <size size> <world-readable |
        no-world-readable>;
      flag flag;
      no-remote-trace;
    }
  }
  finger {
    connection-limit limit;
    rate-limit limit;
  }
  ftp {
    authentication-order [authentication-methods];
    connection-limit limit;
    rate-limit limit;
  }
  service-deployment {
    servers address {
      port-number port-number;
    }
    source-address address;
  }
```

```
ssh {
  authentication-order [authentication-methods];
  ciphers [ cipher-1 cipher-2 cipher-3 ...];
  client-alive-count-max seconds;
  client-alive-interval seconds;
  connection-limit limit;
  fingerprint-hash (md5 | sha2-256);
  hostkey-algorithm (algorithm | no-algorithm);
  key-exchange [algorithm];
  macs [algorithm];
  max-sessions-per-connection <number>;
  no-passwords;
  no-public-keys;
  no-tcp-forwarding;
  protocol-version [v1 v2];
  rate-limit limit;
  root-login (allow | deny | deny-password);
  sftp-server;
}
resource-monitor {
  free-fw-memory-watermark number;
  free-heap-memory-watermark number;
  free-nh-memory-watermark number;
  high-threshold number;
  no-logging;
  no-throttle;
  resource-category jtree {
    resource-type (continguous-pages | free-dwords | free-pages) {
      low-watermark number;
      high-watermark number;
    }
  }
  subscribers-limit {
    client-type (any | dhcp | l2tp | pppoe) {
      chassis {
        limit limit;
      }
      fpc slot-number {
        limit limit;
        pic number {
          limit limit;
          port number {
            limit limit;
          }
        }
      }
    }
  }
  traceoptions {
    file filename <files number> <match regular-expression> <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

```
subscriber-management {
  enable;
  enforce-strict-scale-limit-license;
  gres-route-flush-delay;
  }
  overrides {
    event {
      catastrophic-failure {
        reboot (master | standby);
      }
    }
    interfaces {
      family (inet | inet6) {
        layer2-liveness-detection;
      }
    }
    no-unsolicited-ra;
    ra-initial-interval-max seconds;
    ra-initial-interval-min seconds;
    shmlog {
      disable;
      file filename <files maximum-no-files> <size maximum-file-size>;
      filtering enable;
      log-name {
        all;
        logname {
          <brief | detail | extensive | none | terse>;
          <file-logging |no-file-logging>;
        }
        }
      log-type (debug | info | notice);
    |
  }
  redundancy {
    interface name {
      virtual-inet-address virtual-v4-address;
      virtual-inet6-address virtual-v6-address;
    }
    no-advertise-routes-on-backup;
    protocol vrrp;
  }
  traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
  }
}
telnet {
  authentication-order [authentication-methods];
  connection-limit limit;
  rate-limit limit;
}
web-management {
  http {
    interfaces [ names ];
```

```
        port port;
    }
    https {
        interfaces [ names ];
        local-certificate name;
        port port;
    }
    session {
        idle-timeout [ minutes ];
        session-limit [ limit ];
    }
  }
  xnm-ssl {
    connection-limit limit;
    local-certificate name;
    rate-limit limit;
    ssl-renegotiation;
  }
}
```

Hierarchy Level

[edit system]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
extension-service option added in Junos OS Release 16.1 for MX80, MX104, MX240, MX480, MX960, MX2010, MX2020, vMX Series.
grpc option added in Junos OS Release 16.2 for MX80, MX104, MX240, MX480, MX960, MX2010, MX2020, vMX Series.

Description

Configure the router or switch so that users on remote systems can access the local router or switch through the DHCP server, DTCP over SSH, finger, rlogin, SSH, telnet, Web management, Junos XML protocol SSL, and network utilities, or enable Junos OS to work with the Session and Resource Control (SRC) software. Also, enable configuration of third-party applications developed using the Juniper Extension Toolkit (JET) to run on Junos OS.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- *Configuring the Junos OS to Work with SRC Software*
- *Understanding JET Interaction with Junos OS*
- *Configuring Junos OS Enhanced Subscriber Management*
- *How to Configure M:N Subscriber Redundancy with DHCP Binding Synchronization*

session (Time-out)

Syntax

```
session {
  idle-timeout minutes;
  session-limit session-limit;
}
```

Hierarchy Level

[edit system services web-management]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure limits for the number of minutes a session can be idle before it times out, and configure the number of simultaneous J-Web user login sessions.

Options

idle-timeout *minutes*—Configure the number of minutes a session can be idle before it times out.

Range: 1 through 1440

Default: 1440

session-limit *session-limit*—Configure the maximum number of simultaneous J-Web user login sessions.

Range: 1 through 1024

Default: Unlimited

Required Privilege Level

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

Related Documentation

- *J-Web Interface User Guide*

session (Time-out)

Syntax

```
session {
  idle-timeout minutes;
  session-limit session-limit;
}
```

Hierarchy Level

[edit system services web-management]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure limits for the number of minutes a session can be idle before it times out, and configure the number of simultaneous J-Web user login sessions.

Options

idle-timeout *minutes*—Configure the number of minutes a session can be idle before it times out.

Range: 1 through 1440

Default: 1440

session-limit *session-limit*—Configure the maximum number of simultaneous J-Web user login sessions.

Range: 1 through 1024

Default: Unlimited

Required Privilege Level

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

Related Documentation

- *J-Web Interface User Guide*

session-expiry

Syntax session-expiry *seconds*;

Hierarchy Level [edit services captive-portal interface (all | *interface-names*)]]

Release Information Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description The **session-expiry** statement is used to locally configure the number of seconds before the captive portal authentication session times out and the client must reattempt authentication.

NOTE: If the authentication server sends an authentication session timeout to the client, this takes priority over the value configured locally using the session-expiry statement. The session timeout value is sent from the server to the client as an attribute of the RADIUS Access-Accept message.

Options *seconds*—Duration of session.
Range: 1 through 65535
Default: 3600

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

Related Documentation

- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378
- Understanding Authentication Session Timeout on page 276

session-mode

Syntax

```
session-mode (automatic | multihop | singlehop);
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection], [edit forwarding-options dhcp-relay
  dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method
  bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method
  bfd]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the session mode.

Options

Default: automatic

automatic—Configure single-hop BFD sessions if the peer is directly connected to the router interface and multihop BFD sessions if the peer is not directly connected to the router interface.

multihop—Configure multihop BFD sessions and passive DHCP clients.

single-hop—Configure single hop BFD sessions and non-passive DHCP clients.

Required Privilege Level

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

Related Documentation

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677

single-connection

Syntax

```
single-connection;
```

Hierarchy Level

```
[edit system accounting destination tacplus server server-address]
[edit system tacplus-server server-address],
```

Release Information

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

Description

Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.

Required Privilege Level

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

Related Documentation

- Configuring TACACS+ Authentication on page 207
- Configuring TACACS+ System Accounting on page 219

single-connection

Syntax

```
single-connection;
```

Hierarchy Level

```
[edit system accounting destination tacplus server server-address]
[edit system tacplus-server server-address]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Optimize the attempt to connect to a TACACS+ server. Junos OS maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.

Required Privilege Level

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

sip-server

Syntax

```
sip-server [address | name];
```

Hierarchy Level

```
[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

Release Information Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description Configure Session Initiation Protocol (SIP) server addresses or names for DHCP servers.

Options

address—IPv4 address of the SIP server. To configure multiple SIP servers, include multiple ***address*** options. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).

name—Fully qualified domain name of the SIP server. To configure multiple SIP servers, include multiple ***name*** options. This domain name must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).

Required Privilege Level

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

Related Documentation

- Configuring a DHCP SIP Server (CLI Procedure) on page 592
- Configuring a DHCP Server on Switches (CLI Procedure) on page 588

size

Syntax size *bytes*;

Hierarchy Level [edit accounting-options file *filename*]

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

Description Specify attributes of an accounting-data log file.

Options ***bytes***—Maximum size of each log file, in bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). When a log file (for example, **profilelog**) reaches its maximum size, it is renamed **profilelog.0**, then **profilelog.1**, and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. If you do not specify a size, the file is closed, archived, and renamed when the time specified for the transfer interval is exceeded.

Syntax: ***x*** to specify bytes, ***x***k to specify KB, ***x***m to specify MB, ***x***g to specify GB

Range: 256 KB through 1 GB

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

Related Documentation

- *Configuring the Maximum Size of the File*

snmp

List of Syntax

Syntax: MX, M, T, ACX, PTX Series Routers and EX Series Switches on page 1487
Syntax: QFX Series Switches, QFabric, OCX1100 and EX4600 on page 1487

Syntax: MX, M, T, ACX, PTX Series Routers and EX Series Switches

```
snmp { ... }
```

Syntax: QFX Series Switches, QFabric, OCX1100 and EX4600

```
snmp {
  client-list client-list-name {
    ip-addresses;
  }
  community community-name {
    authorization authorization;
    client-list-name client-list-name;
    clients {
      address restrict;
    }
    logical-system logical-system-name {
      routing-instance routing-instance-name {
        clients {
        addresses;
        }
      }
    }
    routing-instance routing-instance-name {
      clients {
      addresses;
      }
    }
    view view-name;
  }
  contact contact;
  description description;
  filter-duplicates;
  filter-interfaces;
  health-monitor {
    falling-threshold integer;
    interval seconds;
    rising-threshold integer;
  }
  interface [ interface-names ];
  location location;
  name name;
  nonvolatile {
    commit-delay seconds;
  }
  rmon {
    alarm index {
      description description;
      falling-event-index index;
```

```
      falling-threshold integer;
      falling-threshold-interval seconds;
      interval seconds;
      request-type;
      rising-event-index index;
      rising-threshold integer;
      sample-type (absolute-value | delta-value);
      startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
      syslog-subtag syslog-subtag;
      variable oid-variable;
    }
    event index {
      community community-name;
      description description;
      type type;
    }
    history history-index {
      bucket-size number;
      interface interface-name;
      interval seconds;
      owner owner-name;
    }
  }
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match
      regular-expression>;
    flag flag;
  }
  trap-group group-name {
    categories {
      category;
    }
    destination-port port-number;
    routing-instance routing-instance-name;
    targets {
      address;
    }
    version (all | v1 | v2);
  }
  trap-options {
    agent-address outgoing-interface;
    source-address address;
  }
  v3 {
    notify name {
      tag tag-name;
      type trap;
    }
    notify-filter profile-name {
      oid object-identifier (include | exclude);
    }
    snmp-community community-index {
      community-name community-name;
      security-name security-name;
      tag tag-name;
```

```
}
target-address target-address-name {
  address address;
  address-mask address-mask;
  logical-system logical-system;
  port port-number;
  retry-count number;
  routing-instance routing-instance-name;
  tag-list tag-list;
  target-parameters target-parameters-name;
  timeout seconds;
}
target-parameters target-parameters-name {
  notify-filter profile-name;
  parameters {
    message-processing-model (v1 | v2c | V3);
    security-level (authentication | none | privacy);
    security-model (usm | v1 | v2c);
    security-name security-name;
  }
}
usm {
  local-engine {
    user username {
      authentication-sha {
        authentication-password authentication-password;
      }
      authentication-md5 {
        authentication-password authentication-password;
      }
      authentication-none;
      privacy-aes128 {
        privacy-password privacy-password;
      }
      privacy-des {
        privacy-password privacy-password;
      }
      privacy-3des {
        privacy-password privacy-password;
      }
      privacy-none;
    }
  }
  remote-engine engine-id {
    user username {
      authentication-sha {
        authentication-password authentication-password;
      }
      authentication-md5 {
        authentication-password authentication-password;
      }
      authentication-none;
      privacy-aes128 {
        privacy-password privacy-password;
      }
```

```
            privacy-des {
              privacy-password privacy-password;
            }
            privacy-3des {
              privacy-password privacy-password;
            }
            privacy-none {
              privacy-password privacy-password;
            }
          }
        }
      }
      vacm {
        access {
          group group-name {
            (default-context-prefix | context-prefix context-prefix) {
              security-model (any | usm | v1 | v2c) {
                security-level (authentication | none | privacy) {
                  notify-view view-name;
                  read-view view-name;
                  write-view view-name;
                }
              }
            }
          }
        }
        security-to-group {
          security-model (usm | v1 | v2c) {
            security-name security-name {
              group group-name;
            }
          }
        }
      }
    }
    view view-name {
      oid object-identifier (include | exclude);
    }
}
}
```

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series Routers.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure SNMP.

SNMP modules cannot have the slash (/) character or the @ character in the name.

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

Related Documentation
- *Configuring SNMP on a Device Running Junos OS*
- *Understanding SNMP Implementation in Junos OS*
- *Configuring SNMP*

source-address (NTP, RADIUS, System Logging, or TACACS+)

Syntax
source-address *source-address* <routing-instance *routing-instance-name*>;

Hierarchy Level
[edit system accounting destination radius server *server-address*],
[edit system accounting destination tacplus server *server-address*],
[edit system ntp],
[edit system radius-server *server-address*],
[edit system syslog],
[edit system tacplus-server *server-address*]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Specify a source address for each configured IPv4 or IPv6 TACACS+ server, RADIUS server, NTP server, or the source address to record in system log messages that are directed to a remote machine.

Options
source-address—A valid IP address configured on one of the router or switch interfaces. For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all **host *hostname*** statements at the **[edit system syslog]** hierarchy level, but not for messages directed to the other Routing Engine.

routing-instance *routing-instance-name*—(Optional) The routing instance name in which the source address is defined.

Default: The primary address of the interface

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

Related Documentation
- *ntp*

source-address (SRC Software)

Syntax source-address *source-address*;

Hierarchy Level [edit system services service-deployment]

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

Description Enable Junos OS to work with the Session and Resource Control (SRC) software.

Options ***source-address***— Local IPv4 address to be used as source address for traffic to the SRC server. The source address restricts traffic within the out-of-band network.

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

Related Documentation

- *Configuring the Junos OS to Work with SRC Software*

source-address-giaddr

Syntax

```
source-address-giaddr;
```

Hierarchy Level

[edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface *interface-name*]

Release Information

Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description

Configure the gateway IP address (giaddr) as the source IP address of the switch for relayed DHCP packets when the switch is used as the DHCP relay agent.

When this statement is entered in the [**edit forwarding-options helpers bootp**] hierarchy, the gateway IP address is configured as the source IP address of the switch for relayed DHCP packets exiting all interfaces on the switch.

When this statement is entered in the [**edit forwarding-options helpers bootp interface *interface-name***] hierarchy, the gateway IP address is configured as the source IP address of the switch for relayed DHCP packets exiting the specified interface of the switch.

In Junos OS Release 10.1 for EX Series switches and later releases, the IP address of the interface that the DHCP packet exits on the switch acting as a DHCP relay agent is used as the source IP address for relayed DHCP packets by default.

In Junos OS Releases 9.6 and 10.0 for EX Series switches, the gateway IP address of the switch is always used as the source IP address for relayed DHCP packets when the switch is used as the DHCP relay agent.

In Junos OS Releases 9.3 through 9.5 for EX Series switches, the IP address of the interface that the DHCP packet exits on the switch acting as a DHCP relay agent is always used as the source IP address for relayed DHCP packets.

Required Privilege Level

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

Related Documentation

- *DHCP/BOOTP Relay for Switches Overview*

source-classes

Syntax

```
source-classes {
  source-class-name;
}
```

Hierarchy Level

[edit accounting-options class-usage-profile *profile-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 15.1F6 for PTX Series routers with third-generation FPCs installed.

Description

Specify the source classes for which statistics are collected.

Options

source-class-name—Name of the source class to include in the class usage profile.

Required Privilege Level

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

Related Documentation

- *Configuring a Class Usage Profile*

source-ip-change (Forwarding Options)

Syntax

```
source-ip-change;
```

Hierarchy Level

[edit forwarding-options dhcp-relay]

Release Information

Statement changed from **vpn** to **source-ip-change** in Junos OS Release 15.1X49-D130 and later releases.

Description

For Dynamic Host Configuration Protocol (DHCP) client request forwarding, enable source IP change for the device to use address of egress interface as source IP address.

Required Privilege Level

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*

ssh

Syntax

```
ssh {
  authentication-order [method 1 method2...];
  ciphers [ cipher-1 cipher-2 cipher-3 ...];
  client-alive-count-max seconds;
  client-alive-interval seconds;
  connection-limit limit;
  fingerprint-hash (md5 | sha2-256);
  hostkey-algorithm (algorithm | no-algorithm);
  key-exchange [algorithm1 algorithm2...];
  log-key-changes log-key-changes;
  macs [algorithm1 algorithm2...];
  max-sessions-per-connection <number>;
  no-passwords;
  no-public-keys;
  no-tcp-forwarding;
  protocol-version [v2];
  rate-limit limit;
  root-login (allow | deny | deny-password);
  sftp-server;
  }
tcp-forwarding (JDM)
```

Hierarchy Level

```
[edit system services]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
client-alive-interval and **client-alive-max-count** statements introduced in Junos OS Release 12.2.
no-passwords statement introduced in Junos OS Release 13.3.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
no-public-keys statement introduced in Junos OS release 15.1.
tcp-forwarding statement introduced in Junos OS Release 15.1X53-D50 for the NFX250 Network Services Platform.
fingerprint-hash statement introduced in Junos OS Release 16.1.
log-key-changes statement introduced in Junos OS Release 17.4R1.
sftp-server statement introduced in Junos OS Release 19.1R1.

Description

Allow SSH requests from remote systems to access the local router or switch.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 232

ssh

List of Syntax

Syntax on page 1497
Syntax (EX Series Switch and the QFX Series) on page 1497

Syntax

```
ssh host
<bypass-routing>
<inet | inet6>
<interface interface-name>
<logical-system logical-system-name>
<tenant tenant-name>
<routing-instance routing-instance-name>
<source address>
<v2>
<port port-number>
```

Syntax (EX Series Switch and the QFX Series)

```
ssh host
<bypass-routing>
<inet | inet6>
<interface interface-name>
<routing-instance routing-instance-name>
<source address>
<v2>
<port port-number>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
The command **tenant** option is introduced in Junos OS Release 19.2R1 for SRX Series.

Description

Use the SSH program to open a connection between a local router or switch and a remote system and execute commands on the remote system. You can issue the **ssh** command from the Junos OS CLI to log in to a remote system or from a remote system to log in to the local router or switch. When executing this command, you include one or more CLI commands by enclosing them in quotation marks and separating the commands with semicolons:

```
ssh address 'cli-command1 ; cli-command2 '
```

Options

host—Name or address of the remote system.

bypass-routing—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

inet | inet6—(Optional) Create an IPv4 or IPv6 connection, respectively.

interface *interface-name*—(Optional) Interface name for the SSH session. (This option does not work when *default-address-selection* is configured at the **[edit system]** hierarchy level, because this configuration uses the loopback interface as the source address for all locally generated IP packets.)

logical-system *logical-system-name*—(Optional) Name of a particular logical system for the SSH attempt.

tenant *tenant-name*—(Optional) Name of a particular tenant system for the SSH attempt.

routing-instance *routing-instance-name*—(Optional) Name of the routing instance for the SSH attempt.

source *address*—(Optional) Source address of the SSH connection.

v2—(Optional) Use SSH version 2 when connecting to a remote host.

port *port-number*—(Optional) Specify a port number for the SSH connection.

Additional Information

To configure an SSH (version 2) key for your user account, include the **authentication dsa-rsa** statement at the **[edit system login user *user-name*]** hierarchy level.

You can limit the number of times a user can attempt to enter a password while logging in through SSH. To specify the number of times a user can attempt to enter a password to log in through SSH, include the **retry-options** statement at the **[edit system login]** hierarchy level.

Required Privilege Level

network

Related Documentation

- Configuring SSH Host Keys for Secure Copying of Data on page 236

List of Sample Output

ssh on page 1498

Output Fields

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

Sample Output

ssh

```
user@switch> ssh user
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes

Host ?user' added to the list of known hosts.
user@device's password:
Last login: Sun Jun 21 10:43:42 1998 from junos-router
% ...
```

ssh-known-hosts

Syntax

```
ssh-known-hosts {
  host host-name {
    fetch-from-server host-name;
    load-key-file file-name;
  }
}
```

Hierarchy Level

```
[edit security ssh-known-hosts]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure SSH support for known hosts and for administering SSH host key updates.

Options

host *host-name*—Hostname of the SSH known host entry. This option has the following suboptions:

- **fetch-from-server *host-name***—Retrieve SSH public host key information from a specified server.
- **load-key-file *filename***—Import SSH host key information from the **/var/tmp/ssh-known-hosts** file.

Required Privilege Level

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

Related Documentation

- *Understanding Security Features on the QFabric System*
- Configuring SSH Host Keys for Secure Copying of Data on page 236

ssh-known-hosts

Syntax

```
ssh-known-hosts {
  fetch-from-server server-name;
  host hostname {
    dsa-key dsa-key;
    ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key;
    ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key;
    ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key;
    ed25519-key ed25519-key
    rsa-key rsa-key;
    rsa1-key rsa1-key;
  }
  load-key-file key-file;
}
```

Hierarchy Level

```
[edit security]
```

Release Information

Statement modified in Junos OS Release 8.5.

Description

Configure SSH support for known hosts and for administering SSH host key updates.

Options

- **fetch-from-server *server-name***—Retrieve SSH public host key information from a specified server.
- **load-key-file *key-file***—Import SSH host-key information from the specified **/var/tmp/ssh-known-hosts** file.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

ssh-dsa

Syntax

```
ssh-dsa "public-key";
```

Hierarchy Level

```
[edit system root-authentication]
[edit system login user authentication]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify the DSA (SSH version 2) public key. You can specify one or more public keys.

Options

ssh-dsa "*public-key*"—SSH version 2 authentication.

Required Privilege Level

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

Related Documentation

- Configuring the Root Password on page 140
- *authentication*
- root-authentication on page 1434

ssh-rsa

Syntax
```
ssh-dsa "public-key";
```

Hierarchy Level
```
[edit system root-authentication]
[edit system login user authentication]
```

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Specify the RSA (SSH version 2) public key. You can specify one or more public keys.

Options
ssh-rsa "*public-key*"—SSH version 2 authentication. Specify the RSA (SSH version 2) public key. You can specify one or more public keys.

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

Related Documentation
- *Configuring the Root Password*
- *authentication*
- root-authentication on page 1434

ssl-renegotiation

Syntax
```
ssl-renegotiation;
```

Hierarchy Level
```
[edit system services xnm-ssl]
```

Release Information
Statement introduced in Junos Os Release 13.3.

Description
Enable SSL re-negotiation for xnm-ssl service.

Default
SSL re-negotiation for xnm-ssl service is disabled by default.

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

Related Documentation
- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*

start-time

Syntax start-time *time*;

Hierarchy Level [edit accounting-options file *filename*]

Release Information Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the start time for transfer of an accounting-data log file.

Options ***time***—Start time for file transfer.
Syntax: ***YYYY-MM-DD.hh:mm***

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

Related Documentation
- *Configuring the Start Time for File Transfer*

start-time (Authentication Key Transmission)

Syntax start-time (now | *yyyy-mm-dd.hh:mm:ss*);

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify a start time for key transmission. You do not need to specify an end time for the key. If a new key is present with a new start time, the keychain rolls over to the new one. The start time must be unique within the keychain.

Options **now**—Start time as the current year, month, day, hour, minute, and second.

***day*days**—Start time as the specified number of days after the current day. For example, if the current day is the 12th and you configure **start-time 2day**, the start time will be on the 14th, exactly two days after the configuration is entered.

***hour*hours**—Start time as the specified number of hours after the current hour. For example, if the current hour is 9:00 and you configure **start-time 3hour**, the start time will be in 12:00, exactly three hours after the configuration is entered.

***minute*minutes**—Start time as the specified number of minutes after the current minute. For example, if the current minute is 27 minutes after the hour and you configure **start-time 5min**, the start time will be in 32 minutes after the hour, exactly five minutes after the configuration is entered.

***month*months**—Start time as the specified number of months after the current month. For example, if the current month is March and you configure **start-time 4month**, the start time will be in July, exactly four months after the configuration is entered.

***second*seconds**—Start time as the specified number of seconds after the current second. For example, if the current second is 10:20:40 and you configure **start-time 10seconds**, the start time will be 10:20:50, exactly 10 seconds after the configuration is entered.

***year*years**—Start time as the specified number of years after the current year. For example, if the current year is 2011 and you configure **start-time 1year**, the start time will be in 2012, exactly one year after the configuration is entered.

yyyy–mm-dd.hh:mm:ss—Start time in UTC (Coordinated Universal Time). The start time must be unique within the keychain.

Required Privilege Level

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

Related Documentation

- Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols on page 226
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

static (Protocols 802.1X)

Syntax

```
static mac-address {
  interface interface-names;
  vlan-assignment (vlan-id |vlan-name );
}
```

Hierarchy Level

[edit protocols dot1x authenticator]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure MAC addresses to exclude from 802.1X authentication. The static MAC list provides an authentication bypass mechanism for supplicants connecting to a port, permitting devices such as printers that are not 802.1X-enabled to be connected to the network on 802.1X-enabled ports.

Using this 802.1X authentication-bypass mechanism, the supplicant connected to the MAC address is assumed to be successfully authenticated and the port is opened for it. No further authentication is done for the supplicant.

You can optionally configure the VLAN that the supplicant is moved to or the interfaces on which the MAC address can gain access from.

Options

mac-address —The MAC address of the device for which 802.1X authentication should be bypassed and the device permitted access to the port.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- show dot1x static-mac-address on page 1811
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 368
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- *Configuring 802.1X Authentication (J-Web Procedure)*
- Understanding Authentication on Switches on page 268

static (Protocols 802.1X)

Syntax

```
static mac-address {
  interface interface-names;
  vlan-assignment (vlan-id |vlan-name );
}
```

Hierarchy Level

[edit protocols dot1x authenticator]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure MAC addresses to exclude from 802.1X authentication. The static MAC list provides an authentication bypass mechanism for supplicants connecting to a port, permitting devices such as printers that are not 802.1X-enabled to be connected to the network on 802.1X-enabled ports.

Using this 802.1X authentication-bypass mechanism, the supplicant connected to the MAC address is assumed to be successfully authenticated and the port is opened for it. No further authentication is done for the supplicant.

You can optionally configure the VLAN that the supplicant is moved to or the interfaces on which the MAC address can gain access from.

Options

mac-address —The MAC address of the device for which 802.1X authentication should be bypassed and the device permitted access to the port.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- show dot1x static-mac-address on page 1811
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 368
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- *Configuring 802.1X Authentication (J-Web Procedure)*
- Understanding Authentication on Switches on page 268

static-binding

Syntax

```
static-binding mac-address {
  client-identifier (ascii client-id | hexadecimal client-id);
  fixed-address {
    address;
  }
  host-name client-hostname;
}
```

Hierarchy Level

```
[edit system services dhcp],
[edit system services dhcp]
```

Release Information

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

Description

For J Series Services routers and EX Series switches only. Set static bindings for DHCP clients. A static binding is a mapping between a fixed IP address and the client's MAC address or client identifier.

Options

mac-address—The MAC address of the client. This is a hardware address that uniquely identifies a client on the network.

fixed-address *address*—Fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.

host-name *client-hostname*—Hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the **domain-name** statement.

client-identifier (ascii *client-id* | hexadecimal *client-id*)—Used by the DHCP server to index the database of address bindings. The client identifier is an ASCII string or hexadecimal number and can include a type-value pair as specified in RFC 1700, *Assigned Numbers*. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.

Required Privilege Level

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

Related Documentation

static-subscribers

Syntax

```
static-subscribers {
  disable;
}
```

Hierarchy Level [edit system processes]

Release Information Statement introduced in Junos OS Release 8.5.

Description Associate subscribers with statically configured interfaces, and provide dynamic service activation for these subscribers.

Options **disable**—Disable the static subscribers process.

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

statistics (Access Profile)

Syntax

```
statistics (time | volume-time);
```

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
volume-time option added 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.

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*

statistics-service

Syntax

```
statistics-service {
  command binary-file-path;
  disable;
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the Packet Forwarding Engine (PFE) statistics service management process.

Options

- **command *binary-file-path***—Path to the binary process.
- **disable**—Disable the Packet Forwarding Engine (PFE) statistics service management process.

Required Privilege Level

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

strict (DHCP Local Server)

Syntax

```
strict;
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server dhcpv6 group *group-name* reconfigure]

Release Information

Statement introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify whether the server denies a client to bind when the client does not indicate that it accepts reconfigure messages. This feature is available only for DHCPv6.

Default

Accept solicit messages from clients that do not support reconfiguration and permit them to bind.

Required Privilege Level

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

Related Documentation

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview on page 662
- Preventing Binding of Clients That Do Not Support Reconfigure Messages on page 615

sub-prefix-length

Syntax

```
sub-prefix-length sub-prefix-length;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client
  prefix-delegating]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
  family inet6 dhcpv6-client prefix-delegating]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6
  dhcpv6-client prefix-delegating]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30 and in Junos OS Release 15.1X49-D100.
The **logical-systems** and **tenants** options are introduced in Junos OS Release 18.4R1.

Description

Allows you to configure DHCPv6 client sub prefix length. The DHCPv6 client separates the delegated prefix according to sub-prefix lengths. If the delegated prefix is not enough for all interfaces, the client sends out a syslog message.

Required Privilege Level

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

Related Documentation

- preferred-prefix-length on page 1345

subscriber-management-helper

Syntax

```
subscriber-management-helper {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the subscriber management helper process.

Options

- **command** ***binary-file-path***—Path to the binary process.
- **disable**—Disable the subscriber management helper process.
- **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
  - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
  - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

Required Privilege Level

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

supplicant

Syntax

```
supplicant (multiple | single | single-secure);
```

Hierarchy Level

```
[edit protocols dot1x authenticator interface (all | [interface-names])],
[edit services captive-portal interface (all | interface-names)]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement added to the **[edit services captive-portal interface]** hierarchy in Junos OS Release 10.1 for EX Series switches
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure the MAC-based method used to authenticate clients for 802.1X or captive portal authentication.

Default

single

Options

single—Authenticates only the first client that connects to an authenticator port. All other clients connecting to the authenticator port after the first are permitted free access to the port without further authentication. If the first authenticated client logs out, all other supplicants are locked out until a client authenticates again.

single-secure—Authenticates only one client to connect to an authenticator port. The host must be directly connected to the switch.

multiple—Authenticates multiple clients individually on one authenticator port. You can configure the number of clients per port. If you also configure a maximum number of devices that can be connected to a port through port security settings, the lower of the configured values is used to determine the maximum number of clients allowed per port.

Required Privilege Level

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

Related Documentation

- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Understanding Authentication on Switches on page 268
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

supplicant-timeout

Syntax supplicant-timeout *seconds*;

Hierarchy Level [edit protocols dot1x authenticator interface (802.1X) (all | [*interface-name*])

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description For 802.1X authentication, configure how long the port waits for a response when relaying a request from the authentication server to the supplicant before resending the request.

Default 30 seconds

Options ***seconds*** —Number of seconds.
Range: 1 through 60 seconds
Default: 30 seconds

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

Related Documentation

- supplicant on page 1514
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Understanding Authentication on Switches on page 268

system

Syntax

```
system {
  accounting {
    events [ login change-log interactive-commands ];
    destination {
      radius {
        {
          server server-address {
            accounting-port port-number;
            retry number;
            secret password;
            source-address address;
            timeout seconds;
          }
        }
      }
      tacplus {
        server {
          server server-address {
            port port-number;
            secret password;
            single-connection;
            timeout seconds;
          }
        }
      }
    }
  }
}
archival {
  configuration {
    archive-sites {
      ftp://<username>:<password>@<host>:<port>/<url-path>;
      ftp://<username>:<password>@<host>:<port>/<url-path>;
    }
    transfer-interval interval;
    transfer-on-commit;
  }
}
arp {
  aging-timer minutes;
  interfaces;
}
authentication-order [ authentication-methods ];
(compress-configuration-files | no-compress-configuration-files);
default-address-selection;
domain-name domain-name;
domain-search [ domain-list ];
host-name hostname;
internet-options {
  icmpv4-rate-limitbucket-size bucket-size packet-rate packet-rate;
  source-port upper-limit <upper-limit>;
}
```

```
location {
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack number;
    vcoord vertical-coordinate;
}
login {
    announcementtext;
    class class-name {
        access-end;
        access-start;
        allow-configuration “regular-expression”;
        allowed-days “regular-expression”;
        deny-commands “regular-expression”;
        deny-configuration “regular-expression”;
        idle-timeout minutes;
        login-tip;
        permissions [ permissions ];
    }
    message text;
    password {
        change-type (set-transitions | character-set);
        format (md5 | sha1 | des);
        maximum-length length;
        minimum-changes number;
        minimum-length length;
    }
    retry-options {
        backoff-factor seconds;
        backoff-threshold number;
        minimum-time seconds;
        tries-before-disconnect number;
    }
    user username {
        authentication {
            (encrypted-password "password" | plain-text-password);
            load-key-file URL;
            remote-debug-permission (qfabric-admin | qfabric-operator |qfabric-user);
            ssh-rsa "public-key";
            ssh-dsa "public-key";
        }
        uid uid-value;
        class class-name;
        full-name complete-name;
    }
}
name-server {
```

```
    address;
}
no-multicast-echo;
no-redirects;
no-ping-record-route;
no-ping-time-stamp;
ntp {
    authentication-key number type type value password;
    server address <key key-number> <version value> <prefer>;
}
ports {
    auxiliary {
        disable;
        insecure;
        type terminal-type;
    }
    console {
        disable;
        insecure;
        log-out-on-disconnect;
        type terminal-type;
    }
}
radius-server server-address {
    accounting-port port-number;
    port number;
    retry number;
    secret password;
    source-address source-address;
    timeout seconds;
    }
}
radius-options {
    password-protocol mschap-v2;
    }
    attributes {
        nas-ip-address ip-address;
root-authentication {
    (encrypted-password “password” | plain-text-password);
    ssh-rsa “public-key”;
    ssh-dsa “public-key”;
}
(saved-core-context | no-saved-core-context);
saved-core-files saved-core-files;
services {
    finger {
        connection-limit limit;
        rate-limit limit;
    }
    flow-tap-dtcp {
        ssh {
            connection-limit limit;
            rate-limit limit;
        }
    }
```

```
    ftp {
        connection-limit limit;
        rate-limit limit;
    }
    service-deployment {
        servers server-address {
            port port-number;
        }
        source-address source-address;
    }
    ssh {
        root-login (allow | deny | deny-password);
        protocol-version [v1 v2];
        connection-limit limit;
        rate-limit limit;
    }
    telnet {
        connection-limit limit;
        rate-limit limit;
    }
    web-management {
        http {
            interfaces [ interface-names ];
            port port;
        }
        https {
            interfaces [ interface-names ];
            local-certificate name;
            port port;
        }
        session {
            idle-timeout [ minutes ];
            session-limit [ session-limit ];
        }
    }
    xnm-clear-text {
        connection-limit limit;
        rate-limit limit;
    }
    xnm-ssl {
        connection-limit limit;
        local-certificate name;
        rate-limit limit;
    }
}
static-host-mapping {
    hostname {
        alias [ alias ];
        inet [ address ];
        sysid system-identifier;
    }
}
syslog {
    archive {
        files number;
```

```
      size maximum-file-size;
      start-time "YYYY-MM-DD.hh:mm";
      transfer-interval minutes;
      (world-readable | no-world-readable);
    }
    console {
      facility severity;
    }
    file filename {
      archive {
        files number;
        size maximum-file-size;
        start-time "YYYY-MM-DD.hh:mm";
        transfer-interval minutes;
        (world-readable | no-world-readable);
      }
      explicit-priority;
      facility severity;
      match "regular-expression";
      structured-data {
        brief;
      }
    }
    host (hostname | other-routing-engine | scc-master) {
      explicit-priority;
      facility-override facility;
      facility severity;
      log-prefix string;
      match "regular-expression";
    }
    source-address source-address;
    time-format (millisecond | year | year millisecond);
    user (username | *) {
      facility severity;
      match "regular-expression";
    }
}
tacplus-options {
    service-name service-name;
    (no-cmd-attribute-value | exclude-cmd-attribute);
}
tacplus-server server-address {
    port
    secret password;
    single-connection;
    source-address source-address;
    timeout seconds;
}
time-zone (GMThour-offset | time-zone);
}
tracing {
    destination-override {
    syslog host;
    }
}
```

```
  use-imported-time-zones;
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure system management properties.

NOTE: The **radius-server source-address** and **radius-options** statements are not available on the QFabric system.

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

system

Syntax

```
system { ... }
```

Hierarchy Level [edit]

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

Description Configure system management properties.

Options This command has no options.

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

Related Documentation

- *System Management Configuration Statements*

system-generated-certificate

Syntax system-generated-certificate;

Hierarchy Level [edit system services web-management https]

Release Information Command introduced in Junos OS Release 11.1 for EX Series switches.

Description Configure the automatically generated self-signed certificate for enabling HTTPS services.

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

Related Documentation

- *Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure)*

tacplus

Syntax

```
tacplus {
  server {
    server-address {
      port port-number;
      routing-instance (Accounting and Authentication) routing-instance;
      secret password;
      single-connection;
      timeout seconds;
    }
  }
}
```

Hierarchy Level

[edit system accounting destination]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
routing-instance option introduced in Junos OS Release 17.4R1.

Description

Configure the Terminal Access Controller Access Control System Plus (TACACS++).

Options

server-address—Address of the TACACS++ authentication server.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Configuring TACACS+ System Accounting on page 219

tacplus

Syntax

```
tacplus {
  server server-address {
    port port-number;
    secret password;
    single-connection;
    source-address source-address;
    timeout seconds;
  }
}
```

Hierarchy Level

```
[edit system accounting destination]
```

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the TACACS+ accounting server.

Options

- ***server-address*** —Specify the address of the TACACS+ authentication server.
- **port *number***—Configure the port number on which to contact the TACACS+ server.
- **single-connection**—Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.
- **source-address *address***—Configure a source address for each configured TACACS+ server.
- **timeout *seconds***—Configure the amount of time that the local device waits to receive a response from a TACACS+ server.

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

Related Documentation

- Example: Configuring a TACACS+ Server for System Authentication on page 210

tacplus-options

Syntax

```
tacplus-options {
  (exclude-cmd-attribute | no-cmd-attribute-value);
  enhanced-accounting;
  strict-authorization
  service-name service-name;
  timestamp-and-timezone;
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
no-cmd-attribute-value and **exclude-cmd-attribute** options introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 11.1 for QFX Series.
timestamp-and-timezone option introduced in Junos OS Release 12.2.
strict-authorization option introduced in Junos OS Release 13.3 for EX Series, M Series, MX Series, PTX Series, and T Series.
enhanced-accounting option introduced in Junos OS Release 14.1.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Configure TACACS+ options for authentication and accounting.

Options

enhanced-accounting—View the attribute values of a logged in user.

exclude-cmd-attribute—Exclude the **cmd** attribute value completely from start and stop accounting records to enable logging of accounting records in the correct log file on a TACACS+ server.

no-cmd-attribute-value—Set the **cmd** attribute value to an empty string in the TACACS+ accounting start and stop requests to enable logging of accounting records in the correct log file on a TACACS+ server.

service-name *service-name*—Name of the authentication service used when you configure multiple TACACS+ servers to use the same authentication service.

Default: junos-exec

strict-authorization—Deny login if authorization request fails. When a user is logging in, Junos OS issues two TACACS+ requests—first the authentication request followed by the authorization request. By default, when the authorization request is rejected by the TACACS+ server, Junos OS ignores this and allows full access to the user. When the **set system tacplus-options strict-authorization** statement is set, Junos OS denies access to the user even on failure of the authorization request.

timestamp-and-timezone—Include this statement if you want start time, stop time, and timezone attributes included in start/stop accounting records.

Required Privilege Level

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

Related Documentation

- Configuring TACACS+ Authentication on page 207
- Configuring TACACS+ System Accounting on page 219
- Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 169
- **enhanced-accounting on page 1076**

tacplus-server

Syntax

```
tacplus-server server-address {
  routing-instance (Accounting and Authentication) routing-instance;
  secret password;
  single-connection;
  source-address source-address;
  timeout seconds;
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
routing-instance option introduced in Junos OS Release 17.4R1.

Description

Configure the IPv4 or IPv6 TACACS++ server.

Options

server-address—Address of the IPv4 or IPv6 TACACS++ authentication server.

NOTE: Wildcard characters cannot be used in the TACACS+ server address or source address. This is because the TACACS+ server and source can accept both IPv4 and IPv6 addresses and, if you use wildcard characters for these addresses, Junos OS cannot validate mismatching server and source address families.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Configuring TACACS+ Authentication on page 207

tacplus-server

Syntax

```
tacplus-server server-address {
  port port-number;
  secret password;
  single-connection;
  source-address source-address;
  timeoutseconds;
}
```

Hierarchy Level

```
[edit system]
```

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 TACACS+ server.

Options

- **server-address**—Address of the TACACS+ authentication server.

  NOTE: Wildcard characters cannot be used in the TACACS server address or source address. This is because the TACACS server and source can accept both IPv4 and IPv6 addresses and, if you use wildcard characters for these addresses, Junos OS cannot validate mismatching server and source address families.

- **port**—Port number of TACACS+ authentication server.
- **secret**—Password to use with the RADIUS or TACACS+ server. The secret password used by the local router or switch must match that used by the server. Password to use; can include spaces included in quotation marks.
- **single-connection**—Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.
- **source-address**—Source address for each configured TACACS+ server, RADIUS server, NTP server, or the source address to record in system log messages that are directed to a remote machine. Configure a valid IP address on one of the device interfaces. For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all **host *hostname*** statements at the **[edit system syslog]** hierarchy level.
- **timeout**—The amount of time that the local device waits to receive a response from a RADIUS or TACACS+ server. The timeout range is 1 through 90 seconds. The default is 3 seconds.

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

Related Documentation
- Example: Configuring a TACACS+ Server for System Authentication on page 210

targets

Syntax

```
targets {
  address;
}
```

Hierarchy Level

```
[edit snmp trap-group group-name]
```

Release Information
Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Configure one or more systems to receive SNMP traps.

Options
address—IPv4 or IPv6 address of the system to receive traps. You must specify an address, not a hostname.

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

Related Documentation
- *Configuring SNMP Trap Groups*

Configuring SNMP Trap Groups

telnet

Syntax

```
telnet {
  authentication-order [authentication-methods];
  connection-limit limit;
  rate-limit limit;
}
```

Hierarchy Level

[edit system services]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Provide Telnet connections from remote systems to the local router or switch.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Configuring Telnet Service for Remote Access to a Router or Switch on page 230

telnet

List of Syntax

Syntax on page 1531
Syntax (EX Series Switches) on page 1531
Syntax (Junos OS Evolved) on page 1531

Syntax

```
telnet host
<8bit>
<inet | inet6>
<port port-number>
<routing-instance routing-instance-name>
<logical-system logical-system-name>
<tenant tenant-name>
```

Syntax (EX Series Switches)

```
telnet host
<8bit>
<bypass-routing>
<inet | inet6>
<interface interface-name>
<no-resolve>
<port port-number>
<routing-instance routing-instance-name>
<source source-address>
```

Syntax (Junos OS Evolved)

```
telnet host
<8bit>
<inet | inet6>
<port port-number>
<routing-instance routing-instance-name>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
The following options are deprecated in Junos OS Evolved Release 18.3R1: **bypass-routing**, **interface**, **no-resolve**, and **source**.
The command **tenant** option is introduced in Junos OS Release 19.2R1 for SRX Series.

Description

Open a telnet session to a remote system. Type Ctrl+] to escape from the telnet session to the telnet command level, and then type **quit** to exit from telnet.

NOTE: For Junos OS Evolved, use the **routing-instance mgmt_junos** option to access a remote system through the management interface.

Options

host—Name or address of the remote system.

8bit—(Optional) Use an 8-bit data path.

bypass-routing—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

inet | inet6—(Optional) Open an IPv4 or IPv6 session, respectively.

interface ***interface-name***—(Optional) Interface name for the telnet session. (This option does not work when **default-address-selection** is configured at the **[edit system]** hierarchy level, because this configuration uses the loopback interface as the source address for all locally generated IP packets.)

logical-system ***logical-system-name***—(Optional) Name of a particular logical system for the telnet attempt.

tenant ***tenant-name***—(Optional) Name of a particular tenant system for the telnet attempt.

no-resolve—(Optional) This option is not supported for Junos OS Evolved Release 18.3R1. Do not attempt to determine the hostname that corresponds to the IP address.

port ***port-number***—(Optional) Port number or service name on the remote system.

routing-instance ***routing-instance-name***—(Optional) Name of the routing instance for the telnet attempt.

source ***source-address***—(Optional) This option is not supported for Junos OS Evolved Release 18.3R1. Source address of the telnet connection.

Additional Information

You can limit the number of times a user can attempt to enter a password while logging in through telnet. To specify the number of times a user can attempt to enter a password to log in through telnet, include the retry-options statement at the [**edit system login**] hierarchy level.

Required Privilege Level

network

List of Sample Output

telnet on page 1532

Output Fields

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

Sample Output

telnet

```
user@host> telnet 192.154.1.254
Trying 192.154.169.254...
Connected to level5.company.net.
Escape character is '^]'.
```

```
ttypa
login:
```

tftp

Syntax

```
tftp {
  description text-description;
  interface interface-name {
    broadcast;
    description text-description;
    no-listen;
    server address <logical-system logical-system-name> <routing-instance
      routing-instance-name>;
  }
  server address <logical-system logical-system-name> <routing-instance
    routing-instance-name>;
}
```

Hierarchy Level

[edit forwarding-options helpers]

Release Information

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

Description

Enable TFTP request packet forwarding.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring DNS and TFTP Packet Forwarding*

threshold (detection-time)

Syntax

```
threshold milliseconds;
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection method bfd detection-time],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd
  detection-time],
[edit forwarding-options dhcp-relay liveness-detection method bfd detection-time],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd detection-time],
[edit system services dhcp-local-server group group-name liveness-detection method bfd
  detection-time],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method
  bfd detection-time],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd
  detection-time],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method
  bfd detection-time]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the threshold for the adaptation of the detection time. When the BFD session detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.

NOTE: **The threshold time must be greater than or equal to the minimum-interval or the minimum-receive-interval.**

Options

milliseconds— Value for the detection time adaptation threshold.

Range: 1 through 255,000

Required Privilege Level

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

Related Documentation

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677

threshold (transmit-interval)

Syntax

```
threshold milliseconds;
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd
  transmit-interval],
[edit forwarding-options dhcp-relay liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server group group-name liveness-detection method bfd
  transmit-interval],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method
  bfd transmit-interval],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd
  transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method
  bfd transmit-interval]
```

Release Information Statement introduced in Junos OS Release 12.1.

Description Specify the threshold for detecting the adaptation of the transmit interval. When the BFD session transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent.

Options *milliseconds* — Threshold value.

Range: 0 through 4,294,967,295 ($2^{32} - 1$)

NOTE: The threshold value specified in the threshold statement must be greater than the value specified in the minimum-interval statement for the transmit-interval statement.

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

Related Documentation

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677

timeout (System)

Syntax

```
timeout seconds;
```

Hierarchy Level

```
[edit system radius-server server-address],
[edit system tacplus-server server-address],
[edit system accounting destination radius server server-address],
[edit system accounting destination tacplus server server-address]
```

Release Information

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

Description

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

Options

seconds—Amount of time to wait.

Range: 1 through 90 seconds

Default: 3 seconds

Required Privilege Level

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

Related Documentation

- Configuring RADIUS Server Authentication on page 182
- Configuring TACACS+ Authentication on page 207
- retry on page 1427

timeout (DHCP Local Server)

Syntax

timeout *timeout-value*;

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group *group-name* reconfigure],
[edit system services dhcp-local-server dhcpv6 group *group-name* reconfigure]

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6 ...]** hierarchy levels introduced in Junos OS Release 10.4.

Description

Configure the initial value in seconds between attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces.

Options

timeout-value—Initial retry timeout value.

Range: 1 through 10 seconds

Default: 2 seconds

Required Privilege Level

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

Related Documentation

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview on page 662

- Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 664

timeout (Access Control Service)

Syntax timeout *seconds*;

Hierarchy Level [edit services unified-access-control]

Release Information Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description Configure the amount of time that the switch waits to receive a response from the Junos Pulse Access Control Service.

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

Range: **2** through **1000** seconds

Default: **300** seconds

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

Related Documentation

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 401
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 404

timeout (System)

Syntax

```
timeout seconds;
```

Hierarchy Level

```
[edit system radius-server server-address],
[edit system tacplus-server server-address],
[edit system accounting destination radius server server-address],
[edit system accounting destination tacplus server server-address]
```

Release Information

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

Description

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

Options

seconds—Amount of time to wait.

Range: 1 through 90 seconds

Default: 3 seconds

Required Privilege Level

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

Related Documentation

- Configuring RADIUS Server Authentication on page 182
- Configuring TACACS+ Authentication on page 207
- retry on page 1427

timeout-action (Access Control Service)

Syntax timeout-action (close | no-change);

Hierarchy Level [edit services unified-access-control]

Release Information Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description Specify the action to be taken when the timeout is reached for the switch's connection with the Junos Pulse Access Control Service.

Options **close**—Remove existing sessions and block further traffic.

no-change—Preserve existing connections, but block new sessions.

Default: close

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

Related Documentation

- timeout (Access Control Service) on page 1538
- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 401
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 404

tlv-filter

Syntax tlv-filter *tlv-name*;

Hierarchy Level [edit protocols lldp],
[edit protocols lldp-med],
[edit protocols lldp interface *interface-name*],
[edit protocols lldp-med interface *interface-name*]

Release Information Statement introduced in Junos OS Release 18.3 for EX Series switches.

Description Select the type, length, and value (TLV) messages that should not be advertised by Link Layer Discovery Protocol (LLDP) or LLDP Media Endpoint Discovery (LLEP-MED) protocol. LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include information such as chassis and port identification and system name and system capabilities.

In multi-vendor networks, it might not be desirable to send TLV messages because they can contain sensitive information about a network device. You can configure LLDP or LLDP-MED to disable any non-mandatory TLV message. Mandatory TLVs are: chassis-id, port-id, and time-to-live.

When you configure the **tlv-filter** statement, you specify the TLVs that you want to disable. This is useful when you want to allow most, but not all, TLVs.

You can also disable TLVs using the **tlv-select** statement. When you configure the tlv-select statement, you specify the TLVs that you want to be advertised by LLDP or LLDP-MED. All other non-mandatory TLVs are disabled.

NOTE: **The tlv-select and tlv-filter are mutually exclusive and cannot be used on the same configuration stanza at the same time.**

Default All TLVs for LLDP and LLDP-MED are enabled by default.

Options The following options can be configured using **tlv-filter** at the [**edit protocols lldp**] and [**edit protocols lldp interface *interface-name***] hierarchy levels:

port-description—The user-configured port description.

system-name—The user-configured name of the local system.

system-description—The user-configured name of the local system.

system-capabilities—The primary function performed by the system. The capabilities that system supports are defined; for example, bridge or router. This information cannot be configured, but is based on the model of the product.

management-address— IP management address of the local system.

mac-phy-config-status—Advertises information about the physical interface, such as autonegotiation status and support and MAU (medium attachment unit) type.

power-vi-mdi—Advertises MDI (media dependent interface) power support, PSE (power sourcing equipment) power pair, and power class information.

link-aggregation—Advertises whether the port is aggregated and its aggregated port ID.

maximum-frame-size—The maximum transmission unit (MTU) of the interface sending LLDP frames.

jnpr-chassis-serial—The chassis serial number.

jnpr-vcp—Juniper virtual chassis port.

port-vid—Indicates the port VLAN ID that will be associated with an untagged or priority tagged data frame received on the VLAN port.

vlan-name—Indicates the assigned name of any VLAN at the device.

The following options can be configured using **tlv-filter** at the [**edit protocols lldp-med**] and [**edit protocols lldp-med interface *interface-name***] hierarchy levels:

ext-power-via-mdi—The power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.

location-id—The physical location of the endpoint.

med-capabilities—The primary function of the port.

network-policy—The port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types, such as voice or streaming video, 802.1Q VLAN tagging, and 802.1p priority bits and Diffserv code points.

Required Privilege Level

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

Related Documentation

- show lldp on page 1826
- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

tlv-select

Syntax tlv-select *tlv-name*;

Hierarchy Level [edit protocols lldp],
[edit protocols lldp-med],
[edit protocols lldp interface *interface-name*],
[edit protocols lldp-med interface *interface-name*]

Release Information Statement introduced in Junos OS Release 18.3 for EX Series switches.

Description Select the type, length, and value (TLV) messages that should be advertised by Link Layer Discovery Protocol (LLDP) or LLDP Media Endpoint Discovery (LLEP-MED) protocol. LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include information such as chassis and port identification and system name and system capabilities.

In multi-vendor networks, it might not be desirable to send TLV messages because they can contain sensitive information about a network device. You can configure LLDP or LLDP-MED to disable any non-mandatory TLV message. Mandatory TLVs are: chassis-id, port-id, and time-to-live.

When you configure the tlv-select statement, you specify the TLVs that should be advertised by LLDP or LLDP-MED. All other non-mandatory TLVs are disabled. This is useful when you want to disable most, but not all, TLVs.

You can also disable TLVs using the tlv-filter statement. When you configure the tlv-filter statement, you specify the TLVs that should be disabled.

NOTE: **The tlv-select and tlv-filter are mutually exclusive and cannot be used on the same configuration stanza at the same time.**

Default All TLVs for LLDP and LLDP-MED are enabled by default.

Options The following options can be configured using **tlv-select** at the [**edit protocols lldp**] and [**edit protocols lldp interface *interface-name***] hierarchy levels:

port-description—The user-configured port description.

system-name—The user-configured name of the local system.

system-description—The user-configured name of the local system.

system-capabilities—The primary function performed by the system. The capabilities that system supports are defined; for example, bridge or router. This information cannot be configured, but is based on the model of the product.

management-address— IP management address of the local system.

mac-phy-config-status—Advertises information about the physical interface, such as autonegotiation status and support and MAU (medium attachment unit) type.

power-vi-mdi—Advertises MDI (media dependent interface) power support, PSE (power sourcing equipment) power pair, and power class information.

link-aggregation—Advertises whether the port is aggregated and its aggregated port ID.

maximum-frame-size—The maximum transmission unit (MTU) of the interface sending LLDP frames.

jnpr-chassis-serial—The chassis serial number.

jnpr-vcp—Juniper virtual chassis port.

port-vid—Indicates the port VLAN ID that will be associated with an untagged or priority tagged data frame received on the VLAN port.

vlan-name—Indicates the assigned name of any VLAN at the device.

The following options can be configured using **tlv-select** at the [**edit protocols lldp-med**] and [**edit protocols lldp-med interface *interface-name***] hierarchy levels:

ext-power-via-mdi—The power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.

location-id—The physical location of the endpoint.

med-capabilities—The primary function of the port.

network-policy—The port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types, such as voice or streaming video, 802.1Q VLAN tagging, and 802.1p priority bits and Diffserv code points.

Required Privilege Level

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

Related Documentation

- show lldp on page 1826
- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

token (DHCP Local Server)

Syntax

token *token-value*;

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group *group-name* reconfigure],
[edit system services dhcp-local-server dhcpv6 group *group-name* reconfigure]

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6 ...]** hierarchy levels introduced in Junos OS Release 10.4.

Description

Configure a plain-text token for all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. The token enables rudimentary entity authentication to protect against inadvertently instantiated DHCP servers. A null token (empty string) indicates that the configuration token functionality is not enabled. A group configuration takes precedence over a DHCP local server configuration. For more information about tokens, see RFC 3118, *Authentication for DHCP Messages*, section 4.

Options

token-value—Plain-text alphanumeric string.

Default: null (empty string)

Required Privilege Level

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

Related Documentation

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview on page 662
- Configuring a Token for DHCP Local Server Authentication on page 610

trace (DHCP Relay Agent)

Syntax

```
trace;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit forwarding-options dhcp-relay group group-name interface interface-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group
  group-name interface interface-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
  interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay group group-name interface interface-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group
  group-name interface interface-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group
  group-name interface interface-name]
```

Release Information

Statement introduced in Junos OS Release 10.4.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Enable trace operations for a group of interfaces or for a specific interface within a group. Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

EX Series switches do not support DHCPv6.

Required Privilege Level

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

Related Documentation

- Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure) on page 611
- *Tracing Extended DHCP Operations*
- *Tracing Extended DHCP Operations for Specific Interfaces*

traceoptions

Syntax

```
traceoptions {
  file filename <files number> <size size>;
  flag all;
  flag certificates;
  flag database;
  flag general;
  flag ike;
  flag parse;
  flag policy-manager;
  flag routing-socket;
  flag timer;
  level
  no-remote-trace
}
```

Hierarchy Level

```
[edit security],
[edit services ipsec-vpn]
```

Trace options can be configured at either the **[edit security]** or the **[edit services ipsec-vpn]** hierarchy level, but not at both levels.

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure security trace options.

To specify more than one trace option, include multiple **flag** statements. Trace option output is recorded in the **/var/log/kmd** file.

NOTE: The **traceoptionsstatement is not supported on QFabric systems.**

Options

files *number*—(Optional) Maximum number of trace files. When a trace file (for example, **kmd**) reaches its maximum size, it is renamed **kmd.0**, then **kmd.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with the **size** option.

Range: 2 through 1000 files

Default: 0 files

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, **kmd**) reaches this size, it is renamed, **kmd.0**, then **kmd.1** and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Default: 1024 KB

flag *flag*—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace all security events.
- **certificates**—Trace certificate events.
- **database**—Trace database events.
- **general**—Trace general events.
- **ike**—Trace IKE module processing.
- **parse**—Trace configuration processing.
- **policy-manager**—Trace policy manager processing.
- **routing-socket**—Trace routing socket messages.
- **timer**—Trace internal timer events.

level *level*—(Optional) Set traceoptions level.

- **all**—match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

no-remote-trace—(Optional) Disable remote tracing

Required Privilege Level

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

Related Documentation

- *Configuring Tracing Operations*

traceoptions (DNS, Port, and TFTP Packet Forwarding)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression> <size bytes> <world-readable |
    no-world-readable>;
  flag flag;
  level level;
  <no-remote-trace>;
}
```

Hierarchy Level

```
[edit forwarding-options helpers]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement standardized and **match** option introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure tracing operations for BOOTP, DNS, TFTP, or custom UDP port packet forwarding.

Default

If you do not include this statement, no tracing operations are performed.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" "). All files are placed in a file named **fud** in the directory **/var/log**. If you include the **file** statement, you must specify a filename.

files *number*—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **address**—Trace address management events
- **all**—Trace all events
- **bootp**—Trace BOOTP or DHCP services events
- **config**—Trace configuration events
- **domain**—Trace DNS service events
- **ifdb**—Trace interface database operations

- **io**—Trace I/O operations
- **main**—Trace main loop events
- **port**—Trace arbitrary protocol events
- **rtsock**—Trace routing socket operations
- **tftp**—Trace TFTP service events
- **trace**—Trace tracing operations
- **ui**—Trace user interface operations
- **util**—Trace miscellaneous utility operations

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—(Optional) Disable remote tracing globally or for a specific tracing operation.

no-world-readable—(Optional) Restrict file access to the owner.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** file again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and filename.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

Range: 0 bytes through 4,294,967,295 KB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

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

Related Documentation

- *Tracing BOOTP, DNS, and TFTP Forwarding Operations*

traceoptions (802.1X)

Syntax

```
traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable> <match
    regex>;
  flag flag;
}
```

Hierarchy Level

```
[edit protocols dot1x]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **dot1x-event** and **dot1x-ipc** options introduced in Junos OS Release 13.2X50 for EX Series switches.

Description

Define tracing operations for the 802.1X protocol.

Default

Tracing operations are disabled.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size by using the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- **all**—All tracing operations.
- **config-internal**—Trace internal configuration operations.
- **dot1x-event**—(Switches with ELS only) Trace 802.1x events.
- **dot1x-debug**—(Switches without ELS) Trace 802.1x events.
- **dot1x-ipc**—(Switches with ELS only) Trace IPC interactions.
- **eapol**—Trace EAPOL packets transmitted and received.
- **esw-if**—(Switches without ELS) Trace ESW interactions.
- **general**—Trace general operations.
- **normal**—Trace normal operations.

- **parse**—Trace reading of the configuration.
- **regex-parse**—Trace regular-expression parsing operations.
- **state**—Trace protocol state changes.
- **task**—Trace protocol task operations.
- **timer**—Trace protocol timer operations.
- **vlan**—Trace VLAN transactions.

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

no-world-readable—(Optional) Restrict file access to the user who created the file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files with the **files** option, you also must specify a maximum file size.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

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

Related Documentation

- show lldp on page 1826
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- 802.1X for Switches Overview on page 289

traceoptions (Address-Assignment Pool)

Syntax

```
traceoptions {
  file filename {
    files number;
    size maximum-file-size;
    match regex;
    (world-readable | no-world-readable);
  }
  flag address-assignment;
  flag all;
  flag configuration;
  flag framework;
  flag ldap;
  flag local-authentication;
  flag radius;
}
```

Hierarchy Level

```
[edit system processes general-authentication-service]
```

Release Information

Flag for tracing address-assignment pool operations introduced in Junos OS Release 9.0.
option-name option introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure tracing options.

Options

file ***filename***—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory **/var/log**.

files ***number***—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000

Default: 3 files

flag ***flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **address-assignment**—All address-assignment events
- **all**—All tracing operations
- **configuration**—Configuration events
- **framework**—Authentication framework events

- **ldap**—LDAP authentication events
- **local-authentication**—Local authentication events
- **radius**—RADIUS authentication events

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

no-world-readable—(Optional) Restrict access to the originator of the trace operation only.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and filename.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

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

Related Documentation

- *Address-Assignment Pool Configuration Overview*

traceoptions (DHCP)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  level  (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

Hierarchy Level

```
[edit system processes dhcp-service]
[edit security dynamic-address]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 18.4R1.

Description

Define global tracing operations for extended DHCP local server and extended DHCP relay agent processes.

This statement replaces the deprecated **traceoptions** statements at the **[edit forwarding-options dhcp-relay]** and **[edit system services dhcp-local-server]** hierarchy levels.

NOTE: Traceoptions does not differentiate between a logical system and tenant system, and can be configured under the root logical system.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements:

- **all**—Trace all events.
- **auth**—Trace authentication events.
- **database**—Trace database events.
- **fwd**—Trace firewall process events.

- **general**—Trace miscellaneous events.
- **ha**—Trace high availability-related events.
- **interface**—Trace interface operations.
- **io**—Trace I/O operations.
- **liveness-detection**—Trace liveness detection operations.
- **packet**—Trace packet and option decoding operations.
- **performance**—Trace performance measurement operations.
- **profile**—Trace profile operations.
- **rpd**—Trace routing protocol process events.
- **rtsock**—Trace routing socket operations.
- **security-persistence**—Trace security persistence events.
- **session-db**—Trace session database events.
- **state**—Trace changes in state.
- **statistics**—Trace baseline statistics.
- **ui**—Trace user interface operations.

level—Level of tracing to perform; also known as severity level. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

- **all**—Match messages of all levels.
- **error**—Match error messages.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure **verbose**, messages at all higher levels are traced. Therefore, the result is the same as when you configure **all**.
- **warning**—Match warning messages.

Default: error

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access, allowing only the user **root** and users who have the Junos OS **maintenance** permission to access the trace files.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (***maximum-file-size***k), megabytes (***maximum-file-size***m), or gigabytes (***maximum-file-size***g). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Range: 10,240 through 1,073,741,824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

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

Related Documentation

- *Tracing Extended DHCP Operations*

traceoptions (DHCP Server)

Syntax

```
traceoptions {
  file filename <files number> <match regex> <size size> <world-readable |
    no-world-readable>;
  flag flag;
}
```

Hierarchy Level

[edit system services dhcp]

Release Information

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

Description

Define tracing operations for DHCP processes.

Options

file ***filename***—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory **/var/log**.

files ***number***—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000

Default: 3 files

flag ***flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—All tracing operations
- **binding**—Trace binding operations
- **config**—Log reading of configuration
- **conflict**—Trace user-detected conflicts for IP addresses
- **event**—Trace important events
- **ifdb**—Trace interface database operations
- **io**— Trace I/O operations
- **lease**—Trace lease operations
- **main**—Trace main loop operations
- **misc**— Trace miscellaneous operations
- **packet**—Trace DHCP packets

- **options**—Trace DHCP options
- **pool**—Trace address pool operations
- **protocol**—Trace protocol operations
- **rtsock**—Trace routing socket operations
- **scope**—Trace scope operations
- **signal**—Trace DHCP signal operations
- **trace**—All tracing operations
- **ui**—Trace user interface operations

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

- **all**—All tracing operations
- **binding**—Trace binding operations
- **config**— Log reading of configuration
- **conflict**—Trace user-detected conflicts for IP addresses
- **event**—Trace important events
- **ifdb**— Trace interface database operations
- **io**—Trace I/O operations
- **lease**—Trace lease operations
- **main**—Trace main loop operations
- **match *regex***— Refine the output to include lines that contain the regular expression.
- **misc**—Trace miscellaneous operations
- **packet**—Trace DHCP packets
- **options**—Trace DHCP options
- **pool**—Trace address pool operations
- **protocol**—Trace protocol operations
- **rtsock**—Trace routing socket operations
- **scope**—Trace scope operations
- **signal**—Trace DHCP signal operations
- **trace**—All tracing operations
- **ui**—Trace user interface operations

no-world-readable—(Optional) Disable unrestricted file access.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the ***trace-file*** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and filename.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

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

Related Documentation

- Configuring Tracing Operations for DHCP Processes on page 557
- *System Management Configuration Statements*

traceoptions (LLDP)

Syntax

```
traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable> <no-stamp>
    <replace>;
  flag flag <disable>;
}
```

Hierarchy Level

```
[edit protocols lldp]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Define tracing operations for the Link Layer Discovery Protocol (LLDP). You can trace messages under LLDP for LLDP and PTOPO MIBs.

NOTE: The traceoptions statement is not supported on the QFX3000 QFabric system.

Default

Tracing operations are disabled.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- **all**—All tracing operations.
- **configuration**—Trace configuration operations.
- **interface**—Trace interface update events.
- **netbios**—Trace NetBIOS events.

- **packet**—Trace packet events.
- **rtsock**—Trace routing socket operations.
- **snmp**—Trace SNMP configuration operations.
- **vlan**—Trace VLAN update events.

no-stamp—(Optional) Do not timestamp the trace file.

Default: If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

no-world-readable—(Optional) Restrict file access to the user who created the file.

replace—(Optional) Replace an existing trace file if there is one rather than appending output to it.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **files** option.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

Default: If you do not include this option, tracing output is appended to an existing trace file.

world-readable—(Optional) Enable unrestricted file access.

NOTE: **The traceoptions statement is not supported on the QFX3000 QFabric system.**

Required Privilege Level

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

Related Documentation

- Configuring LLDP-MED (CLI Procedure) on page 521
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518
- Understanding LLDP on page 511

traceoptions (Outbound SSH)

Syntax

```
traceoptions {
  file {
    filename ;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level

```
[edit system services outbound-ssh]
```

Release Information Statement introduced in Junos OS Release 10.4.

Description Set the trace options.

Options

- **file**—Configure the trace file information.
  - **filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files** *number*—Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed to**trace-file.0** , then **trace-file.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match** ***regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size** ***maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Syntax: x K to specify KB, x m to specify MB, or x g to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Specify the tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags.
  - **all**—Trace all events.
  - **configuration**—Trace configuration events.
  - **connectivity**—Trace TCP connection handling.
- **no-remote-trace**—Disable remote tracing.

Required Privilege Level

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

Related Documentation

- *Displaying Log and Trace Files*

traceoptions (SBC Configuration Process)

Syntax

```
traceoptions {
  file filename <files number> <match regex> <size size>
    <world-readable | no-world-readable>;
  flag flag;
}
```

Hierarchy Level

```
[edit system processes sbc-configuration-process]
```

Release Information

Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 9.5 for EX Series switches.

Description

Configure trace options for the session border controller (SBC) process of the border signaling gateway (BSG).

Options

file *filename*—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory **/var/log**. You can include the following file options:

- **files *number***—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

  If you specify a maximum number of files, you must also specify a maximum file size with the **size** option and a filename.

  Range: 2 through 1000

  Default: 3 files

- **match *regex***—(Optional) Refine the output to include lines that contain the regular expression.
- **no-world-readable**—(Optional) Disable unrestricted file access.
- **size *size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the trace-file again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

  Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB.

  Range: 10 KB through 1 GB

  Default: 128 KB

- **world-readable**—(Optional) Enable unrestricted file access.

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all *trace-level***—Trace all SBC process operations.
- **common *trace-level***—Trace common events.
- **configuration *trace-level***—Trace configuration events.
- **device-monitor *trace-level***—Trace device monitor events.
- **ipc *trace-level***—Trace IPC events.
- **memory—pool *trace-level***—Trace memory pool events.
- ***trace-level***—Trace level options are related to the severity of the event being traced. When you choose a trace level, messages at that level and higher levels are captured. Enter one of the following trace levels as the ***trace-level***:
  - **debug**—Log all code flow of control.
  - **error**—Log failures with a short-term effect.
  - **info**—Log summary for normal operations, such as the policy decisions made for a call.
  - **trace**—Log program trace START and EXIT macros.
  - **warning**—Log failure recovery events or failure of an external entity.
- **ui *trace-level***—Trace user interface operations.

Required Privilege Level

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

Related Documentation

- See “Troubleshooting the IMSG” in the *Junos Multiplay Solutions Guide*
- *System Management Configuration Statements*

transfer-interval

Syntax transfer-interval *minutes*;

Hierarchy Level [edit accounting-options file *filename*]

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 length of time the file remains open and receives new statistics before it is closed and transferred to an archive site.

Options ***minutes***—Time the file remains open and receives new statistics before it is closed and transferred to an archive site.

Range: 5 through 2880 minutes

Default: 30 minutes

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

Related Documentation

- *Configuring the Transfer Interval of the File*

transmit-interval

Syntax

```
transmit-interval {
  threshold milliseconds;
  minimum-interval milliseconds;
}
```

Hierarchy Level

[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group *group-name* liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group *group-name* liveness-detection method bfd],
[edit forwarding-options dhcp-relay group *group-name* liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name* liveness-detection method bfd]

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the Bidirectional Forwarding Detection (BFD) transmit interval.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677

transmit-period

Syntax transmit-period *seconds*;

Hierarchy Level [edit protocols dot1x authenticator interface (802.1X) (all | [*interface-name*])

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description For 802.1X authentication, how long the port waits before retransmitting the initial EAPOL PDUs to the supplicant.

Default 30 seconds

Options *seconds*—Number of seconds the port waits before retransmitting the initial EAPOL PDUs to the supplicant.

Range: 1 through 65,535 seconds

Default: 30 seconds

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

Related Documentation

- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- 802.1X for Switches Overview on page 289

transmit-delay

Syntax transmit-delay *seconds*;

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 11.1 for EX Series switches.

Description Specify the number of seconds the device delays before sending advertisements to neighbors after a change is made in a TLV (type, length, or value) element in the Link Layer Discovery Protocol (LLDP) or in the state of the local system, such as a change in hostname or management address. You can set this value to reduce the delay in notifying neighbors of a change in the local system.

The **advertisement-interval** value must be greater than or equal to four times the **transmit-delay** value, or an error will be returned when you attempt to commit the configuration.

Default Enabled

Options *seconds*—Delay after a change to the local TLVs or system state before LLDP advertisements are sent.

Range: 1 through 8192 seconds

Default:

- 2 seconds if the **advertisement-interval** value is set to 8 seconds or more
- 1 second if the **advertisement-interval** value is set to less than 8 seconds

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

Related Documentation

- show lldp on page 1826
- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

trap-group

List of Syntax

Syntax: MX, M, T, ACX and PTX Series routers, OCX1100, EX and QFX Series Switches and SRX and vSRX firewalls on page 1571
Syntax: QFX and EX Series Switches and OCX1100 on page 1571

Syntax: MX, M, T, ACX and PTX Series routers, OCX1100, EX and QFX Series Switches and SRX and vSRX firewalls

```
trap-group group-name {
  categories {
    category;
  }
  destination-port port-number;
  routing-instance instance;
  targets {
    address;
  }
  version (all | v1 | v2);
}
```

Syntax: QFX and EX Series Switches and OCX1100

```
trap-group group-name {
  categories {
    category;
  }
  destination-port port-number;
  targets {
    address;
  }
}
```

Hierarchy Level

[edit snmp]

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers, and SRX and vSRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for QFX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Create a named group of hosts to receive the specified trap notifications. The name of the trap group is embedded in SNMP trap notification packets as one variable binding (varbind) known as the community name. At least one trap group must be configured for SNMP traps to be sent.

Options

group-name—Name of the trap group. If the name includes spaces, enclose it in quotation marks (" ").

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring SNMP Trap Groups*
- *Configuring SNMP Trap Groups*

trap-options

List of Syntax

Syntax: MX, M, T, ACX and PTX Series Routers, EX Series Switches and SRX Firewalls on page 1573
QFX Series Switches, EX4600, OCX1100 on page 1573

Syntax: MX, M, T, ACX and PTX Series Routers, EX Series Switches and SRX Firewalls

```
trap-options {
  agent-address outgoing-interface;
  context-oid;
  enterprise-oid;
  logical-system logical-system-name {
    routing-instance routing-instance-name {
      source-address address;
    }
  }
  routing-instance routing-instance-name {
    source-address address;
  }
}
```

QFX Series Switches, EX4600, OCX1100

```
trap-options {
  agent-address outgoing-interface;
  source-address address;
}
```

Hierarchy Level

[edit snmp]

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series Routers, and SRX Firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
context-oid option introduced in Junos OS Release 17.1.

Description

Using SNMP trap options, you can set the source address of every SNMP trap packet sent by the router or switch to a single address, regardless of the outgoing interface. In addition, you can set the agent address of each SNMPv1 trap. For more information about the contents of SNMPv1 traps, see RFC 1157.

Default

Disabled

Options

context-oid—Add context oid in varbind of all traps originating from non-default logical system and routing instance. If your network management system is not able to handle prefixes such as **<routing-instance name>@<trap-group-name>** or **<logical-system name>/<routing-instance name>@<trap-group-name>**, setting the

context-oid configuration statement will send only the **<trap-group-name>** and add **<logical-system name>/<routing-instance name>** as an additional varbind.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring SNMP Trap Options*

trigger (DHCP Local Server)

Syntax

```
trigger {
  radius-disconnect;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* reconfigure],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* reconfigure],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* reconfigure],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group *group-name* reconfigure],
[edit system services dhcp-local-server dhcpv6 group *group-name* reconfigure]

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6 ...]** hierarchy levels introduced in Junos OS Release 10.4.

Description

Configure behavior in response to a trigger for all DHCP clients or only the DHCP clients serviced by the specified group of interfaces.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview on page 662

- Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 666
- radius-disconnect on page 1377

tries-before-disconnect

Syntax tries-before-disconnect *number*;

Hierarchy Level [edit system login retry-options]

Release Information Statement introduced in Junos OS Release 8.0.

Description Configure the maximum number of times the user is allowed to enter a password to attempt to log in to the router through SSH or Telnet.

Options *number*—Maximum number of times a user is allowed to attempt to enter a password to log in through SSH or Telnet.

Range: 1 through 10

Default: 10

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

Related Documentation

- Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 60
- retry-options on page 1428

trust-option-82

Syntax

```
trust-option-82;
```

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* interface *interface-name* overrides]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Enable processing of DHCP client packets that have a gateway IP address (giaddr) of 0 (zero) and contain option 82 information. By default, the DHCP relay agent treats such packets as if they originated at an untrusted source, and drops them without further processing.

Required Privilege Level

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

Related Documentation

- Enable Processing of Untrusted Packets So Option 82 Information Can Be Used on page 642
- Overriding the Default DHCP Relay Configuration Settings on page 627

trusted-key

Syntax trusted-key [*key-numbers*];

Hierarchy Level [edit system *ntp*]

Release Information Statement introduced before Junos OS Release 7.4.

Description For NTP, configure the keys you are allowed to use when you configure the SRX Series device to synchronize its time with other systems on the network.

Options **key-numbers**—One or more key numbers. Each key can be any 32-bit unsigned integer except 0.

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

Related Documentation
- *ntp*

uac-policy

Syntax uac-policy;

Hierarchy Level [edit ethernet-switching-options]

Release Information Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description Configure Junos Pulse Access Control Service as the access policy to authenticate and authorize users connected to the switch for admission to the network and for access to protected network resources.

Default The Access Control Service access policy is disabled.

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

Related Documentation
- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 401
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 404

uac-policy (MX Series in Enhanced LAN Mode)

Syntax

```
uac-policy;
```

Hierarchy Level

```
[edit protocols authentication-access-control]
```

Release Information

Statement introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description

Configure Junos Pulse Access Control Service as the access policy to authenticate and authorize users connected to the switch for admission to the network and for access to protected network resources.

Default

The Access Control Service access policy is disabled.

Required Privilege Level

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

Related Documentation

uac-service

Syntax

```
uac-service {
  timeout {
timeout-action {
```

Hierarchy Level

```
[edit system processes]
```

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Configure Junos Pulse Access Control Service as one of the system processes.

Default

Junos Pulse Access Control Service process is disabled.

Required Privilege Level

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

Related Documentation

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 401
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 404
- Understanding Centralized Network Access Control and EX Series Switches on page 399

uac-service

Syntax

```
uac-service {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the unified access control daemon process.

Options

- **command** ***binary-file-path***—Path to the binary process.
- **disable**—Disable the unified access control daemon process.
- **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
  - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
  - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

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

Related Documentation

- *Firewall User Authentication Overview*

uid

Syntax uid *uid-value*;

Hierarchy Level [edit system login user]

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

Description Numeric identifier associated with the user account name, either assigned by an administrator or assigned automatically when you commit the user configuration. It is used by applications that request numeric identifiers, such as some RADIUS queries or secure applications such as flow-tap monitoring.

Options ***uid-value***—Number associated with the login account. This value must be unique on the router or switch.

Range: 100 through 64000

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

Related Documentation

- Configuring Junos OS User Accounts by Using a Configuration Group on page 76

unattended-boot

Syntax unattended-boot;

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 13.2X51-D20 for EX Series switches.

Description Set the switch to unattended mode for U-Boot to prevent unauthorized access to the system before the JUNOS OS login prompt appears. In unattended mode, access to the loader CLI is blocked, as well as recovery mechanisms such as password recovery by using single-user mode and booting the switch by using a USB flash drive. In order to access the CLI in U-Boot mode, the user must enter a boot-loader password that has been previously configured.

NOTE: If the root password is lost while the switch is in unattended mode, the switch must be reset to the factory default configuration using the LCD panel. For more information see *Reverting to the Default Factory Configuration for the EX Series Switch*.

Default Unattended mode is not enabled by default.

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

Related Documentation

- Using Unattended Mode for U-Boot to Prevent Unauthorized Access on page 280
- boot-loader-authentication on page 911

unified-access-control

Syntax

```
unified-access-control {
  infranet-controllerhostname {
    address ip-address;
    interface interface-name;
    password password;
    port port-number;
  }
```

Hierarchy Level [edit services]

Release Information Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description Configure Junos Pulse Access Control Service to authenticate and authorize users connected to the switch for admission to the network and for access to protected network resources.

The remaining statements are explained separately. See CLI Explorer.

Default Junos Pulse Access Control Service is disabled.

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

Related Documentation

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 401
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 404

update-interval

Syntax update-interval *minutes*;

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

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

Description Enable interim accounting updates and configure the amount of time that the router or switch waits before sending a new accounting update.

Interim accounting updates are included in the exchange of messages between the client and the accounting server. In RADIUS accounting, the client is the network access server (NAS), which can be the router or switch. The NAS sends Accounting-Request messages to the server, which acknowledges receipt of the requests with Accounting-Response messages. Interim accounting updates are sent in Accounting-Request packets with the Acct-Status-Type attribute set to Interim-Update.

When a user is authenticated, the authentication server issues an Access-Accept message in response to a successful Access-Request message. The interval between interim updates can be configured directly on the server using the Acct-Interim-Interval attribute of the Access-Accept message. However, if the update interval is configured on the NAS using **update-interval**, then the locally configured value overrides the value found in an Access-Accept message from the server.

NOTE: **All information in an interim update message is cumulative from the beginning of the session, not from the last interim update message.**

Default No interim updates are sent from the client to the accounting server.

Options ***minutes***—Amount of time between updates, in minutes. All values are rounded 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

- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications*

update-router-advertisement

Syntax

```
update-router-advertisement (interface interface-name);
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
  family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6
  dhcpv6-client]
```

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.
The **logical-systems** and **tenant** options are introduced in Junos OS Release 18.4R1.

Description

Specify the interface used to delegate prefixes.

Options

interface *interface-name*—Interface on which to delegate prefixes

Required Privilege Level

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

Related Documentation

update-server

Syntax

```
update-server;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet dhcp]
```

Release Information

Statement introduced in Junos OS Release 8.5 for J Series devices.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.2 for SRX Series devices.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Propagate TCP/IP settings learned from an external DHCP server to the DHCP server running on the switch, router, or device.

Required Privilege Level

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

Related Documentation

- Configuring a DHCP Client (CLI Procedure) on page 591
- Example: Configuring the Device as a DHCP Client on page 737
- *interfaces*
- *unit*
- *family*

update-server (dhcp-client)

Syntax
```
update-server;
```

Hierarchy Level
```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client]
```

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option **dhcp-clinet** at **[edit interfaces interface-name unit logical-unit-number family inet]** hierarchy is changed to **dhcp** to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option **dhcp**.

Description
Propagate DHCP options to a local DHCP server.

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

Related Documentation

update-server (dhcpv6-client)

Syntax
```
update-server;
```

Hierarchy Level
```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
```

Release Information
Statement introduced in Junos OS Release 12.1X45-D10 for SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

Description
Propagate TCP/IP settings to the DHCPv6 server.

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

Related Documentation

use-interface

Syntax

```
use-interface-description {logical |device};
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client
  client-identifier]
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description

The description configured at the physical or logical interface level is used for client identification.

Required Privilege Level

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

Related Documentation

use-interface-description

Syntax

```
use-interface-description (logical | device);
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id |
  relay-agent-remote-id)],
[edit forwarding-options dhcp-relay dhcpv6 group group-name (relay-agent-interface-id |
  relay-agent-remote-id)],
[edit forwarding-options dhcp-relay relay-option-82 (circuit-id | remote-id)],
[edit forwarding-options dhcp-relay group group-name relay-option-82 (circuit-id |
  remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay dhcpv6
  (relay-agent-interface-id | relay-agent-remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay ... relay-option-82
  (circuit-id | remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6
  (relay-agent-interface-id | relay-agent-remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...
  relay-option-82 (circuit-id | remote-id)],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-18],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-37]
```

Release Information

Statement introduced in Junos OS Release 9.6.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.
Support at the **[edit ... relay-agent-remote-id]** and **[edit ... remote-id]** hierarchy levels introduced in Junos OS Release 14.1.
Support at the **[edit vlans *vlan-name* dhcp-security dhcpv6-options option-18]** and **[edit vlans *vlan-name* dhcp-security dhcpv6-options option-37]** hierarchy levels introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description

Use the textual interface description instead of the interface identifier in the DHCP base option 82 Agent Circuit ID (suboption 1) or Agent Remote ID (suboption 2) information, or in the DHCPv6 option 18 (Relay Agent Interface ID) or option 37 (Relay Agent Remote ID) information in DHCP packets that the DHCP relay agent sends to a DHCP server.

NOTE: For integrated routing and bridging (IRB) interfaces, the option 82 field must be able to uniquely identify the incoming interface based on either the Agent Circuit ID or Agent Remote ID. You can modify the information in the textual interface description to match the raw IFD (physical interface without a subunit) name and configure the option 82 field to use the interface description.

The textual description is configured using the **description** statement at the **[edit interfaces *interface-name*]** hierarchy level. If you specify that the textual description be used and no description is configured for the interface, DHCP relay defaults to using the Layer 2

interface name. When you use the interface description rather than the interface name, the interface description has to be specified under interface unit ("set interfaces ge-0/0/0 unit 0 description "client"). If you do not do this, then the interface name is used.

In the case of integrated routing and bridging (IRB) interfaces, the textual description of the Layer 2 interface is used instead of the IRB interface. If there is no description configured, the Layer 2 logical interface name is used. To include the IRB interface description instead of the Layer 2 interface description, configure the **use-interface-description** and the **no-vlan-interface-name** statements. If no description is configured for the IRB interface, DHCP relay defaults to using the IRB interface name.

NOTE: The use-interface-description statement is mutually exclusive with the use-vlan-id statement.

If you specify the textual interface description, rather than accepting the default syntax, the identification is for packets returned from the server, and only for instances where that identification would be required by the DHCP relay, such as a stateless pass-through.

NOTE: By default, DHCP relay accepts a maximum of 253 ASCII characters. If the textual interface description exceeds 253 characters, DHCP relay drops the packet, which results in the DHCP client failing to bind.

Options

logical—Use the textual description that is configured for the logical interface.

device—Use the textual description that is configured for the device interface.

Required Privilege Level

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

Related Documentation

- *Including a Textual Description in DHCP Options*
- Using DHCP Relay Agent Option 82 Information on page 633
- *Configuring DHCPv6 Relay Agent Options*

use-primary (DHCP Local Server)

Syntax

use-primary *primary-profile-name*;

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* system services dhcp-local-server dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* dynamic-profile *profile-name*],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dynamic-profile *profile-name*],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* dynamic-profile *profile-name*],
[edit system services dhcp-local-server dynamic-profile *profile-name*],
[edit system services dhcp-local-server group *group-name* dynamic-profile *profile-name*]

Release Information

Statement introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the dynamic profile to configure as the primary dynamic profile. The primary dynamic profile is instantiated when the first subscriber or DHCP client logs in. Subsequent subscribers (or clients) are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber (or client) logs out, the next subscriber (or client) that logs in is assigned the primary dynamic profile.

Options

primary-profile-name—Name of the dynamic profile to configure as the primary dynamic profile

Required Privilege Level

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

Related Documentation

- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*

use-primary (DHCP Relay Agent)

Syntax

use-primary *primary-profile-name*;

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 dynamic-profile *profile-name*],
[edit forwarding-options dhcp-relay dynamic-profile *profile-name*],
[edit forwarding-options dhcp-relay dhcpv6 group *group-name* dynamic-profile *profile-name*],
[edit forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name* dynamic-profile *profile-name*],
[edit forwarding-options dhcp-relay group *group-name* dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay dhcpv6 group *group-name* dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* dynamic-profile *profile-name*],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 dynamic-profile *profile-name*],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dynamic-profile *profile-name*],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 group *group-name* dynamic-profile *profile-name*],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* dynamic-profile *profile-name*]

Release Information

Statement introduced in Junos OS Release 9.3.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Support at the **[edit ... dual-stack-group *dual-stack-group-name*]** hierarchy level introduced in Junos OS Release 15.1.

Description

Specify the dynamic profile to configure as the primary dynamic profile. The primary dynamic profile is instantiated when the first subscriber logs in. Subsequent subscribers are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber logs out, the next subscriber that logs in is assigned the primary dynamic profile.

Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

EX Series switches do not support DHCPv6.

Options ***primary-profile-name***—Name of the dynamic profile to configure as the primary dynamic profile

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

Related Documentation
- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*

use-vlan-id

Syntax

```
use-vlan-id;
```

For Platforms with Enhanced Layer 2 Software (ELS)

```
[edit forwarding-options helpers bootp dhcp-option82-circuit-id]
[edit forwarding-options helpers bootp interface interface-name dhcp-option82-circuit-id]
```

For MX Series Platforms

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security option-82
  circuit-id]
```

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Hierarchy level **[edit vlans *vlan-name* forwarding-options dhcp-security]** introduced in Junos OS Release 13.2X50-D10. (See *Using the Enhanced Layer 2 Software CLI* for information about ELS.)
Hierarchy level **[edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]** introduced in Junos OS Release 14.1 for the MX Series.

NOTE: The EX Series switches that support the **use-vlan-id** statement are the EX4300, EX4600, and EX9200 switches.

Description

Use the VLAN ID rather than the VLAN name (the default) in the circuit ID or remote ID value in the DHCP option 82 information.

NOTE: The **use-vlan-id** statement is mutually exclusive with the **use-interface-description** and **no-vlan-interface-name** statements.

The **use-vlan-id** statement only applies to interfaces in a bridge domain. The format of the Agent Circuit ID or Agent Remote ID information for Fast Ethernet or Gigabit Ethernet interfaces is as follows:

```
(fe | ge)-fpc/pic/port.subunit:svlan_id-vlan_id
```

NOTE: The *subunit* is required and used to differentiate the interface for remote systems, and *svlan_id-vlan_id* represents the VLANs associated with the bridge domain.

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

Related Documentation
- *Example: Setting Up DHCP Option 82 Using the Same VLAN*
- *Example: Setting Up DHCP Option 82*
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

user (Access)

Syntax

```
user username {
  authentication {
    (encrypted-password "password" | plain-text-password);
    load-key-file URL;
    remote-debug-permission (qfabric-admin | qfabric-operator |qfabric-user);
    ssh-dsa "public-key" <from hostname>;
    ssh-rsa "public-key" <from hostname>;
  }
  class class-name;
  full-name "complete-name";
  uid uid-value;
}
```

Hierarchy Level
[edit system login]

Release Information
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Configure access permission for individual users.

Options
The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation
- *Configuring Junos OS User Accounts*
- class on page 943

user (Access)

Syntax

```
user username {
  authentication {
  cli {
    prompt name;
  }
  class class-name;
  (encrypted-password "password" | plain-text-password);
  full-name complete-name;
  load-key-file URL filename;
  ssh-dsa “public-key” <from hostname>;
  ssh-rsa “public-key” <from hostname>;
  uid uid-value;
  }
}
```

Hierarchy Level

```
[edit system login]
```

Release Information

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

Description

Configure access permission for individual users. Starting in Junos OS Release 18.3R1, the **ssh-dsa** hostkey algorithm is deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Options

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Configuring Junos OS User Accounts by Using a Configuration Group on page 76
- class on page 941

user-defined-option-82

Syntax

```
user-defined-option-82 string;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides
  user-defined-option82 string],
[edit forwarding-options dhcp-relay group group-name overrides user-defined-option82
  string],
[edit forwarding-options dhcp-relay overrides user-defined-option82 string]
```

Release Information

Statement introduced in Junos OS Release 17.2 for QFX Series switches.

Description

Configure a custom text string to use as the interface description in the DHCP option 82 Agent Circuit ID (suboption 1) information. This text string is defined independently of the interface description that is configured using the **description** statement at the **[edit interfaces *interface-name*]** hierarchy level.

The custom text string is configured using the **user-defined-option-82** statement at the following hierarchy levels:

- To configure a custom string on an interface level:

  ```
  [edit forwarding-options dhcp-relay group group-name interface interface-name overrides
    user-defined-option82 string]
  ```

- To configure a custom string at the group level:

  ```
  [edit forwarding-options dhcp-relay group group-name overrides user-defined-option82
    string]
  ```

- To configure a custom string globally:

  ```
  [edit forwarding-options dhcp-relay overrides user-defined-option82 string]
  ```

You can define a custom string up to 251 characters in length. To include the custom string in the DHCP option 82 Agent Circuit ID, you must configure the **user-defined** statement at the **[edit forwarding-options dhcp-relay group *group-name* relay-option-82 circuit-id]** hierarchy level.

Required Privilege Level

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

Related Documentation

- *Including a Textual Description in DHCP Options*
- Using DHCP Relay Agent Option 82 Information on page 633

user-id

Syntax

```
user-id {ascii ascii hexadecimal hexadecimal};
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client
  client-identifier]
```

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Specify an ASCII or hexadecimal user ID for the Dynamic Host Configuration Protocol (DHCP) client.

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

Related Documentation

usb-control

Syntax

```
usb-control {
  command binary-file-path;
  disable;
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information Statement introduced in Junos OS Release 8.5 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Description Specify the universal serial bus (USB) supervise process.

Options

- **command *binary-file-path***—Path to the binary process.
- **disable**—Disable the universal serial bus (USB) supervise process.

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

user-keepalive

Syntax user-keepalive *minutes*;

Hierarchy Level [edit services captive-portal interface (all | *interface-names*)]

Release Information Statement introduced in Junos OS Release 16.1 for EX Series switches.

Description The **user-keepalive** statement is used to extend a captive portal authentication session after the MAC table aging timer expires. The keep-alive timer is started when the MAC address of the authenticated host ages out of the Ethernet switching table. If traffic is received within the keep-alive timeout period, the timer is deleted. If there is no traffic within the keep-alive timeout period, the session is deleted, and the host must re-authenticate.

Default Disabled. The captive portal authentication session ends when the associated MAC address ages out of the Ethernet switching table.

Options ***minutes***—Duration of keep-alive period.

Range: 7 through 65535

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

Related Documentation

- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378
- Understanding Authentication Session Timeout on page 276

user-prefix (DHCP Local Server)

Syntax

user-prefix *user-prefix-string*;

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the user prefix that is concatenated with the username during the subscriber authentication or DHCP client authentication process.

Options

user-prefix-string—User prefix string.

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

Related Documentation
- Using External AAA Authentication Services with DHCP on page 651

username-include (DHCP Local Server)

Syntax

```
username-include {
  circuit-type;
  client-id;
  delimiter delimiter-character;
  domain-name domain-name-string;
  interface-description  (device-interface | logical-interface);
  interface-name;
  logical-system-name;
  mac-address;
  option-60;
  option-82 <circuit-id> <remote-id>;
  relay-agent-interface-id;
  relay-agent-remote-id;
  relay-agent-subscriber-id;
  routing-instance-name;
  user-prefix user-prefix-string;
  vlan-tags;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
  services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...],
[edit system services dhcp-local-server authentication],
[edit system services dhcp-local-server dhcpv6 authentication],
[edit system services dhcp-local-server dhcpv6 group group-name authentication],
[edit system services dhcp-local-server group group-name authentication]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
vlan-tags option added in Junos OS Release 18.3R1 on MX Series routers.

Description

Configure the username that the router or switch passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router (or switch) accesses the local authentication service only and does not use external authentication services, such as RADIUS.

The following statements are not supported in the DHCPv6 hierarchy levels:

- **option-60**
- **option-82**

The following statements are supported in the DHCPv6 hierarchy levels only:

- **client-id**
- **relay-agent-interface-id**
- **relay-agent-remote-id**

- **relay-agent-subscriber-id**

Options

vlan-tags—Include the subscriber session VLAN tags in the username for interactions with an external authority. Both single-tagged and double-tagged VLANs are supported: The tags are added in the format ***outer-vlan-tag-inner-vlan-tag***. The outer tag is always included; the inner tag is included for double-tagged VLANs.

Use this option instead of the **interface-name** option when the outer VLAN tag is unique across the system and you do not need the underlying physical interface name to be part of the format.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Using External AAA Authentication Services with DHCP on page 651
- Creating Unique Usernames for DHCP Clients on page 653

username-include (DHCP Relay Agent)

Syntax

```
username-include {
  circuit-type;
  client-id;
  delimiter delimiter-character;
  domain-name domain-name-string;
  interface-description  (device-interface | logical-interface);
  interface-name;
  logical-system-name;
  mac-address;
  option-60;
  option-82 <circuit-id> <remote-id>;
  relay-agent-interface-id;
  relay-agent-remote-id;
  relay-agent-subscriber-id;
  routing-instance-name;
  user-prefix user-prefix-string;
  vlan-tags;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay authentication],
[edit forwarding-options dhcp-relay dhcpv6 authentication],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication],
[edit forwarding-options dhcp-relay group group-name authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the **[edit ... dhcpv6]** hierarchy levels introduced in Junos OS Release 11.4.
Support at the **[edit ... dual-stack-group *dual-stack-group-name*]** hierarchy level introduced in Junos OS Release 15.1.
vlan-tags option added in Junos OS Release 18.3R1 on MX Series routers.

Description

Configure the username that the router (or switch) passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router (or switch) accesses the local authentication service only and does not use external authentication services, such as RADIUS. Use the statement at the **[edit...dhcpv6]** hierarchy levels to configure DHCPv6 support.

The following statements are not supported in the DHCPv6 hierarchy levels:

- **option-60**
- **option-82**

The following statements are supported in the DHCPv6 hierarchy levels only:

- **client-id**
- **relay-agent-interface-id**
- **relay-agent-remote-id**
- **relay-agent-subscriber-id**

Options

vlan-tags—Include the subscriber session VLAN tags in the username for interactions with an external authority. Both single-tagged and double-tagged VLANs are supported: The tags are added in the format ***outer-vlan-tag-inner-vlan-tag***. The outer tag is always included; the inner tag is included for double-tagged VLANs.

Use this option instead of the **interface-name** option when the outer VLAN tag is unique across the system and you do not need the underlying physical interface name to be part of the format.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Creating Unique Usernames for DHCP Clients on page 653
- Using External AAA Authentication Services with DHCP on page 651

vendor-id

Syntax vendor-id *vendor-id*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option **dhcp-clinet** at **[edit interfaces interface-name unit logical-unit-number family inet]** hierarchy is changed to **dhcp** to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option **dhcp**.

Description Configure a vendor class ID for the Dynamic Host Configuration Protocol (DHCP) client.

Options **vendor-id**—Vendor class ID.

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

Related Documentation

vendor-option

Syntax

```
vendor-option {
  default-local-server-group local-server-group-name |
  default-relay-server-group server-group-name
  drop;
  equals
  starts-with
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option-60]
```

Release Information

Statement introduced before Junos OS Release 12.1 for EX Series switches.
Statement deprecated in Junos OS Release 12.3 for EX Series switches.

Description

Configure the match criteria when you use the DHCP vendor class identifier option (option 60) in DHCP client packets to forward client traffic to specific DHCP servers. The extended DHCP relay agent compares the option 60 vendor-specific strings received in DHCP client packets against the match criteria that you specify. If there is a match, you can define certain actions for the associated DHCP client packets.

NOTE: The vendor-option statement has been deprecated and might be removed from future product releases. We recommend that you phase out its use. See option-number.

Required Privilege Level

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

Related Documentation

- Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure) on page 611
- *Understanding the Extended DHCP Relay Agent for EX Series Switches*

vendor-option

Syntax

```
vendor-option {
  (default-relay-server-group server-group-name | default-local-server-group
    local-server-group-name | drop);
  (equals | starts-with) (ascii match-string | hexadecimal match-hex) {
    (drop | local-server-group local-server-group-name | relay-server-group
      server-group-name);
  }
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option-60],
[edit forwarding-options dhcp-relay group group-name relay-option-60],
[edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-60],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
  relay-option-60],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay relay-option-60],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay group group-name relay-option-60],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay
  relay-option-60],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group
  group-name relay-option-60]
```

Release Information Statement introduced in JUNOS Release 9.0.

Description Configure the match criteria when you use the DHCP vendor class identifier option (option 60) in DHCP client packets to forward client traffic to specific DHCP servers. The extended DHCP relay agent compares the option 60 vendor-specific strings received in DHCP client packets against the match criteria that you specify. If there is a match, you can define certain actions for the associated DHCP client packets.

The **vendor-option** statement enables you to specify either an exact, left-to-right match (with the **equals** statement) or a partial match (with the **starts-with** statement), and configure either an ASCII match string (with the **ascii** statement) or a hexadecimal match string (with the **hexadecimal** statement).

You can configure an unlimited number of match strings. Match strings do not support the use of wildcard attributes.

Options

equals—Exact, left-to-right match of the ASCII or hexadecimal match string with the option 60 string.

starts-with—Partial match of the ASCII or hexadecimal match string with the option 60 string. The option 60 string can contain a superset of the ASCII or hexadecimal match string, provided that the leftmost characters of the option 60 string entirely match the characters in the configured match string. When you use the **starts-with**

statement, the longest match rule applies; that is, the router matches the string "test123" before it matches the string "test".

ascii *match-string*—ASCII match string of 1 through 255 alphanumeric characters.

hexadecimal *match-hex*—Hexadecimal match string of 1 through 255 hexadecimal characters (0 through 9, a through f, A through F).

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

version (BFD)

Syntax

```
version (0 | 1 | automatic);
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols ldp oam bfd-liveness-detection],
[edit logical-systems logical-system-name protocols ldp oam fec address
  bfd-liveness-detection],
[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method
  bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method
  bfd],
[edit protocols ldp oam bfd-liveness-detection],
[edit protocols ldp oam fec address bfd-liveness-detection]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the BFD protocol version to detect.

Options

0—Use BFD protocol version 0.

1—Use BFD protocol version 1.

automatic—Autodetect the BFD protocol version.

Default: automatic

Required Privilege Level

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

Related Documentation

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients on page 682
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients on page 677
- *Configuring BFD for LDP LSPs*

version (SNMP)

Syntax

```
version (all | v1 | v2);
```

Hierarchy Level

```
[edit snmp trap-group group-name]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers, EX Series switches and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX4600 switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX1100 switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Specify the version number of SNMP traps.

Default

all—Send an SNMPv1 and SNMPv2 trap for every trap condition.

Options

all—Send an SNMPv1 and SNMPv2 trap for every trap condition.

v1—Send SNMPv1 traps only.

v2—Send SNMPv2 traps only.

Required Privilege Level

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

Related Documentation

- *Configuring SNMP Trap Groups*
- *Configuring SNMP Trap Groups*

view-configuration

Can view all of the configuration (not including secrets).

Commands

```
No associated CLI commands.
```

Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.

Related Documentation

- Understanding Junos OS Access Privilege Levels on page 90
- Example: Configuring User Permissions with Access Privilege Levels on page 95

- Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 112
- Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies on page 125

vlan (VoIP)

Syntax

```
vlan (vlan-id | vlan-name | untagged);
```

Hierarchy Level

```
[edit ethernet-switching-options voip interface (VoIP) (all | [interface-name | access-ports])
```

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

Description (EX Series switches only) Specify the VLAN name or VLAN tag identifier associated with the VLAN to be sent from the authenticating server to the IP phone.

Options

vlan-name—Name of a VLAN.

vlan-id—The VLAN tag identifier.

Range: 0 through 4095. Tags 0 and 4095 are reserved by Junos OS; do not configure them.

untagged—Allow untagged VLAN traffic.

Required Privilege Level

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

Related Documentation

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication on page 426
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 421

vlan-assignment

Syntax

```
vlan-assignment (vlan-id | vlan-name);
```

Hierarchy Level

```
[edit protocols dot1x authenticator authentication-profile-name static (Protocols 802.1X)
  mac-address];
[edit ethernet-switching-options authentication-whitelist];
[edit switch-options authentication-whitelist]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement added to the **[edit ethernet-switching-options authentication-whitelist]** hierarchy in Junos OS Release 10.1 for EX Series switches.
Statement added to the **[edit switch-options authentication-whitelist]** hierarchy in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure the VLAN that is associated with the list of MAC addresses that are excluded from RADIUS authentication.

Options

vlan-id | ***vlan-name***—The name of the VLAN or the VLAN tag identifier to associate with the device. The VLAN already exists on the switch.

Required Privilege Level

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

Related Documentation

- show dot1x static-mac-address on page 1811
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 368
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Understanding Authentication on Switches on page 268
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

vpn (Forwarding Options)

Syntax

```
vpn;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay]
```

Release Information

Statement introduced in Junos OS Release 9.0.
Statement changed from **vpn** to **source-ip-change** in Junos OS Release 15.1X49-D130 and later releases.

Description

For Dynamic Host Configuration Protocol (DHCP) client request forwarding, enable source IP change for the device to use address of egress interface as source IP address.

Required Privilege Level

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

Related Documentation

- *DHCP Server, Client, and Relay Agent Overview*

version (SNMP)

Syntax

```
version (all | v1 | v2);
```

Hierarchy Level

```
[edit snmp trap-group group-name]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers, EX Series switches and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX4600 switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX1100 switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Specify the version number of SNMP traps.

Default

all—Send an SNMPv1 and SNMPv2 trap for every trap condition.

Options

all—Send an SNMPv1 and SNMPv2 trap for every trap condition.

v1—Send SNMPv1 traps only.

v2—Send SNMPv2 traps only.

Required Privilege Level

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

Related Documentation

- *Configuring SNMP Trap Groups*
- *Configuring SNMP Trap Groups*

versioning

Syntax versioning;

Hierarchy Level [edit system dynamic-profile-options]

Release Information Statement introduced in Junos OS Release 11.4.

Description Enable version support for dynamic profiles on the system.

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

Related Documentation

- *Versioning for Dynamic Profiles*

voip

Syntax

```
voip {
  interface (all | [interface-name | access-ports]) {
    vlan vlan-name );
    forwarding-class <assured-forwarding | best-effort | expedited-forwarding |
      network-control>;
  }
}
```

Hierarchy Level

```
[edit ethernet-switching-options];
[edit switch-options]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure VoIP interfaces.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication on page 426
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 421

what

Syntax what *number*;

Hierarchy Level [edit protocols lldp-med interface (all | *interface-name*) location civic-based]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Modified in Junos OS Release 9.2 for EX Series switches to display new default.

Description For Link Layer Discovery Protocol–Media Endpoint Device (LLDP-MED), configure the location to which the DHCP entry refers. This information is advertised, along with other location information, from the switch to the MED. It is used during emergency calls to identify the location of the MED.

Options **0** and **1** should not be used unless it is known that the DHCP client is in close physical proximity to the server or network element.

Default 1

Options *number*—Location:

- **0**—Location of the DHCP server.
- **1**—Location of a network element believed to be closest to the client.
- **2**—Location of the client.

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

Related Documentation

- show lldp on page 1826
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 408
- Configuring LLDP-MED (CLI Procedure) on page 521

wait-for-acct-on-ack (Access Profile)

Syntax

```
wait-for-acct-on-ack;
```

Hierarchy Level

[edit access profile *profile-name* accounting]

Release Information

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure the router's authd process to wait for an Acct-On-Ack response message from RADIUS before sending new authentication and accounting updates to the RADIUS server. This configuration ensures that when a new subscriber session starts, the authentication and accounting information for the new session does not get deleted when RADIUS clears previously existing session state information.

At subscriber session startup, the Junos OS authd process sends an Acct-On message to the RADIUS server and the new session starts authentication and accounting operations. However, in some service provider environments, upon receipt of the Acct-On message, the RADIUS server cleans up the previous session state and removes accounting statistics. In this scenario, the RADIUS server's cleanup operation can inadvertently delete the new session's authentication and accounting information, which might include customer billing information.

To ensure that the new session's authentication and accounting information is not deleted, you can include the **wait-for-acct-on-ack** statement to configure authd to wait for an Acct-On-Ack response message from the RADIUS accounting server, so the RADIUS cleanup can finish before authd sends any new authentication and accounting updates.

Required Privilege Level

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

Related Documentation

- *Configuring Per-Subscriber Session Accounting*
- *RADIUS Servers and Parameters for Subscriber Access*

watchdog

Syntax

```
watchdog {
  disable;
  enable;
  timeout value;
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information Statement introduced in Junos OS Release 8.5.

Description Enable or disable the watchdog timer when Junos OS encounters a problem.

Options

- **disable**—Disable the watchdog timer.
- **enable**—Enable the watchdog timer.
- **timeout *value***—Specify amount of time to wait in seconds.

  Range: 1 through 3600 seconds.

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

web-management

Syntax

```
web-management {
  http {
    interfaces [ interface-names ];
    port port;
  }
  https {
    interfaces [ interface-names ];
    local-certificate name;
    port port;
  }
}
```

Hierarchy Level

[edit system services]

Release Information

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

Description

Configure settings for HTTP or HTTPS access. HTTP access allows management of the router or switch using the browser-based J-Web graphical user interface. HTTPS access allows secure management of the router or switch using the J-Web interface. With HTTPS access, communication between the router or switch Web server and your browser is encrypted.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Secure Management Access Configuration Summary*
- *J-Web Interface User Guide*
- http on page 1128
- https on page 1129
- port on page 1337

web-management

Syntax

```
web-management {
  disable;
  failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the Web management process.

Options

- **disable**—Disable the Web management process.
- **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
  - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
  - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

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

web-management (System Services)

Syntax

```
web-management {
  http {
    interfaces interface-names ;
    port port;
  }
  https {
    interfaces interface-names;
    local-certificate name;
    pki-local-certificate name;
    system-generated-certificate name;
    port port;
  }
  management url management url;
  session {
    idle-timout minutes;
    session-limit number;
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (no-world-readable | world-readable);
    }
    flag flag;
    level level;
    no-remote-trace;
  }
}
```

Hierarchy Level

```
[edit system services]
```

Release Information

Statement introduced in Junos OS Release 9.0.
Support for **https** introduced for SRX5400, SRX5600, and SRX5800 devices starting from Junos OS Release 12.1X44-D10 and on vSRX, SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices starting from Junos OS Release 15.1X49-D40.

Description

Configure settings for HTTP or HTTPS access. HTTP access allows management of the device using the J-Web interface. HTTPS access allows secure management of the device using the J-Web interface. With HTTPS access, communication is encrypted between your browser and the webserver for your device.

NOTE: On SRX340 and SRX345 devices, the factory-default configuration has a generic HTTP configuration. To use ge and fxp0 ports as management ports, you must use the set system services web-management http command.

The Web management HTTP and HTTPS interfaces are changed to fxp0.0 and from ge-0/0/1.0 through ge-0/0/7.0.

Options **control**—Disable the SBC process.

- **max-threads**—Maximum simultaneous threads to handle requests.

  Range: 0 through 16

http—Configure HTTP.

- **interface [*value*]**—Interface value that accepts HTTP access.
- **port *number***—TCP port for incoming HTTP connections.

  Range: 1 through 65,535

https—Configure HTTPS.

- **interface [*value*]**—Interface value that accept HTTP access.
- **port *number***—TCP port for incoming HTTP connections.

  Range: 1 through 65,535
- **local-certificate**—X.509 certificate to use from the configuration.
- **pki-local-certificate**—X.509 certificate to use from the PKI local store.
- **system-generated-certificate**—X.509 certificate generated automatically by the system.

management url *management url*—URL path for Web management access.

session—Configure the Web-management session.

- **idle-timout *minutes***—Default timeout of Web-management sessions in minutes.
- **session-limit *number***—Maximum number of Web-management sessions to allow.

traceoptions—Set the trace options.

- **file**—Configure the trace file information.
  - *filename*—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***— Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size *maximum file-size*** option.

    Range: 2 through 1000 files

Default: 10 files

- **match** ***regular-expression***—Refine the output to include lines that contain the regular expression.
- **size** ***maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).

  Range: 10 KB through 1 GB

  Default: 128 KB

  If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** ***number*** option.
- **(world-readable | no-world-readable)**— By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag** ***flag***—Specify which tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags.
  - **all**—Trace all areas.
  - **configuration**—Trace configuration.
  - **dynamic-vpn**—Trace dynamic VPN events.
  - **init**—Trace the daemon init process.
  - **mgd**—Trace MGD requests.
  - **webauth**—Trace Web authentication requests.
- **level** ***level*** —Specify the level of debugging output.
  - **all**—Match all levels.
  - **error**—Match error conditions.
  - **info**—Match informational messages.
  - **notice**—Match conditions that should be handled specially.
  - **verbose**—Match verbose messages.
  - **warning**—Match warning messages.
- **no-remote-trace**—Disable remote tracing.

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

Related Documentation

- *Firewall User Authentication Overview*
- *Dynamic VPN Overview*

wins-server (System)

Syntax

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

Hierarchy Level

```
[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

Release Information

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

Description

For J Series Services Routers and EX Series switches only. Specify one or more NetBIOS Name Servers. When a DHCP client is added to the network and assigned an IP address, the NetBIOS Name Server manages the Windows Internet Name Service (WINS) database that matches IP addresses (such as **192.168.1.3**) to Windows NetBIOS names (such as **\\Marketing**). List servers in order of preference.

Options

address—IPv4 address of the NetBIOS Name Server running WINS. To configure multiple servers, include multiple ***address*** options.

Required Privilege Level

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

Related Documentation

wins-server (System)

Syntax

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

Hierarchy Level

```
[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

Release Information

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

Description

For J Series Services Routers and EX Series switches only. Specify one or more NetBIOS Name Servers. When a DHCP client is added to the network and assigned an IP address, the NetBIOS Name Server manages the Windows Internet Name Service (WINS) database that matches IP addresses (such as **192.168.1.3**) to Windows NetBIOS names (such as **\\Marketing**). List servers in order of preference.

Options

address—IPv4 address of the NetBIOS Name Server running WINS. To configure multiple servers, include multiple ***address*** options.

Required Privilege Level

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

Related Documentation

xnm-clear-text

Syntax

```
xnm-clear-text {
  connection-limit limit;
  rate-limit limit;
}
```

Hierarchy Level

[edit system services]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Allow Junos XML protocol clear-text requests from remote systems to the local router.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*

xnm-ssl

Syntax

```
xnm-ssl {
  connection-limit limit;
  local-certificate name;
  rate-limit limit;
  ssl-renegotiation ;
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.
Support for the **ssl-renegotiation** statement added in Junos OS Release 13.3.

Description Allow Junos XML protocol SSL requests from remote systems to the local router.

The remaining statements are explained separately.

WARNING: Starting with Junos OS Release 15.1, the **sslv3-support** option is not available for configuration with the **set system services xnm-ssl** and **file copy** commands. SSLv3 is no longer supported and available.

For all releases prior to and including Junos OS Release 14.2, SSLv3 is disabled by default at runtime. The **sslv3-support** option is hidden and deprecated in Junos OS Release 14.2 and earlier releases. However, you can use the **set system services xnm-ssl sslv3-support** command to enable SSLv3 for a Junos XML protocol client application to use as the protocol to connect to the Junos XML protocol server on a router, and you can use the **file copy source destination sslv3-support** command to enable the copying of files from an SSLv3 URL.

Using SSLv3 presents a potential security vulnerability, and we recommend that you not use SSLv3. For more details about this security vulnerability, go to https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10656.

NOTE: When FIPS mode is enabled on the device, the **xnm-ssl** service does not support TLS 1.0. For a device in FIPS mode, the clients must communicate with the **xnm-ssl** service using TLS 1.1 or later. In non-FIPS mode, clients can communicate with the **xnm-ssl** service using TLS 1.0 or later. The **xnm-ssl** service never negotiates with the SSLv2 or SSLv3 (the predecessors to TLS 1.0) even if the FIPS mode is enabled or disbaled.

Required Privilege Level

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

Related Documentation

- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*

CHAPTER 15

Operational Commands

- clear system services dhcp statistics
- request component login
- request dhcp client renew
- request dhcp server reconfigure
- request dhcpv6 server reconfigure
- request dhcpv6 client renew
- request ipsec switch
- request message
- request security certificate enroll (Signed)
- request security certificate enroll (Unsigned)
- request security key-pair
- request security pki generate-key-pair
- request security pki local-certificate generate-self-signed
- request security ssh key-pair-identity generate
- request security tpm master-encryption-password set
- request system autorecovery state
- request system decrypt password
- request system download abort
- request system download clear
- request system download pause
- request system download resume
- request system download start
- request system firmware upgrade
- request system license update
- request system reboot
- request system reboot (SRX Series)
- request system services dhcp
- request system snapshot (Maintenance)
- request system software abort in-service-upgrade (ICU)
- request system software add (Maintenance)
- request system software rollback (SRX Series)
- request system zeroize
- show accounting server statistics archival-transfer
- Show SNMP on page 1724
- show captive-portal authentication-failed-users
- show captive-portal firewall
- show captive-portal interface

- show ethernet-switching interfaces
- show chassis routing-engine (View)
- show dhcp client binding
- show dhcp client statistics
- show dhcp relay binding
- show dhcp relay statistics
- show dhcp server binding
- show dhcp server statistics
- show dhcpv6 client binding
- show dhcpv6 client statistics
- show dhcpv6 relay binding
- show dhcpv6 relay statistics
- show dhcpv6 server binding
- show dhcpv6 server binding (View)
- show dhcpv6 server statistics
- show dhcpv6 server statistics (View)
- show firewall (View)
- show dot1x
- show dot1x accounting attribute
- show dot1x authentication-failed-users
- show dot1x firewall
- show dot1x static-mac-address
- show dot1x statistics
- show ethernet-switching interfaces
- show ethernet-switching interface
- show lldp
- show lldp local-information
- show lldp neighbors
- show lldp neighbors
- show lldp statistics
- show lldp statistics
- show lldp remote-global-statistics
- show network-access aaa statistics accounting
- show network-access aaa statistics authentication
- show network-access aaa statistics dynamic-requests
- show network-access radsec local-certificate
- show network-access radsec statistics

- show network-access radsec state
- show route extensive
- show route instance
- show route protocol
- show security tpm status
- show security ssh key-pair-identity
- show security pki local-certificate
- show services unified-access-control authentication-table
- show services unified-access-control policies
- show services unified-access-control status
- show snmp statistics
- show ssl-certificates
- show subscribers
- show system autorecovery state
- show system license (View)
- show system login lockout
- show system download
- show system services dhcp binding
- show system services dhcp client
- show system services dhcp conflict
- show system services dhcp global
- show system services dhcp pool
- show system services dhcp relay-statistics
- show system services dhcp statistics
- show system services service-deployment
- show system snapshot media
- show system storage partitions
- show system users
- test access profile
- test access radius-server

clear accounting server statistics archival-transfer

Syntax clear accounting server statistics archival-transfer

Release Information Command introduced in Junos OS Release 19.2.

Description Clears the statistics of transfer attempted, succeeded, and failed for accounting statistics files and router configuration archives.

Options This command has no options.

Required Privilege Level clear

Output Fields When you enter this command, the transfer statistics are cleared.

Sample Output

clear accounting server statistics archival-transfer

```
user@host> clear accounting server statistics archival-transfer
```

clear captive-portal

Syntax

clear captive-portal (**firewall** [*interface-names*] | **interface** (802.1X) (**all** | [*interface-names*]) | **mac-address** [*mac-addresses*])

Release Information

Command introduced in Junos OS Release 10.1 for EX Series switches.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description

Reset the authentication state of a captive portal interface or captive portal firewall statistics on one or more interfaces.

Options

firewall [*interface-names*]—Resets captive portal statistics on all interfaces or on the specified interface.

interface (all | *interface-names*)—Resets the authentication state of users connected to all interfaces or the specified interfaces.

mac-address *mac-addresses*—Resets the authentication state for the specified MAC addresses.

Required Privilege Level

view

Related Documentation

- show captive-portal authentication-failed-users on page 1727
- show captive-portal interface on page 1731
- show captive-portal firewall on page 1729
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

List of Sample Output

clear captive-portal interface on page 1639
clear captive-portal interface on page 1639
clear captive-portal mac-address on page 1639
clear captive-portal firewall on page 1639

Output Fields

Table 59 on page 1638 lists the output fields for the **clear captive-portal interface** command. (The **clear captive-portal firewall** and **clear captive-portal mac-address** commands have no output). Output fields are listed in the approximate order in which they appear.

Table 59: clear captive-portal interface Output Fields

Field Name	Field Description
Interface	Interface on which captive portal has been configured.

Table 59: clear captive-portal interface Output Fields (continued)

Field Name	Field Description
State	The state of the port: • **Authenticated**—The client has been authenticated through the RADIUS server or has been permitted access through server fail fallback. • **Authenticating**—The client is authenticating through the RADIUS server. • **Connecting**—Switch is attempting to contact the RADIUS server. • **Initialize**—The interface link is down. • **Held**—An action has been triggered through server fail fallback during a RADIUS server timeout. A supplicant is denied access, permitted access through a specified VLAN, or maintains the authenticated state granted to it before the RADIUS server timeout occurred.
MAC address	The MAC address of the connected client on the interface.
User	Users connected to the captive portal interface.

Sample Output

clear captive-portal interface

```
user@switch> clear captive-portal interface
ge-0/0/3.0
```

clear captive-portal interface

```
user@switch> clear captive-portal interface
Captive Portal Information:
Interface      State           MAC address          User
ge-0/0/3.0     Authenticated   00:03:47:e1:ba:b9    aclallow
ge-0/0/5.0     Connecting
ge-0/0/7.0     Connecting
ge-0/0/9.0     Connecting
```

clear captive-portal mac-address

```
user@switch> clear captive-portal mac-address 00:03:47:e1:ba:b9
```

This command has no output.

clear captive-portal firewall

```
user@switch> clear captive-portal firewall
```

This command has no output.

clear dhcp client binding

Syntax

```
clear dhcp client binding
[all|interface <interface-name>]
[routing-instance <routing-instance-name>]
```

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the DHCP client table.

Options

all—(Optional) Clear the binding state for all DHCP clients.

interface <interface-name>—(Optional) Clear the binding state for DHCP clients on the specified interface.

routing-instance <routing-instance-name>—(Optional) Clear the binding state for DHCP clients on the specified routing instance. If you do not specify a routing instance, binding state is cleared for DHCP clients on the default routing instance.

Required Privilege Level clear

Related Documentation

- show dhcp client binding on page 1746

Output Fields This command produces no output.

clear dhcp client statistics

Syntax

```
clear dhcp client statistics
<all>
<interface>
<routing-instance>
```

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Clear all Dynamic Host Configuration Protocol (DHCP) client statistics.

Options

all—(Optional) Clear all the DHCP client statistics.

interface—(Optional) Clear the statistics for DHCP clients on the specified interface.

routing-instance —(Optional) Clear the statistics for DHCP clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

Required Privilege Level clear

Related Documentation

- show dhcp client statistics on page 1749

Output Fields This command produces no output.

clear dhcp relay binding

Syntax

```
clear dhcp relay binding
<all | ip-address | mac-address>
<interface interface-name>
<routing-instance routing-instance-name>
```

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table.

Options

all—(Optional) Clear the binding state for all DHCP clients.

ip-address— (Optional) Clear the binding state for the DHCP client, using the specified IP address.

mac-address—(Optional) Clear the binding state for the DHCP client, using the specified MAC address.

interface interface-name—(Optional) Clear the binding state for DHCP clients on the specified interface

routing-instance routing-instance-name—(Optional) Clear the binding state for DHCP clients on the specified routing instance. If you do not specify a routing instance, the binding state is cleared for the default routing instance.

Required Privilege Level clear

Related Documentation

- show dhcp relay binding on page 1752

Output Fields This command produces no output.

clear dhcp relay statistics

Syntax

```
clear dhcp relay statistics
<routing-instance routing-instance-name>
```

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Clear all Dynamic Host Configuration Protocol (DHCP) relay statistics.

Options

routing-instance routing-instance-name—(Optional) Clear the DHCP relay statistics on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance.

Required Privilege Level clear

Related Documentation

- show dhcp relay statistics on page 1755

Output Fields This command produces no output.

clear dhcp server binding

Syntax

```
clear dhcp server binding
<all | ip-address | mac-address>
<interface interface-name>
<routing-instance routing-instance-name>
```

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table on the DHCP local server.

Options

all—(Optional) Clear the binding state for all DHCP clients.

ip-address— (Optional) Clear the binding state for the DHCP client, using the specified IP address.

mac-address—(Optional) Clear the binding state for the DHCP client, using the specified MAC address.

interface interface-name—(Optional) Clear the binding state for DHCP clients on the specified interface.

routing-instance routing-instance-name—(Optional) Clear the binding state for DHCP clients on the specified routing instance.

Required Privilege Level clear

Related Documentation

- show dhcp server binding on page 1757

Output Fields This command produces no output.

clear dhcp server statistics

Syntax

```
clear dhcp server statistics
<routing-instance routing-instance-name>
```

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Clear all Dynamic Host Configuration Protocol (DHCP) local server statistics.

Options

routing-instance routing-instance-name—(Optional) Clear the statistics for DHCP clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

Required Privilege Level clear

Related Documentation

- show dhcp server statistics on page 1759

Output Fields This command produces no output.

clear dhcpv6 client binding

Syntax

```
clear dhcpv6 client binding
[all | interface interface-name]
[routing-instance routing-instance-name]
```

Release Information Statement introduced in Junos OS Release 12.1X45-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Clear the binding state of a Dynamic Host Configuration Protocol (DHCPv6) client from the DHCPv6 client table.

Options

all—(Optional) Clear the binding state for all DHCPv6 clients.

interface *interface-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.

routing-instance *routing-instance-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, the binding state is cleared for DHCPv6 clients on the default routing instance.

Required Privilege Level clear

Related Documentation

- show dhcpv6 client binding on page 1761

Output Fields This command produces no output.

clear dhcpv6 client statistics

Syntax

```
clear dhcpv6 client statistics
routing-instance routing-instance-name
```

Release Information Statement introduced in Junos OS Release 12.1X45-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Clear all DHCPv6 client statistics.

Options

routing-instance *routing-instance-name*—(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

Required Privilege Level clear

Related Documentation

- show dhcpv6 client statistics on page 1763

Output Fields This command produces no output.

clear dhcpv6 relay binding

Syntax

```
clear dhcpv6 relay binding
<address>
<all>
<dual-stack>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Release Information

Command introduced in Junos OS Release 11.4.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Options *interfaces-vlan* and *interfaces-wildcard* added in Junos OS Release 12.1.
Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.
Option **dual-stack** added in Junos OS Release 15.1.

Description

Clear the binding state of Dynamic Host Configuration Protocol for IPv6 (DHCPv6) clients from the client table.

Options

address—(Optional) Clear the binding state for the DHCPv6 client, using one of the following entries:

- *CID*—The specified Client ID (CID).
- *ipv6-prefix*—The specified IPv6 prefix.
- *session-id*—The specified session ID.

all—(Optional) Clear the binding state for all DHCPv6 clients.

dual-stack—(Optional) Clear the binding state for DHCPv6 clients and the associated DHCPv4 bindings in the single-session DHCP dual stack. DHCPv4 clients created in a DHCPv4-only stack are not affected.

interfaces-vlan—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.

interfaces-wildcard—(Optional) The set of interfaces on which to clear bindings. This option supports the use of the wildcard character (*).

interface *interface-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.

logical-system *logical-system-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified logical system.

routing-instance ***routing-instance-name***—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.

Required Privilege Level view

Related Documentation
- *Viewing and Clearing DHCP Bindings*
- show dhcpv6 relay binding on page 1766

List of Sample Output
clear dhcpv6 relay binding on page 1649
clear dhcpv6 relay binding <prefix> on page 1649
clear dhcpv6 relay binding all on page 1650
clear dhcpv6 relay binding dual-stack all on page 1650
clear dhcv6p relay binding interface on page 1650
clear dhcpv6 relay binding <interfaces-vlan> on page 1650
clear dhcpv6 relay binding <interfaces-wildcard> on page 1650

Output Fields See show dhcpv6 relay binding for an explanation of output fields.

Sample Output

clear dhcpv6 relay binding

The following sample output displays the DHCPv6 bindings before and after the **clear dhcpv6 relay binding** command is issued.

```
user@host> show dhcpv6 relay binding

Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:db8:3c4d:15::/64   1           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
2001:db8:3c4d:16::/64   2           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02
2001:db8:3c4d:17::/64   3           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03
2001:db8:3c4d:18::/64   4           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04
2001:db8:3c4d:19::/64   5           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05
2001:db8:3c4d:20::/64   6           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06
```

clear dhcpv6 relay binding <prefix>

```
user@host> clear dhcpv6 relay binding 2001:db8:3c4d:15::/64
user@host> show dhcpv6 relay binding

Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:db8:3c4d:16::/64   2           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02
2001:db8:3c4d:17::/64   3           83720    BOUND    ge-1/0/0.0
```

```
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03
2001:db8:3c4d:18::/64    4           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04
2001:db8:3c4d:19::/64    5           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05
2001:db8:3c4d:20::/64    6           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06
```

clear dhcpv6 relay binding all

The following command clears all DHCP relay agent bindings:

```
user@host> clear dhcpv6 relay binding all
```

clear dhcpv6 relay binding dual-stack all

The following command clears all DHCPv6 relay agent bindings for all DHCPv6 clients and the associated DHCPv4 bindings in the single-session DHCP dual stack. DHCPv4 clients created in a DHCPv4-only stack are not affected.

```
user@host> clear dhcpv6 relay binding dual-stack all
```

clear dhcv6p relay binding interface

The following command clears DHCPv6 relay agent bindings on a specific interface:

```
user@host> clear dhcpv6 relay binding interface fe-0/0/2
```

clear dhcpv6 relay binding <interfaces-vlan>

The following command uses the *interfaces-vlan* option to clear all DHCPv6 relay agent bindings on top of the underlying interface **ae0**, which clears DHCPv6 bindings on all demux VLANs on top of **ae0**:

```
user@host> clear dhcpv6 relay binding interface ae0
```

clear dhcpv6 relay binding <interfaces-wildcard>

The following command uses the *interfaces-wildcard* option to clear all DHCPv6 relay agent bindings over a specific interface:

```
user@host> clear dhcpv6 relay binding ge-1/0/0.*
```

clear dhcpv6 relay statistics

Syntax

```
clear dhcpv6 relay statistics
<bulk-leasequery-connections>
<leasequery>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Release Information

Command introduced in Junos OS Release 11.4.
Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.
bulk-leasequery-connections option introduced in Junos OS Release 16.1.

Description

Clear all Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay statistics.

Options

bulk-leasequery-connections—(Optional) Clear DHCPv6 relay bulk leasequery statistics.

leasequery—(Optional) Clear DHCPv6 relay individual leasequery statistics.

logical-system *logical-system-name*—(Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are cleared for the default logical system.

routing-instance *routing-instance-name*—(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance.

Required Privilege Level

view

List of Sample Output

clear dhcpv6 relay statistics on page 1651

Output Fields

See show dhcpv6 relay statistics for an explanation of output fields.

Sample Output

clear dhcpv6 relay statistics

The following sample output displays the DHCPv6 relay statistics before and after the **clear dhcpv6 relay statistics** command is issued.

```
user@host> show dhcpv6 relay statistics
```

```
DHCPv6 Packets dropped:
    Total                       0
    Lease Time Violated         1

Messages received:
    DHCPV6_DECLINE              0
    DHCPV6_SOLICIT              10
```

```
    DHCPV6_INFORMATION_REQUEST  0
    DHCPV6_RELEASE              0
    DHCPV6_REQUEST              10
    DHCPV6_CONFIRM              0
    DHCPV6_RENEW                0
    DHCPV6_REBIND               0
    DHCPV6_RELAY_REPL           0

Messages sent:
    DHCPV6_ADVERTISE            0
    DHCPV6_REPLY                0
    DHCPV6_RECONFIGURE          0
    DHCPV6_RELAY_FORW           0
```

```
user@host> clear dhcpv6 relay statistics
user@host> show dhcpv6 relay statistics
```

```
DHCPv6 Packets dropped:
    Total                       0

Messages received:
    DHCPV6_DECLINE              0
    DHCPV6_SOLICIT              0
    DHCPV6_INFORMATION_REQUEST  0
    DHCPV6_RELEASE              0
    DHCPV6_REQUEST              0
    DHCPV6_CONFIRM              0
    DHCPV6_RENEW                0
    DHCPV6_REBIND               0
    DHCPV6_RELAY_REPL           0

Messages sent:
    DHCPV6_ADVERTISE            0
    DHCPV6_REPLY                0
    DHCPV6_RECONFIGURE          0
    DHCPV6_RELAY_FORW           0
```

clear dhcpv6 server binding

Syntax

```
clear dhcpv6 server binding
<address>
<all>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
<dual-stack>
```

Release Information

Command introduced in Junos OS Release 9.6.
Options *interfaces-vlan* and *interfaces-wildcard* added in Junos OS Release 12.1.
Command updated with **dual-stack** statement in Junos OS Release 17.3.

Description

Clear the binding state of a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client from the client table on the extended DHCPv6 local server.

Options

address—(Optional) Clear the binding state for the DHCPv6 client, using one of the following entries:

- *CID*—The specified Client ID (CID).
- *ipv6-prefix*—The specified IPv6 prefix.
- *session-id*—The specified session ID.

all—(Optional) Clear the binding state for all DHCPv6 clients.

interface *interface-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.

interfaces-vlan—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.

interfaces-wildcard—(Optional) Clear bindings on a set of interfaces. This option supports the use of the wildcard character (*).

logical-system *logical-system-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified logical system.

routing-instance *routing-instance-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.

dual-stack—(Optional) Remove either both arms or single arm of dual-stack.

NOTE:

- The **dual-stack** command is added in the syntax removes both arms of the dual-stack with a single command entry.
- When the **dual-stack** command is not added in the syntax, the **clear dhcpv6 server binding** command clears only the family specific arm of the dual-stack.

Required Privilege Level clear

Related Documentation
- *Viewing and Clearing DHCP Bindings*
- show dhcpv6 server binding on page 1779

List of Sample Output
clear dhcpv6 server binding all on page 1654
clear dhcpv6 server binding <ipv6-prefix> on page 1654
clear dhcpv6 server binding interface on page 1654
clear dhcpv6 server binding <interfaces-vlan> on page 1655
clear dhcpv6 server binding <interfaces-wildcard> on page 1655
clear dhcpv6 server binding dual-stack all on page 1655

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

Sample Output

clear dhcpv6 server binding all

The following command clears all DHCPv6 local server bindings:

```
user@host> clear dhcpv6 server binding all
```

clear dhcpv6 server binding <ipv6-prefix>

The following command clears DHCPv6 local server bindings for a specific IPv6 prefix:

```
user@host> clear dhcpv6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005
```

clear dhcpv6 server binding interface

The following command clears DHCPv6 local server bindings on a specific interface:

```
user@host> clear dhcpv6 server binding interface fe-0/0/2
```

clear dhcpv6 server binding <interfaces-vlan>

The following command uses the *interfaces-vlan* option to clear all DHCPv6 local server bindings on top of the underlying interface **ae0**, which clears DHCPv6 bindings on all demux VLANs on top of **ae0**:

```
user@host> clear dhcpv6 server binding interface ae0
```

clear dhcpv6 server binding <interfaces-wildcard>

The following command uses the *interfaces-wildcard* option to clear all DHCPv6 local server bindings over a specific interface:

```
user@host> clear dhcpv6 server binding ge-1/0/0.*
```

clear dhcpv6 server binding dual-stack all

The following command clears all the dual-stack local server bindings.

```
user@host> clear dhcpv6 server binding dual-stack all
```

clear dhcpv6 server binding (Local Server)

Syntax

```
clear dhcpv6 server binding
<all | client-id | ip-address | session-id>
<interface interface-name>
<routing-instance routing-instance-name>
```

Release Information Command introduced in Junos OS Release 10.4.

Description Clear the binding state of a DHCPv6 client from the client table on the DHCPv6 local server.

Options

- all—(Optional) Clear the binding state for all DHCPv6 clients.
- *client-id*—(Optional) Clear the binding state for the DHCPv6 client with the specified client ID (option 1).
- *ip-address*—(Optional) Clear the binding state for the DHCPv6 client with the specified address.
- *session-id*—(Optional) Clear the binding state for the DHCPv6 client with the specified session ID.
- interface *interface-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.
- routing-instance *routing-instance-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.

Required Privilege Level clear

Related Documentation

- show dhcpv6 server binding (View) on page 1786

clear dhcpv6 server statistics

Syntax

```
clear dhcpv6 server statistics
<bulk-leasequery-connections>
<interface interface-name>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Release Information

Command introduced in Junos OS Release 9.6.
bulk-leasequery-connections option introduced in Junos OS Release 16.1.

Description

Clear all extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.

Options

bulk-leasequery-connections—(Optional) Clear DHCPv6 local server bulk leasequery statistics.

logical-system *logical-system-name*—(Optional) Clear the statistics for DHCPv6 clients on the specified logical system. If you do not specify a logical system, statistics are cleared for the default logical system.

routing-instance *routing-instance-name*—(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

Required Privilege Level

clear

Related Documentation

- show dhcpv6 server statistics on page 1790

List of Sample Output

clear dhcpv6 server statistics on page 1657

Output Fields

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

Sample Output

clear dhcpv6 server statistics

```
user@host> clear dhcpv6 server statistics
```

clear dhcpv6 server statistics (Local Server)

Syntax

```
clear dhcpv6 server statistics
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Release Information Command introduced in Junos OS Release 10.4.

Description Clear all DHCPv6 local server statistics.

Options

logical-system *logical-system-name*—(Optional) Clear the statistics for DHCPv6 clients on the specified logical system. If you do not specify a logical system, statistics are cleared for the default logical system.

routing-instance *routing-instance-name*—(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

Required Privilege Level clear

Related Documentation

- show dhcpv6 server statistics (View) on page 1794

clear dot1x

Syntax

clear dot1x (**firewall** <*counter-name*> | **interface** <[*interface-name*]> | **mac-address** [*mac-addresses*] | **statistics** <**interface** *interface-name*>)

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
firewall option added in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.
Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.
Support for **eapol-block** introduced in Junos OS Releases 14.1X53-D40 and 15.1X53-D51 for EX Series switches.

Description

Reset the authentication state of an interface or delete 802.1X statistics from the switch. When you reset an interface using the **interface** or **mac-address** options, reauthentication on the interface is also triggered. The switch sends out a multicast message on the interface to restart the authentication of all connected supplicants. If a MAC address is reset, then the switch sends out a unicast message to that specific MAC address to restart authentication.

If a supplicant is sending traffic when the **clear dot1x interface** command is issued, the authenticator immediately initiates reauthentication. This process happens quickly, and it might seem that reauthentication did not occur. To verify that reauthentication has happened, issue the **show dot1x interface detail** command. The values for **Reauthentication due** and **Reauthentication interval** will be about the same.

CAUTION: When you clear the learned MAC addresses from an interface using the **clear dot1x interface** command, all MAC addresses are cleared, including those in static MAC bypass list.

If you have enabled Media Access Control Security (MACsec) using static secure association key (SAK) security mode on an EX Series switch, the SAKs are rotated when the **clear dot1x** command is entered. The **clear dot1x** command has no impact on MACsec when MACsec is enabled using static connectivity association keys (CAK) or any other security mode.

Options

eapol-block—Clear EAPOL block on the interface and allow the switch to receive EAPOL messages from a supplicant connected to that interface.

firewall <*counter-name*>—Clear 802.1X firewall counter statistics. If the *counter-name* option is specified, clear 802.1X firewall statistics for that counter.

interface <[*interface-name*]>—Reset the authentication state of all the supplicants (also, clears all the authentication bypassed clients) connected to the specified

interface (when the interface is an authenticator) or reset the authentication state for the interface itself (when the interface is a supplicant).

mac-address [*mac-addresses*]—Reset the authentication state of the specified MAC addresses.

statistics <interface *interface-name*>—Clear 802.1X statistics on all 802.1X-enabled interfaces. If the **interface** option is specified, clear 802.1X firewall statistics for that interface or interfaces.

Required Privilege Level view

Related Documentation

- show dot1x on page 1799
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 297

List of Sample Output

clear dot1x firewall on page 1660
clear dot1x interface (Specific Interfaces) on page 1660
clear dot1x mac-address (Specific MAC Address) on page 1660
clear dot1x statistics interface (Specific Interface) on page 1660
clear dot1x eapol-block on page 1660

Sample Output

clear dot1x firewall

```
user@switch> clear dot1x firewall c1
```

clear dot1x interface (Specific Interfaces)

```
user@switch> clear dot1x interface ge-1/0/0 ge-2/0/0 ge-2/0/0 ge5/0/0
```

clear dot1x mac-address (Specific MAC Address)

```
user@switch> clear dot1x mac-address 00:04:ae:cd:23:5f
```

clear dot1x statistics interface (Specific Interface)

```
user@switch> clear dot1x statistics interface ge-1/0/1
```

clear dot1x eapol-block

```
user@switch> clear dot1x eapol-block
```

clear lldp neighbors

Syntax

```
clear lldp neighbors
<interface interface>
```

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.

Description Clear the learned remote neighbor information on all or selected interfaces.

Options

none—Clear the remote neighbor information on all interfaces.

interface *interface*—(Optional) Clear the remote neighbor information from one or more selected interfaces.

Required Privilege Level view

Related Documentation

- show lldp on page 1826
- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

List of Sample Output

Sample Output

clear lldp neighbors

```
user@switch> clear lldp neighbors
```

clear lldp neighbors interface ge-0/1/1.0

```
user@switch> clear lldp neighbors interface ge-0/1/1.0
```

clear lldp statistics

Syntax

```
clear lldp statistics
<interface interface>
```

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.

Description Clear LLDP statistics on one or more interfaces.

Options

none—Clears LLDP statistics on all interfaces.

interface *interface-names*—(Optional) Clear LLDP statistics on one or more interfaces.

Required Privilege Level view

Related Documentation

- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

List of Sample Output

clear lldp statistics on page 1662
clear lldp statistics interface ge-0/1/1.0 on page 1662

Sample Output

clear lldp statistics

```
user@switch> clear lldp statistics
```

clear lldp statistics interface ge-0/1/1.0

```
user@switch> clear lldp statistics interface ge-0/1/1.0
```

clear lldp neighbors

Syntax clear lldp neighbors <interface *interface*>

Release Information Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description Clear the learned remote neighbor information on all or selected interfaces.

Options **none**—Clear the remote neighbor information on all interfaces.

interface *interface*—(Optional) Clear the remote neighbor information from the selected interface.

Required Privilege Level view

Related Documentation
- Understanding LLDP on page 511

List of Sample Output
clear lldp neighbors on page 1663
clear lldp neighbors interface on page 1663

Sample Output

clear lldp neighbors

```
user@switch> clear lldp neighbors
```

clear lldp neighbors interface

```
user@switch> clear lldp neighbors interface ge-0/1/1.0
```

clear lldp statistics

Syntax

```
clear lldp statistics
<interface interface>
```

Release Information

Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Clear LLDP statistics on one or more interfaces.

Options

none—Clears LLDP statistics on all interfaces.

interface *interface-names*—(Optional) Clear LLDP statistics on an interface.

Required Privilege Level

view

Related Documentation

- Understanding LLDP on page 511

List of Sample Output

clear lldp statistics on page 1664
clear lldp statistics interface on page 1664

Sample Output

clear lldp statistics

```
user@switch> clear lldp statistics
```

clear lldp statistics interface

```
user@switch> clear lldp statistics interface ge-0/1/1.0
```

clear network-access radsec state

Syntax

```
clear network-access radsec state
<destination destination-id>
```

Release Information Command introduced in Junos OS Release 19.1R1.

Description Clear the connection state information for RADSEC destinations.

Options

destination ***destination–id***—(Optional) Clear connection state information for the specified RADSEC destination.

Required Privilege Level clear

Related Documentation

- RADIUS over TLS (RADSEC) on page 203

Output Fields This command produces no output.

clear network-access radsec statistics

Syntax

```
clear network-access radsec statistics
<destination destination-id>
```

Release Information Command introduced in Junos OS Release 19.1R1.

Description Clear the connection statistics for RADSEC destinations.

Options

destination ***destination–id***—(Optional) Clear connection statistics for the specified RADSEC destination.

Required Privilege Level clear

Related Documentation

- RADIUS over TLS (RADSEC) on page 203

Output Fields This command produces no output.

clear security pki local-certificate

Syntax

```
clear security pki local-certificate
<all | certificate-id certificate-id-name | system-generated>
```

Release Information Command introduced in Junos OS Release 11.1 for EX Series switches.

Description Delete local digital certificates, certificate requests, and the corresponding public/private key pairs from the switch.

Options

all—(Optional) Delete all local digital certificates, certificate requests, and the corresponding public and private key pairs from the router.

NOTE: This option does not delete the automatically generated self-signed certificate or its public/private key pair.

certificate-id *certificate-id-name*—(Optional) Delete the specified local digital certificate and corresponding public and private key pair.

system-generated—(Optional) Delete the automatically generated self-signed certificate.

Required Privilege Level clear

Related Documentation

- Deleting Self-Signed Certificates (CLI Procedure) on page 255

List of Sample Output clear security pki local-certificate all on page 1667

Output Fields This command produces no output.

Sample Output

clear security pki local-certificate all

```
user@switch> clear security pki local-certificate all
```

clear security ssh key-pair-identity

Syntax clear security ssh key-pair-identity <all> | <*identity-name*>

Release Information Command introduced in Junos OS Release 15.1X49-D70.

Description Clear private and public SSH key pair for the specified files.

Options

- **all**— Clear all the key-pair files.
- ***identity-name***—Clear identity name.

Required Privilege Level clear

Related Documentation

- request security ssh key-pair-identity generate on page 1690
- show security ssh key-pair-identity on page 1905

List of Sample Output clear security ssh key-pair-identity sample on page 1668

Output Fields

Sample Output

clear security ssh key-pair-identity sample

```
user@host> clear security ssh key-pair-identity sample
SSH key sample was removed
```

clear system login lockout

Syntax

```
clear system login lockout
<all>
<user username>
```

Release Information Command introduced in Junos OS Release 11.2.

Description Unlock the user account locked as a result of invalid login attempts.

Options **all**—Clear all locked user accounts.

user *username*—Clear the specified locked user account.

Required Privilege Level clear

Related Documentation

- lockout-period on page 1208
- show system login lockout on page 1967

Output Fields This command produces no output.

clear system services dhcp binding

Syntax

```
clear system services dhcp binding
<address>
```

Release Information

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

Description

(EX Series switches only) Remove obsolete IP address bindings on a Dynamic Host Configuration Protocol (DHCP) server and return them to the IP address pool.

Options

address—(Optional) Remove a specific IP address binding and return it to the address pool.

Required Privilege Level

view and system

Related Documentation

- show system services dhcp binding on page 1970

List of Sample Output

clear system services dhcp binding on page 1670

Output Fields

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

Sample Output

clear system services dhcp binding

```
user@host> clear system services dhcp binding
```

clear system services dhcp conflict

Syntax

```
clear system services dhcp conflict
<address>
```

Release Information

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

Description

(J Series routers and EX Series switches only) Remove IP addresses from the Dynamic Host Configuration Protocol (DHCP) server conflict list and return them to the IP address pool.

Options

address—(Optional) Remove a specific IP address from the conflict list and return it to the address pool.

Required Privilege Level

view and system

Related Documentation

- show system services dhcp conflict on page 1976

List of Sample Output

clear system services dhcp conflict on page 1671

Output Fields

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

Sample Output

clear system services dhcp conflict

```
user@host> clear system services dhcp conflict
```

clear system services dhcp statistics

Syntax clear system services dhcp statistics

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (J Series routers and EX Series switches only) Clear Dynamic Host Configuration Protocol (DHCP) server statistics.

Options This command has no options.

Required Privilege Level view and system

Related Documentation
- show system services dhcp statistics on page 1984

List of Sample Output clear system services dhcp statistics on page 1672

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear system services dhcp statistics

```
user@host> clear system services dhcp statistics
```

request component login

Syntax request component login *component-name*

Release Information Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description (QFabric systems only) Log in to a QFabric system component. To gain access to individual components by way of the **request component login** command, you must first provide the **qfabric-admin** or **qfabric-operator** class privilege to your user (for more information, see: remote-debug-permission).

Options ***component-name***—Specify the QFabric system component to which you wish to log in.

Required Privilege Level admin

Related Documentation
- remote-debug-permission on page 1416

List of Sample Output
request component login (with qfabric-admin Privileges) on page 1673
request component login (with qfabric-operator Privileges) on page 1674
request component login (with qfabric-user Privileges) on page 1674

Sample Output

The three sample output displays show the results of attempts to log in to Node device EE3093. The results differ depending on the privilege level assigned to the user.

request component login (with qfabric-admin Privileges)

```
admin@qfabric> request component login EE3093
Warning: Permanently added 'qfabric-node-ee3093,192.0.2.0' (RSA) to the list of
known hosts.
--- JUNOS 11.3I built 2011-11-04 12:46:16 UTC
{master}
qfabric-admin@node-ee3093> ?
Possible completions:
  clear                Clear information in the system
  file                 Perform file operations
  help                 Provide help information
  load                 Load information from file
  monitor              Show real-time debugging information
  mtrace               Trace multicast path from source to receiver
  op                   Invoke an operation script
  ping                 Ping remote target
  quit                 Exit the management session
  request              Make system-level requests
  restart              Restart software process
  save                 Save information to file
```

```
  set                  Set CLI properties, date/time, craft interface message
  show                 Show system information
  ssh                  Start secure shell on another host
  start                Start shell
  telnet               Telnet to another host
  test                 Perform diagnostic debugging
  traceroute           Trace route to remote host{master}
qfabric-admin@node-ee3093>
```

request component login (with qfabric-operator Privileges)

```
operator@qfabric> request component login EE3093
Warning: Permanently added 'qfabric-node-EE3093,192.0.2.0' (RSA) to the list of
known hosts.
--- JUNOS 11.3I built 2011-11-04 12:46:16 UTC
{master}
qfabric-operator@node-EE3093> ?
Possible completions:
  file                 Perform file operations
  help                 Provide help information
  load                 Load information from file
  op                   Invoke an operation script
  quit                 Exit the management session
  request              Make system-level requests
  save                 Save information to file
  set                  Set CLI properties, date/time, craft interface message
  show                 Show system information
  start                Start shell
  test                 Perform diagnostic debugging
{master}
qfabric-operator@node-ee3093>
```

request component login (with qfabric-user Privileges)

```
user0@qfabric> request component login EE3093
error: User user0 does not have sufficient permissions to login to device ee3093
```

request dhcp client renew

Syntax

```
request dhcp client renew
[all|interface <interface-name>]
routing-instance <routing-instance-name>
```

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Initiates a renew request for the specified clients if they are in the bound state.

Options

all—Initiate renew requests for all DHCP clients. If you specify a routing instance, renew requests are initiated for all DHCP clients within that routing instance.

interface <interface-name>—Initiate renew requests for DHCP clients on the specified interface.

routing-instance <routing-instance-name>—Initiate renew requests for DHCP clients in the specified routing instance. If you do not specify a routing instance, renew requests are initiated on the default routing instance.

Required Privilege Level view

Related Documentation

- request dhcpv6 client renew on page 1680

Output Fields This command produces no output.

request dhcp server reconfigure

Syntax **request dhcp server reconfigure (all | *address* | interface *interface–name* | logical-system *logical-system–name* | routing-instance *routing-instance–name*)**

Release Information Command introduced in Junos OS Release 10.0.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Initiate reconfiguration processing for the specified DHCP clients if they are in the bound state. If the clients are in the reconfiguring state, this command has no effect. If the clients are in any state other than bound or reconfiguring, this command has the same effect as the **clear dhcp server binding** command.

When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfiguring state and the local server sends a forcerenew message to the client. Because the client was in the bound state before entering the reconfiguring state, all subscriber (or DHCP client) services, such as forwarding and statistics, continue to work. An exponential back-off timer determines the interval at which the forcerenew message is sent. If the final attempt is unsuccessful, the client is returned to its original state by default. You can optionally include the **clear-on-abort** statement to configure the client to be cleared when reconfiguration fails.

Options **all**—Initiate reconfiguration for all DHCP clients.

address—Initiate reconfiguration for DHCP client with the specified IP address or MAC address.

interface *interface-name*—Initiate reconfiguration for all DHCP clients on this logical interface (clients whose initial login requests were received over the specified interface).

NOTE: You cannot use the **interface *interface-name*** option with the **request dhcp server reconfigure** command for DHCP passive clients (clients that are added as a result of DHCP snooped packets). For passive clients, the interface is not guaranteed to be the next-hop interface to the client, as is the case for active clients.

logical-system *logical-system-name*—Initiate reconfiguration for all DHCP clients on the specified logical system.

routing-instance *routing-instance-name*—Initiate reconfiguration reconfigured for all DHCP clients in the specified routing instance.

Required Privilege Level view

Related Documentation
- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview on page 662

List of Sample Output request dhcp server reconfigure on page 1677

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request dhcp server reconfigure

```
user@host> request dhcp server reconfigure interface fe-0/0/0.100
```

request dhcpv6 server reconfigure

Syntax

request dhcpv6 server reconfigure (all | *address* | *client-id* | interface *interface-name* | logical-system *logical-system-name* | routing-instance *routing-instance-name* | *session-id*)

Release Information

Command introduced in Junos OS Release 10.4.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Initiate reconfiguration processing for the specified DHCPv6 clients if they are in the bound state. If the clients are in the reconfiguring state, this command has no effect. If the clients are in any state other than bound or reconfiguring, this command has the same effect as the **clear dhcpv6 server binding** command.

When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfigure state and the local server sends a reconfigure message to the client. Because the client was in the bound state before entering the reconfiguring state, all subscriber (or DHCP client) services, such as forwarding and statistics, continue to work. An exponential back-off timer determines the interval at which the reconfigure message is sent. If the final attempt is unsuccessful, the client is returned to its original state by default. You can optionally include the **clear-on-abort** statement to configure the client to be cleared when reconfiguration fails.

Options

all—Initiate reconfiguration for all DHCPv6 clients.

address—Initiate reconfiguration for DHCPv6 client with the specified IPv6 address.

client-id—Initiate reconfiguration for DHCPv6 client with the specified client ID.

interface *interface-name*—Initiate reconfiguration for all DHCPv6 clients on this logical interface (clients whose initial login requests were received over the specified interface).

logical-system *logical-system-name*—Initiate reconfiguration for all DHCPv6 clients on the specified logical system.

routing-instance *routing-instance-name*—Initiate reconfiguration reconfigured for all DHCPv6 clients in the specified routing instance.

session-id—Initiate reconfiguration for DHCPv6 client with the specified session ID.

Required Privilege Level

view

Related Documentation

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview on page 662

List of Sample Output

request dhcpv6 server reconfigure on page 1679

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request dhcpv6 server reconfigure

```
user@host> request dhcpv6 server reconfigure 2001db8::2/16
```

request dhcpv6 client renew

Syntax

```
request dhcpv6 client renew
[all | interface interface-name]
routing-instance <routing-instance-name>
```

Release Information Statement introduced in Junos OS Release 12.1X45-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Initiate a renew request for the specified DHCPv6 clients if they are in the bound state.

Options

all—Initiate renew requests for all DHCPv6 clients. If you specify a routing instance, renew requests are initiated for all DHCPv6 clients within that routing instance.

interface-name *interface-name*—Initiate renew requests for DHCPv6 clients on the specified interface.

routing-instance *routing-instance-name*—Initiate renew requests for DHCPv6 clients in the specified routing instance. If you do not specify a routing instance, renew requests are initiated on the default routing instance.

Required Privilege Level view

Output Fields This command produces no output.

request ipsec switch

Syntax request ipsec switch (interface <es-*fpc/pic/port*> | security-associations <*sa-name*>)

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (Encryption interface on M Series, PTX Series, and T Series routers and EX Series switches only) Manually switch from the primary to the backup encryption services interface, or switch from the primary to the backup IP Security (IPsec) tunnel.

Options **interface <es-*fpc/pic/port*>**—Switch to the backup encryption interface.

security-associations <*sa-name*>—Switch to the backup tunnel.

Required Privilege Level view

Related Documentation
- *show ipsec redundancy*

List of Sample Output request ipsec switch security-associations on page 1681

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request ipsec switch security-associations

```
user@host> request ipsec switch security-associations sa-private
```

request message

Syntax

```
request message all message "text"
request message message "text" (terminal terminal-name  | user user-name)
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display a message on the screens of all users who are logged in to the router or switch or on specific screens.

Options

all—Display a message on the terminal of all users who are currently logged in.

message "*text*"—Message to display.

terminal *terminal-name*—Name of the terminal on which to display the message.

user *user-name*—Name of the user to whom to direct the message.

Required Privilege Level

maintenance

List of Sample Output

request message message on page 1682

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request message message

```
user@host> request message message "Maintenance window in 10 minutes" user maria

Message from user@host on ttyp0 at 20:27 ...
Maintenance window in 10 minutes
EOF
```

request security certificate enroll (Signed)

Syntax

```
request security certificate enroll filename filename subject subject
alternative-subject alternative-subject certification-authority certification-authority encoding
  (binary | pem) key-file key-file  domain-name domain-name
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

(Encryption interface on M Series and T Series routers and EX Series switches only) Obtain a signed certificate from a certificate authority (CA). The signed certificate validates the CA and the owner of the certificate. The results are saved in a specified file to the **/var/etc/ikecert** directory.

NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard. The **request security key-pair** command is deprecated and not available with Junos in FIPS mode because it generates RSA and DSA keys with sizes of 512 and 1024 bits that are not compliant with the NIST SP 800-131A standard.

Options

filename *filename*—File that stores the certificate.

subject *subject*—Distinguished name (**dn**), which consists of a set of components—for example, an organization (**o**), an organization unit (**ou**), a country (**c**), and a locality (**l**).

alternative-subject *alternative-subject*—Tunnel source address.

certification-authority *certification-authority*—Name of the certificate authority profile in the configuration.

encoding (binary | pem)—File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default format is binary.

key-file *key-file*—File containing a local private key.

domain-name *domain-name*—Fully qualified domain name.

Required Privilege Level

maintenance

List of Sample Output

request security certificate enroll filename subject alternative-subject certification-authority key-file domain-name (Signed) on page 1684

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security certificate enroll filename subject alternative-subject certification-authority key-file domain-name (Signed)

```
user@host> request security certificate enroll filename host.crt subject c=uk,o=london
alternative-subject 10.50.1.4 certification-authority verisign   key-file host-1.prv domain-name
host.example.com
CA name: example.com CA file: ca_verisign
local pub/private key pair: host.prv
subject: c=uk,o=london domain name: host.example.com
alternative subject: 10.50.1.4
Encoding: binary
Certificate enrollment has started. To view the status of your enrollment, check
 the key management process (kmd) log file at /var/log/kmd. <--------------
```

request security certificate enroll (Unsigned)

Syntax

request security certificate enroll filename *filename* ca-file *ca-file* ca-name *ca-name* encoding (binary | perm) url *url*

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

(Encryption interface on M Series and T Series routers and EX Series switches only) Obtain a certificate from a certificate authority (CA). The results are saved in a specified file to the **/var/etc/ikecert** directory.

Options

filename *filename*—File that stores the public key certificate.

ca-file *ca-file*—Name of the certificate authority profile in the configuration.

ca-name *ca-name*—Name of the certificate authority.

encoding (binary | pem)—File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default value is **binary**.

url *url*—Certificate authority URL.

Required Privilege Level

maintenance

List of Sample Output

request security certificate enroll filename ca-file ca-name url (Unsigned) on page 1685

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security certificate enroll filename ca-file ca-name url (Unsigned)

```
user@host> request security certificate enroll filename ca_verisign ca-file verisign ca-name
example.com urlxyzcompany URL

http://<verisign ca-name xyzcompany url>/cgi-bin/pkiclient.exe CA name: example.com
 CA file: verisign Encoding: binary
Certificate enrollment has started. To view the status of your enrollment, check
 the key management process (kmd) log file at /var/log/kmd. <--------------
```

request security key-pair

Syntax

```
request security key-pair filename
<size key-size>
<type (rsa | dsa)>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

(Encryption interface on M Series and T Series routers and EX Series switches only) Generate a public and private key pair for a digital certificate.

NOTE: The request security-certificates command is deprecated and are not available with Junos in FIPS mode because security certificates are not compliant with the NIST SP 800-131A standard.

Options

filename—Name of a file in which to store the key pair.

size *key-size*—(Optional) Key size, in bits. The key size can be **512**, **1024**, or **2048**. The default value is **1024**.

type—(Optional) Algorithm used to encrypt the key:

- **rsa**—RSA algorithm. This is the default.
- **dsa**—Digital signature algorithm with Secure Hash Algorithm (SHA).

Required Privilege Level

maintenance

List of Sample Output

request security key-pair on page 1686

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security key-pair

```
user@host> request security key-pair security-key-file
```

request security pki generate-key-pair

Syntax

```
request security pki generate-key-pair certificate-id certificate-id-name
<size (512 | 1024 | 2048)>
<type (dsa | rsa)>
```

Release Information Command introduced in Junos OS Release 11.1 for EX Series switches.

Description Generate a public key infrastructure (PKI) public/private key pair for a local digital certificate.

Options

certificate-id *certificate-id-name*—Name of the local digital certificate and the public/private key pair.

size—(Optional) Key pair size. The key pair size can be **512**, **1024**, or **2048** bits. If a key pair size is not specified, the default value, **1024** bits, is applied.

type—(Optional) The algorithm to be used for encrypting the public/private key pair. The encryption algorithm can be **dsa** or **rsa** . If an encryption algorithm is not specified, the default value, **rsa**, is applied.

Required Privilege Level maintenance

Related Documentation

- Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 256

List of Sample Output request security pki generate-key-pair on page 1687

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki generate-key-pair

```
user@switch> request security pki generate-key-pair certificate-id billy size 2048
Generated key pair billy, key size 2048 bits
```

request security pki local-certificate generate-self-signed

Syntax

```
request security pki local-certificate  generate-self-signed certificate-id certificate-id-name
  domain-name domain-name ip-address ip-address email email-address
  subject subject-distinguished-name
```

Release Information Command introduced in Junos OS Release 11.1 for EX Series switches.

Description Manually generate a self-signed certificate for the given distinguished name.

Options

certificate-id ***certificate-id-name***—Name of the local digital certificate and the public/private key pair.

domain-name ***domain-name***—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.

email ***email-address***—E-mail address of the certificate holder.

ip-address ***ip-address***—IP address of the switch.

subject ***subject-distinguished-name***—Distinguished name format that contains the common name, department, company name, state, and country:

- **CN**—Common name
- **OU**—Organizational unit name
- **O**—Organization name
- **ST**—State
- **C**—Country

Required Privilege Level
maintenance
security

Related Documentation

- Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 256

List of Sample Output request security pki local-certificate generate-self-signed on page 1689

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki local-certificate generate-self-signed

```
user@switch> request security pki local-certificate generate-self-signed certificate-id self-cert
subject cn=abc domain-name abc.net email jdoe@abc.net
Self-signed certificate generated and loaded successfully
```

request security ssh key-pair-identity generate

Syntax request security ssh key-pair-identity generate <*identity-name*> passphrase *passphrase*

Release Information Command introduced in Junos OS Release 15.1X49-D70.

Description Generate the SSH private and public key pair for a specified identity. The private and public key files are stored in the **/var/db** directory, which is accessible through root only. Filenames are based on the **identity-name** with extensions. The files are similar to the certificate files that are stored in Junos OS.

Options

- ***identity-name***—Identity name.
- **passphrase *passphrase***— An SSH identity generated with a passphrase. The passphrase is used to protect the private key file stored in the file system. This option does not allow the user to enter a weak passphrase, which ensures stronger security. A private key is used to connect to a remote server and is never displayed or transferred between servers, even if the system is compromised. The private key cannot be used to connect to a remote server if the passphrase is not known.

NOTE: By default, the **passphrase** uses Advanced Encryption Standard (AES) 128 in cipher block chaining (CBC) mode to encrypt a private key. All generated keys are stored in the **/var/db/ssh_key** directory.

Required Privilege Level maintenance

Related Documentation

- show security ssh key-pair-identity on page 1905
- clear security ssh key-pair-identity on page 1668

List of Sample Output request security ssh key-pair-identity with passphrase on page 1690

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security ssh key-pair-identity with passphrase

```
user@host> request security ssh key-pair-identity generate myident passphrase 1q2w3e
Created SSH key myident
```

request security tpm master-encryption-password set

Syntax request security tpm master-encryption-password set plain-text-password

Release Information Command introduced in Junos OS Release 15.1X49-D80.

Description Use this command to set or replace the password (in plain text).

Options **plain-text-password**—Set or replace the password (in plain text).

Required Privilege Level maintenance

Related Documentation
- show security tpm status on page 1903

List of Sample Output show security tpm status on page 1691

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

show security tpm status

```
user@host> request security tpm master-encryption-password set plain-text-password
  Enter new master encryption password:
  Repeat new master encryption password:
  Binding password with TPM
  Master encryption password is bound to TPM
  Encoding master password ..
  Successfully encoded master password
  Encrypted key-pair files
```

request system autorecovery state

Syntax

```
request system autorecovery state (save | recover | clear)
```

Release Information Command introduced in Junos OS Release 15.1X49-D35 for SRX300, SRX320, SRX345, and SRX550M devices.

Description Prepare the system for autorecovery of configuration, licenses, and disk information.

Options

save—Save the current state of the disk partitioning, configuration, and licenses for autorecovery.

The active Junos OS configuration is saved as the Junos rescue configuration, after which the rescue configuration, licenses, and disk partitioning information is saved for autorecovery. Autorecovery information must be initially saved using this command for the autorecovery feature to verify integrity of data on every bootup.

NOTE:

- Any recovery performed at a later stage will restore the data to the same state as it was when the save command was executed.
- A fresh rescue configuration is generated when the command is executed. Any existing rescue configuration will be overwritten.

recover—Recover the disk partitioning, configuration, and licenses.

After autorecovery data has been saved, the integrity of saved items is always checked automatically on every bootup. The recovery command allows you to forcibly re-run the tests at any time if required.

clear—Clear all saved autorecovery information.

Only the autorecovery information is deleted; the original copies of the data used by the router are not affected. Clearing the autorecovery information also disables all autorecovery integrity checks performed during bootup.

Required Privilege Level maintenance

Related Documentation

- show system autorecovery state on page 1962

List of Sample Output

request system autorecovery state save on page 1693
request system autorecovery state recover on page 1693

request system autorecovery state clear on page 1693

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system autorecovery state save

```
user@host> request system autorecovery state save

Saving config recovery information
      Saving license recovery information
      Saving bsdlabel recovery information
```

Sample Output

request system autorecovery state recover

```
user@host> request system autorecovery state recover

Configuration:
File            Recovery Information    Integrity Check    Action / Status
rescue.conf.gz  Saved                   Passed             None
Licenses:
File            Recovery Information    Integrity Check    Action / Status
JUNOS282736.lic Saved                   Passed             None
JUNOS282737.lic Saved                   Failed             Recovered
BSD Labels:
Slice           Recovery Information    Integrity Check    Action / Status
s1              Saved                   Passed             None
s2              Saved                   Passed             None
s3              Saved                   Passed             None
s4              Saved                   Passed             None
```

Sample Output

request system autorecovery state clear

```
user@host> request system autorecovery state clear

Clearing config recovery information
       Clearing license recovery information
       Clearing bsdlabel recovery information
```


request system decrypt password

Syntax

```
request system decrypt password
```

Release Information

Statement introduced in Junos OS Release 15.1X49-D50 for SRX Series devices.
Statement introduced in Junos OS Release 16.2 for M, MX, PTX, and T Series devices.

Description

Use to display plain text versions of obfuscated ($9) or encrypted ($8) passwords. If the password was encrypted using the new 8 method, you are prompted for the master password.

Options

- **decrypt**—Decrypt a 8-encrypted or 9-encrypted password.

Required Privilege Level

system

Related Documentation

- master-password on page 1222
- Hardening Shared Secrets in Junos OS on page 155

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
// Decrypting a $9 password
user@host> request system decrypt password $9$ABC123
Plaintext password: mysecret
```

Sample Output

```
// Decrypting a $8 password
user@host> request system decrypt password $8$ABC123
Master password:
Plaintext password: mysecret
(Simple passwords like "mysecret" are discouraged. This is an example only.)
```

request system download abort

Syntax

```
request system download abort <download-id>
```

Release Information

Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description

Abort a download. The download instance is stopped and cannot be resumed. Any partially downloaded file is automatically deleted to free disk space. Information regarding the download is retained and can be displayed with the **show system download** command until a **request system download clear** operation is performed.

NOTE: Only downloads in the active, paused, and error states can be aborted.

Options

download-id—(Required) The ID number of the download to be aborted.

Required Privilege Level

maintenance

Related Documentation

- request system download start on page 1699
- request system download pause on page 1697
- request system download resume on page 1698
- request system download clear on page 1696

List of Sample Output

request system download abort on page 1695

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download abort

```
user@host> request system download abort 1
Aborted download #1
```

request system download clear

Syntax

```
request system download clear
```

Release Information

Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description

Delete the history of completed and aborted downloads.

Required Privilege Level

maintenance

Related Documentation

- request system download start on page 1699
- request system download pause on page 1697
- request system download resume on page 1698
- request system download abort on page 1695

List of Sample Output

request system download clear on page 1696

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download clear

```
user@host> request system download clear
Cleared information on completed and aborted downloads
```

request system download pause

Syntax request system download pause <*download-id*>

Release Information Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description Suspend a particular download instance.

NOTE: Only downloads in the active state can be paused.

Options **download-id**—(Required) The ID number of the download to be paused.

Required Privilege Level maintenance

Related Documentation

- request system download start on page 1699
- request system download resume on page 1698
- request system download abort on page 1695
- request system download clear on page 1696

List of Sample Output request system download pause on page 1697

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download pause

```
user@host> request system download pause 1
Paused download #1
```

request system download resume

Syntax request system download resume *download-id* <max-rate>

Release Information Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description Resume a download that has been paused. Download instances that are not in progress because of an error or that have been explicitly paused by the user can be resumed by the user. The file will continue downloading from the point where it paused. By default, the download resumes with the same bandwidth specified with the **request system download start** command. The user can optionally specify a new (maximum) bandwidth with the **request system download resume** command.

NOTE: Only downloads in the paused and error states can be resumed.

Options **download-id**—(Required) The ID number of the download to be resumed.

max-rate—(Optional) The maximum bandwidth for the download.

Required Privilege Level maintenance

Related Documentation

- request system download start on page 1699
- request system download pause on page 1697
- request system download abort on page 1695
- request system download clear on page 1696

List of Sample Output request system download resume on page 1698

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download resume

```
user@host> request system download resume 1
Resumed download #1
```

request system download start

Syntax

request system download start (*sftp-url* | *delay* | *identity-file* | *login* | *max-rate* | *passphrase* | *save as*)

Release Information

Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description

Create a download instance and identify it with a unique integer called the download ID.

Options

sftp-url—(Required) The FTP or HTTP URL location of the file to be downloaded securely.

delay—(Optional) The number of hours after which the download should start (range from 1 through 48 hours).

identity-file—(Required) The name of the file requesting a Secure FTP (SFTP) download. The SFTP in smart download leverages public key authentication to authenticate a download request. Users need to generate a private or public key pair before starting a download, and then upload a public key to an SFTP server.

login—(Optional) The username and password for the server in the format **username:password**.

max-rate—(Optional) The maximum average bandwidth for the download. Numbers with the suffix k or K, m or M, and g or G are interpreted as Kbps, Mbps, or Gbps, respectively.

passphrase—(Required) The passphrase to protect the private key file stored on the file system. This option does not allow the user to enter a weak passphrase, which ensures stronger security.

save-as—(Optional) The filename to be used for saving the file in the **/var/tmp** location.

Required Privilege Level

maintenance

Related Documentation

- request system download pause on page 1697
- request system download resume on page 1698
- request system download abort on page 1695
- request system download clear on page 1696

List of Sample Output

request system download start on page 1700

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download start

```
user@host> request system download start identity-file mytestkey
sftp://mysftpserver/homes/kelly/test.tgz max-rate 200 save as newfile.tgz

Starting download #8
```

request system firmware upgrade

Syntax request system firmware upgrade

Release Information Command introduced in Junos OS Release 10.2.

Description Upgrade firmware on a system.

Options **fpc**—Upgrade FPC ROM monitor.

pic—Upgrade PIC firmware.

re—Upgrade baseboard BIOS/FPGA. There is an active BIOS image and a backup BIOS image.

- **bios**—(Optional) Upgrade BIOS.
- **fpga**—(Optional)Upgrade baseboard FPGA.
- **ssd**—(Optional)Upgrade Routing Engine solid-state drive (SSD) firmware.

  disk1—Upgrade SSD disk1 firmware.

  disk2—Upgrade SSD disk2 firmware.

NOTE: Starting in Junos OS Release 17.2R1, you can upgrade the SSD firmware on MX Series routers with the RE-S-X6-64G and RE-MX2K-X8-64G Routing Engines.

vcpu—Upgrade VCPU ROM monitor.

Required Privilege Level maintenance

Related Documentation
- *request system halt*

List of Sample Output request system firmware upgrade on page 1701

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system firmware upgrade

```
user@host> request system firmware upgrade re bios
```

```
Part             Type           Tag Current   Available Status
                                    version   version
Routing Engine 0 RE BIOS        0   1.5       1.9       OK
Routing Engine 0 RE BIOS Backup 1   1.7       1.9       OK
Perform indicated firmware upgrade ? [yes,no] (no) yes
```

```
user@host> request system firmware upgrade re bios backup
```

```
Part             Type           Tag Current   Available Status
                                    version   version
Routing Engine 0 RE BIOS        0   1.5       1.9       OK
Routing Engine 0 RE BIOS Backup 1   1.7       1.9       OK
Perform indicated firmware upgrade ? [yes,no] (no) yes
```

```
user@host> request system firmware upgrade re ssd disk1
```

```
Part    Type    Tag        Current   Available    Status
                                 version   version
Routing Engine   0 RE SSD1    4      12028     12029        OK
Perform indicated firmware upgrade ? [yes,no] (no) yes

Firmware upgrade initiated, use "show system firmware"  to monitor status.
```

request system license update

Syntax request system license update

Release Information Command introduced in Junos OS Release 9.5.

Description Starts autoupdating license keys from the license portal.

NOTE:

- The request system license update command always uses the default Juniper license server: https://ae1.juniper.net/.
- The request system license update command is supported only on SRX, vSRX, and QFX Series devices.

NOTE: The products supported by the Juniper Agile Licensing (JAL) portal includes: QFX series, SRX Series, EX Series, NFX, vBNG, vMX, vSRX, and ACX. For other Juniper products (SPACE, JSA, SBR Carrier, Screen OS and so on) access the License Management System (LMS).

Options **trial**—Immediately updates trial license keys from the license portal.

Required Privilege Level maintenance

List of Sample Output request system license update on page 1703
request system license update trial on page 1703

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system license update

```
user@host> request system license update

Trying to update license keys from https://ae1.juniper.net has been sent, use
show system license to check status.
```

request system license update trial

```
user@host> request system license update trial
```



```
Request to automatically update trial license keys from https://ae1.juniper.net
has been sent, use show system license to check status.
```

request system reboot

List of Syntax

Syntax

```
request system reboot
<at time>
<both-routing-engines>
<in minutes>
<media (compact-flash | disk | removable-compact-flash | usb)>
<message "text">
<other-routing-engine>
```

Syntax (EX Series Switches and EX Series Virtual Chassis)

```
request system reboot
<all-members | local | member member-id>
<at time>
<in minutes>
<media (external | internal)> | <media (compact-flash | disk | removable-compact-flash |
  usb)>
<message "text">
<slice slice>
```

Syntax (MX Series Routers and MX Series Virtual Chassis, EX9200 Switches and EX9200 Virtual Chassis)

```
request system reboot
<all-members | local | member member-id>
<at time>
<both-routing-engines>
<in minutes>
<media (external | internal)> | <media (compact-flash | disk | usb)> | <junos | network | oam
  | usb>
<message "text">
<other-routing-engine>
```

Syntax (QFabric Systems)

```
request system reboot
<all <graceful>>
<at time>
<director-device name>
<director-group <graceful>>
<fabric <graceful>>
<in minutes>
<in-service>
<media>
```

```
<message “text”>
<node-group name>
<slice slice>
```

Syntax (QFX Series Switches and QFX Series Virtual Chassis, Virtual Chassis Fabric)

```
request system reboot
<all-members | local | member member-id>
<at time>
<in minutes>
<in-service>
<hypervisor>
<junos | network | oam | usb>
<message “text”>
<slice slice>
```

Syntax (TX Matrix Router)

```
request system reboot
<all-chassis | all-lcc | lcc number |  scc>
<at time>
<both-routing-engines>
<in minutes>
<media (compact-flash | disk)>
<message "text">
<other-routing-engine>
```

Syntax (TX Matrix Plus Router)

```
request system reboot
<all-chassis | all-lcc | lcc number | sfc number>
<at time>
<both-routing-engines>
<in minutes>
<media (compact-flash | disk)>
<message "text">
<other-routing-engine>
<partition (1 | 2 | alternate)>
```

Release Information

Command introduced before Junos OS Release 7.4.
Option **other-routing-engine** introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option **sfc** introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Option **partition** changed to **slice** in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Option **both-routing-engines** introduced in Junos OS Release 12.1.

Description

Reboot the software.

This command can be used on standalone devices and on devices supported in a Virtual Chassis, Virtual Chassis Fabric, or QFabric system.

NOTE: Starting with Junos OS Release 15.1F3, the statement **request system reboot** reboots only the guest operating system on the PTX5000 with RE-PTX-X8-64G and, MX240, MX480, and MX960 with RE-S-X6-64G.

Starting with Junos OS Release 15.1F5, the statement **request system reboot** reboots only the guest operating system on the MX2010, and MX2020 with REMX2K-X8-64G.

NOTE: Starting from Junos OS Release 17.2R1, PTX10008 routers do not support the **request system reboot** command. Starting from Junos OS Release 17.4R1, PTX10016 routers do not support the **request system reboot** command. Use the **request vmhost reboot** command instead of the **request system reboot** command on the PTX10008 and PTX10016 routers to reboot the Junos OS software package or bundle on the router. See *request vmhost reboot*.

NOTE: On a QFabric system, to avoid traffic loss on the network Node group, switch mastership of the Routing Engine to the backup Routing Engine, and then reboot.

Options The options described here are not all supported on every platform or release of Junos OS. Refer to the Syntax sections for the options commonly available on each type of platform.

none—Reboot the software immediately.

all-chassis—(Optional) On a TX Matrix router or TX Matrix Plus router, reboot all routers connected to the TX Matrix or TX Matrix Plus router, respectively.

all-lcc—(Optional) On a TX Matrix router or TX Matrix Plus router, reboot all line card chassis connected to the TX Matrix or TX Matrix Plus router, respectively.

all-members | local | member ***member-id***—(Optional) Specify which member of the Virtual Chassis to reboot:

- **all-members**—Reboots each switch that is a member of the Virtual Chassis.
- **local**—Reboots only the local switch (switch where you are logged in).
- **member** ***member-id***—Reboots the specified member switch of the Virtual Chassis

at ***time***—(Optional) Time at which to reboot the software, specified in one of the following ways:

- **now**—Stop or reboot the software immediately. This is the default.
- ***+minutes***—Number of minutes from now to reboot the software.
- ***yymmddhhmm***—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute.
- ***hh:mm***—Absolute time on the current day at which to stop the software, specified in 24-hour time.

both-routing-engines—(Optional) Reboot both Routing Engines at the same time.

hypervisor—(Optional) Reboot Junos OS, host OS, and any installed guest VMs.

in *minutes*—(Optional) Number of minutes from now to reboot the software. This option is an alias for the **at *+minutes*** option.

in-service—(Optional) Enables you to reset the software state (no software version change) of the system with minimal disruption in data and control traffic.

junos—(Optional) Reboot from the Junos OS (main) volume.

lcc *number*——(Optional) Line-card chassis (LLC) number.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

media (compact-flash | disk | removable-compact-flash | usb)—(Optional) Use the indicated boot medium for the next boot.

media (external | internal)—(Optional) Use the indicated boot medium for the next boot:

- **external**—Reboot the device using a software package stored on an external boot source, such as a USB flash drive.
- **internal**—Reboot the device using a software package stored in an internal memory source.

message "*text*"—(Optional) Message to display to all system users before stopping or rebooting the software.

network—(Optional) Reboot using the Preboot Execution Environment (PXE) boot method over the network.

oam—(Optional) Reboot from the maintenance volume (OAM volume, usually the compact flash drive).

other-routing-engine—(Optional) Reboot the other Routing Engine from which the command is issued. For example, if you issue the command from the master Routing Engine, the backup Routing Engine is rebooted. Similarly, if you issue the command from the backup Routing Engine, the master Routing Engine is rebooted.

partition ***partition***—(Optional) Reboot using the specified partition on the boot media. This option is equivalent to the **slice** option that is supported on some devices. Specify one of the following *partition* values:

- **1**—Reboot from partition 1.
- **2**—Reboot from partition 2.
- **alternate**—Reboot from the alternate partition.

scc—(Optional) Reboot the Routing Engine on the TX Matrix switch-card chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted.

sfc ***number***—(Optional) Reboot the Routing Engine on the TX Matrix Plus switch-fabric chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted. Replace *number* with 0.

slice ***slice***—(Optional) Reboot using the specified partition on the boot media. This option was originally the **partitiion** option but was renamed to **slice** on EX Series and QFX Series switches. Specify one of the following *slice* values:

- **1**—Reboot from partition 1.
- **2**—Reboot from partition 2.
- **alternate**—Reboot from the alternate partition (which did not boot the switch at the last bootup).

NOTE: The slice option is not supported on QFX Series switches that have no alternate slice when Junos OS boots as a Virtual Machine (VM). To switch to the previous version of Junos OS, issue the request system software rollback command.

usb—(Optional) Reboot from a USB device.

The following options are available only on QFabric Systems:

all—(Optional) Reboots the software on the Director group, fabric control Routing Engines, fabric manager Routing Engines, Interconnect devices, and network and server Node groups.

director-device ***name***—(Optional) Reboots the software on the Director device and the default partition (QFabric CLI).

director-group—(Optional) Reboots the software on the Director group and the default partition (QFabric CLI).

fabric—(Optional) Reboots the fabric control Routing Engines and the Interconnect devices.

node-group ***name***—(Optional) Reboots the software on a server Node group or a network Node group.

graceful—(Optional) Enables the QFabric component to reboot with minimal impact to network traffic. This sub-option is only available for the **all**, **fabric**, and**director-group** options.

Additional Information

Reboot requests are recorded in the system log files, which you can view with the **show log** command (see *show log*). Also, the names of any running processes that are scheduled to be shut down are changed. You can view the process names with the **show system processes** command (see *show system processes*).

On a TX Matrix or TX Matrix Plus router, if you issue the **request system reboot** command on the master Routing Engine, all the master Routing Engines connected to the routing matrix are rebooted. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are rebooted.

NOTE: Before issuing the **request system reboot** command on a TX Matrix Plus router with no options or the **all-chassis**, **all-lcc**, **lcc** ***number***, or **sfc** options, verify that master Routing Engine for all routers in the routing matrix are in the same slot number. If the master Routing Engine for a line-card chassis is in a different slot number than the master Routing Engine for a TX Matrix Plus router, the line-card chassis might become logically disconnected from the routing matrix after the **request system reboot** command.

NOTE: To reboot a router that has two Routing Engines, reboot the backup Routing Engine (if you have upgraded it) first, and then reboot the master Routing Engine.

Required Privilege Level maintenance

Related Documentation
- *clear system reboot*
- *request system halt*
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*
- *request vmhost reboot*

List of Sample Output

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system reboot

```
user@host> request system reboot
Reboot the system ? [yes,no] (no)
```

request system reboot (at 2300)

```
user@host> request system reboot at 2300 message ?Maintenance time!?
Reboot the system ? [yes,no] (no) yes

shutdown: [pid 186]
*** System shutdown message from root@test.example.net ***
System going down at 23:00
```

request system reboot (in 2 Hours)

```
The following example, which assumes that the time is 5 PM (17:00), illustrates
three different ways to request the system to reboot in two hours:

user@host> request system reboot at +120
user@host> request system reboot in 120
user@host> request system reboot at 19:00
```

request system reboot (Immediately)

```
user@host> request system reboot at now
```

request system reboot (at 1:20 AM)

```
To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is
 the next day, you must specify the absolute time.
```

```
user@host> request system reboot at 06060120
request system reboot at 120
Reboot the system at 120? [yes,no] (no) yes
```

request system reboot in-service

```
user@switch> request system reboot in-service
Reboot the system ? [yes,no]
[Feb 22 02:37:04]:ISSU: Validating Image

 PRE ISSR CHECK:
 ---------------
 PFE Status                          : Online
 Member Id zero                      : Valid
 VC not in mixed or fabric mode      : Valid
 Member is single node vc            : Valid
 BFD minimum-interval check done     : Valid
 GRES enabled                        : Valid
 NSR enabled                         : Valid
 drop-all-tcp not configured         : Valid
 Ready for ISSR                      : Valid

warning: Do NOT use /user during ISSR. Changes to /user during ISSR may get lost!
Current image is jinstall-jcp-i386-flex-18.1.img
[Feb 22 02:37:14]:ISSU: Preparing Backup RE
Prepare for ISSR
[Feb 22 02:37:19]:ISSU: Backup RE Prepare Done
Spawning the backup RE
Spawn backup RE, index 1 successful
Starting secondary dataplane
Second dataplane container started
GRES in progress
Waiting for backup RE switchover ready
GRES operational
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade for ISSR
Chassis ISSU Started
[Feb 22 02:42:55]:ISSU: Preparing Daemons
[Feb 22 02:43:00]:ISSU: Daemons Ready for ISSU
[Feb 22 02:43:05]:ISSU: Starting Upgrade for FRUs
[Feb 22 02:43:15]:ISSU: FPC Warm Booting
[Feb 22 02:44:16]:ISSU: FPC Warm Booted
[Feb 22 02:44:27]:ISSU: Preparing for Switchover
[Feb 22 02:44:31]:ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status                  Reason
  FPC 0          Online (ISSU)
Send ISSR done to chassisd on backup RE
Chassis ISSU Completed
Removing dcpfe0 eth1 128.168.0.16 IP
Bringing down bme00
Post Chassis ISSU processing done
[Feb 22 02:44:33]:ISSU: IDLE
Stopping primary dataplane
Clearing ISSU states
Console and management sessions will be disconnected. Please login again.
```

```
device_handoff successful ret: 0
Shutdown NOW!
[pid 14305]

*** FINAL System shutdown message from root@sw-duckhorn-01 ***

System going down IMMEDIATELY
```

request system reboot (SRX Series)

Syntax

```
request system reboot <at time> <in minutes><media><message “text”>
```

Release Information

Command introduced in Junos OS Release 10.1.
Command **hypervisor** option introduced in Junos OS Release 15.1X49-D10 for vSRX.
Command introduced in Junos OS Release 15.1X49-D50 for SRX1500 devices.

Description

Reboot the software.

Options

- at *time* (Optional)— Specify the time at which to reboot the device. You can specify time in one of the following ways:
  - now— Reboot the device immediately. This is the default.
  - *+minutes*— Reboot the device in the number of minutes from now that you specify.
  - *yymmddhhmm*— Reboot the device at the absolute time on the date you specify. Enter the year, month, day, hour (in 24-hour format), and minute.
  - *hh:mm*— Reboot the device at the absolute time you specify, on the current day. Enter the time in 24-hour format, using a colon (:) to separate hours from minutes.
- in *minutes*(Optional)— Specify the number of minutes from now to reboot the device. This option is a synonym for the at +minutes option
- media *type*(Optional)— Specify the boot device to boot the device from:
  - disk/internal— Reboot from the internal media. This is the default.
  - usb— Reboot from the USB storage device.
  - compact flash— Reboot from the external CompactFlash card.

NOTE: **The media command option is not available on vSRX.**

- message *“text”* (Optional)— Provide a message to display to all system users before the device reboots.

  Example: **request system reboot at 5 in 50 media internal message stop**

Required Privilege Level

maintenance

Related Documentation

- request system software rollback (SRX Series) on page 1721

request system services dhcp

Syntax request system services dhcp (release *interface-name* | renew *interface-name)*

Release Information Command introduced in Junos OS Release 8.5.

Description Release or renew the acquired IP address for a specific interface.

To view the status of the Dynamic Host Configuration Protocol (DHCP) clients on the specified interfaces, enter the **show system services dhcp client** *interface-name* command.

Options

- **release** *interface-name* —Clears other resources received earlier from the server, and reinitializes the client state to INIT for the particular interface.
- **renew** *interface-name* —Reacquires an IP address from the server for the interface. When you use this option, the command sends a discover message if the client state is INIT and a renew request message if the client state is BOUND. For all other states it performs no action.

Required Privilege Level maintenance

Related Documentation

- *dhcp*
- show system services dhcp client on page 1973

Output Fields This command produces no output.

request system snapshot (Maintenance)

Syntax

```
request system snapshot
<config-partition>
<media (compact-flash | hard-disk | internal | usb)>
<partition>
<root-partition>
<factory>
<node (all | local | node-id | primary)>
<slice (alternate) >
```

Release Information Command introduced in Junos OS Release 10.2.

Description Back up the currently running and active file system partitions on the device.

Options

- **config-partition**— Creates a snapshot of the configuration partition only and stores it onto the default **/altconfig** on the hard disk device or an **/altconfig** on a USB device.
- **root-partition**— Creates a snapshot of the root partition only and stores it onto the default **/altroot** on the hard disk device or an **/altroot** on a USB device.
- **factory**— (Optional) Specifies that only the files shipped from the factory are included in the snapshot.
- **media**—(Optional) Specify the boot device the software is copied to:
  - **compact-flash**—Copy software to the primary compact flash drive.
  - **hard-disk**— Copy software to the hard disk.
  - **usb**— Copy software to the device connected to the USB port.
  - **internal**— Copy software to an internal flash drive. This is the default option.

    NOTE: USB option is available on all SRX series devices; hard disk and compact-flash options are available only on SRX5800, SRX5600, and SRX5400 devices; media internal option is available only on SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

  - external— Copies software to an external storage device. This option is available for the compact flash on the SRX650 Services Gateway.
- **node**—(Optional) Specify the archive data and executable areas of a specific node. If you do not specify the node option, the device considers the current node as default option.
  - **node-id**—Specify for node (0, 1).
  - **all**—Specify for all nodes.

  - **local**—Specify for local nodes.
  - **primary**— Specify for primary nodes.
- **partition**—(Default) Specify that the target media should be repartitioned before the backup is saved to it.

NOTE: The target media is partitioned whether or not it is specified in the command, because this is a mandatory option.

Example: **request system snapshot media usb partition**

Example: **request system snapshot media usb partition factory**

- **slice**—(Optional) Take a snapshot of the root partition the system has currently booted from to another slice in the same media.
  - **alternate**—(Optional) Store the snapshot on the other root partition in the system.

NOTE: The slice option cannot be used along with the other **request system snapshot** options, because the options are mutually exclusive. If you use the factory, media, or partition option, you cannot use the slice option; if you use the slice option, you cannot use any of the other options.

Required Privilege Level maintenance

List of Sample Output
request system snapshot config-partition on page 1717
request system snapshot root-partition on page 1718
request system snapshot media hard-disk on page 1718
request system snapshot media usb (when usb device is missing on page 1718
request system snapshot media compact-flash on page 1718
request system snapshot partition on page 1718

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system snapshot config-partition

```
user@host> request system snapshot config-partition
Doing the initial labeling...
Verifying compatibility of destination media partitions...
Running newfs (391MB) on hard-disk media  /config partition (ad1s1e)...
Copying '/dev/ad0s1e' to '/dev/ad1s1e' .. (this may take a few minutes)
The following filesystems were archived: /config
```


request system snapshot root-partition

```
user@host> request system snapshot root-partition
Doing the initial labeling...
Verifying compatibility of destination media partitions...
Running newfs (3GB) on hard-disk media  / partition (ad1s1a)...
Copying '/dev/ad0s1a' to '/dev/ad1s1a' .. (this may take a few minutes)
The following filesystems were archived: /
```

request system snapshot media hard-disk

```
user@host> request system snapshot media hard-disk
Verifying compatibility of destination media partitions...
Running newfs (880MB) on hard-disk media  / partition (ad2s1a)...
Running newfs (98MB) on hard-disk media  /config partition (ad2s1e)...
Copying '/dev/ad0s1a' to '/dev/ad2s1a' .. (this may take a few minutes)
...
```

request system snapshot media usb (when usb device is missing

```
user@host> request system snapshot media usb
Verifying compatibility of destination media partitions...
Running newfs (254MB) on usb media  / partition (da1s1a)...
Running newfs (47MB) on usb media  /config partition (da1s1e)...
Copying '/dev/da0s2a' to '/dev/da1s1a' .. (this may take a few minutes)
Copying '/dev/da0s2e' to '/dev/da1s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

request system snapshot media compact-flash

```
user@host> request system snapshot media compact-flash
error: cannot snapshot to current boot device
```

request system snapshot partition

```
user@host> request system snapshot partition
Verifying compatibility of destination media partitions...
Running newfs (439MB) on internal media  / partition (da0s1a)...
Running newfs (46MB) on internal media  /config partition (da0s1e)...
Copying '/dev/da1s1a' to '/dev/da0s1a' .. (this may take a few minutes)
Copying '/dev/da1s1e' to '/dev/da0s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

request system software abort in-service-upgrade (ICU)

Syntax

```
request system software abort in-service-upgrade
```

Release Information Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Description Abort an in-band cluster upgrade (ICU). This command must be issued from a router session other than the one on which you issued the **request system in-service-upgrade** command that launched the ICU. If an ICU is in progress, this command aborts it. If the node is being upgraded, this command will cancel the upgrade. The command is also helpful in recovering the node in case of a failed ICU.

NOTE: We recommend that you use the command only when there is an issue with the ongoing session of ISSU. You may need to manually intervene to bring the system to sane state if after issuing the command the system does not recover from the abort.

Options This command has no options.

Required Privilege Level view

Related Documentation

- *Upgrading Devices in a Chassis Cluster Using ICU*

List of Sample Output request system software abort in-service-upgrade on page 1719

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software abort in-service-upgrade

```
user@host> request system software abort in-service-upgrade
In-Service-Upgrade aborted
```

request system software add (Maintenance)

Syntax request system software add *package-name*

Release Information Partition option introduced in the command in Junos OS Release 10.1.

Description Install the new software package on the device, for example: **request system software add junos-srxsme-10.0R2-domestic.tgz no-copy no-validate partition reboot**.

Options

- **delay–restart**—Install the software package but does not restart the software process.
- **best-effort-load**—Activate a partial load and treat parsing errors as warnings instead of errors.
- **no-copy**—Install the software package but does not saves the copies of package files.
- **no-validate**—Do not check the compatibility with current configuration before installation starts.
- **partition**—Format and re-partition the media before installation.
- **reboot**—Reboot the device after installation is completed.
- **unlink**—Remove the software package after successful installation.
- **validate**—Check the compatibility with current configuration before installation starts.

Required Privilege Level maintenance

Related Documentation

- request system reboot (SRX Series) on page 1714

request system software rollback (SRX Series)

Syntax

```
request system software rollback <node-id>
```

Release Information

Command introduced in Junos OS Release 10.1.
Command introduced in Junos OS Release 15.1X49-D50 for SRX1500 devices.
Command introduced in Junos OS Release 17.4R1 for SRX4100 and SRX4200 devices.

Description

Revert to the software that was loaded at the last successful **request system software add** command. The upgraded FreeBSD 11.x (supported in Junos OS Release 17.4R1) Junos OS image provides an option to save a recovery image in an Operation, Administration, and Maintenance (OAM) partition, but that option will save only the Junos OS image, not the Linux image. If a user saves the Junos OS image and recovers it later, it might not be compatible with the Linux software loaded on the system.

Options

node-id—Identification number of the chassis cluster node. It can be 0 or 1.

Required Privilege Level

maintenance

Related Documentation

- request system reboot (SRX Series) on page 1714
- *Upgrading Junos OS with Upgraded FreeBSD*
- *Release Information for Junos OS with Upgraded FreeBSD*
- *What Is Junos OS with Upgraded FreeBSD?*

request system zeroize

Syntax

```
request system zeroize <media>
```

Description

Erases all configuration information and resets all key values. The command removes all data files, including customized configuration and log files, by unlinking the files from their directories.

The command removes all user-created files from the system including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication, IPsec, RADIUS, TACACS+, and SNMP.

This command reboots the device and sets it to the factory default configuration. After the reboot, you cannot access the device through the management Ethernet interface. Log in through the console as root and start the Junos OS CLI by typing cli at the prompt.

Options

media—(Optional) In addition to removing all configuration and log files, the media option causes memory and the media to be scrubbed, removing all traces of any user-created files. Every storage device attached to the system is scrubbed, including disks, flash drives, removable USBs, and the like. The duration of the scrubbing process is dependent on the size of the media being erased. As a result, the request system zeroize media operation can take considerably more time than the request system zeroize operation. However, the critical security parameters are all removed at the beginning of the process.

NOTE: **The media option is not supported on SRX5000 line devices.**

Required Privilege Level

Not applicable.

Related Documentation

- request system reboot (SRX Series) on page 1714
- request system software rollback (SRX Series) on page 1721

List of Sample Output

request system zeroize on page 1722

Sample Output

request system zeroize

```
user@host> request system zeroize
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no)  yes
```

```
warning: zeroizing re0

Loading /boot/loader   Consoles: serial port
BIOS driver C: is disk0
BIOS 607kB/2087552kB available memory

FreeBSD/i386 bootstrap loader, Revision 1.1
(builder@youcompany.com, Mon Mar 28 20:49:26 UTC 2011)
Loading /boot/defaults/loader.confg
/kernel text-0x837a60 data=0x46a78+0x9d44c syms=[0x4+0x8f38+0x4+0xca1ee]

Hit [Enter[ to boot immediately, or space bar for command prompt.
Booting [/kernel]...
platform_early_bootinit: MAG Series Early Boot Initilaization
GDB: debug ports: sio
GDB: current port: sio
KDB: debugger backends: ddb gdb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights resrved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 18\989, 1991, 1992, 1993,1994
 The Regents of the University of California. All rights reserved.
...
output truncated
```

show accounting server statistics archival-transfer

Syntax **show accounting server statistics archival-transfer**

Release Information Command introduced in Junos OS Release 19.2.

Description Display the statistics of transfer attempted, succeeded, and failed for accounting statistics files and router configuration archives.

Options This command has no options.

Required Privilege Level view

Sample Output

show accounting server statistics archival-transfer

```
user@host> show accounting server statistics archival-transfer
               File Name : /var/transfer/config/*
URL                                  :scp://root@ce-bras-nvsrv-a:/var/www/html
Last transfer attempted timestamp      :20190603_143642
Last successful transfer timestamp     :20190603_143642
Success Count                          : 5
Failure Count                          : 0
```

Show SNMP

There are several commands that you can access in Junos OS operational mode to monitor SNMP information. Some of the commands are:

- **show snmp health-monitor**, which displays the health monitor log and alarm information.
- **show snmp mib**, which displays information from the MIBs, such as device and system information.
- **show snmp statistics**, which displays SNMP statistics such as the number of packets, silent drops, and invalid output values.
- **show snmp rmon**, which displays the RMON alarm, event, history, and log information

The following example provides sample output from the **show snmp health-monitor** command:

user@switch> show snmp health-monitor

```
Alarm
Index  Variable description                          Value State

 32768 Health Monitor: root file system utilization
```

```
      jnxHrStoragePercentUsed.1                          58 active

 32769 Health Monitor: /config file system utilization
      jnxHrStoragePercentUsed.2                           0 active

 32770 Health Monitor: RE 0 CPU utilization
      jnxOperatingCPU.9.1.0.0                             0 active

 32773 Health Monitor: RE 0 Memory utilization
      jnxOperatingBuffer.9.1.0.0                         35 active

 32775 Health Monitor: jkernel daemon CPU utilization
      Init daemon                                         0 active
      Chassis daemon                                     50 active
      Firewall daemon                                     0 active
      Interface daemon                                    5 active
      SNMP daemon                                        11 active
      MIB2 daemon                                        42 active
      ...
```

The following example provides sample output from the **show snmp mib** command:

user@switch> show snmp mib walk system

```
sysDescr.0    = Juniper Networks, Inc. qfx3500s internet router, kernel
JUNOS 11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC builder@abc.example.net:
/volume/build/junos/11.1/production/20100926.0/obj-xlr/bsd/sys/compile/JUNIPER-xxxxx

Build date: 2010-09-26 06:00:10 U
sysObjectID.0 = jnxProductQFX3500
sysUpTime.0   = 24444184
sysContact.0  = J Smith
sysName.0     = Lab QFX3500
sysLocation.0 = Lab
sysServices.0 = 4
```

The following example provides sample output from the **show snmp statistics** command:

user@switch> show snmp statistics

```
SNMP statistics:
  Input:
    Packets: 0, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 0, Total set varbinds: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0, Duplicate request drops: 0
    Output:
    Packets: 0, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0
```

Related Documentation

- health-monitor on page 1123
- *show snmp mib*
- show snmp statistics on page 1916

show captive-portal authentication-failed-users

Syntax **show captive-portal authentication-failed-users**

Release Information Command introduced in Junos OS Release 10.1 for EX Series switches.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description Display the users that have failed captive portal authentication.

Required Privilege Level view

Related Documentation

- show captive-portal interface on page 1731
- show captive-portal firewall on page 1729
- clear captive-portal on page 1638
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

List of Sample Output show captive-portal authentication-failed-users on page 1727

Output Fields Table 60 on page 1727 lists the output fields for the **show captive-portal authentication-failed-users** command. Output fields are listed in the approximate order in which they appear.

Table 60: show captive-portal authentication-failed-users Output Fields

Field Name	Field Description	Level of Output
Interface	The MAC address configured to bypass captive portal authentication.	**all**
MAC address	The MAC address configured statically on the interface.	**all**
User	Name of the user that has failed captive portal authentication.	**all**
Failure Count	The number of times that 802.1X authentication has failed on the interface.	**all**

Sample Output

show captive-portal authentication-failed-users

```
user@host> show captive-portal authentication-failed-users
```

```
Interface     MAC address          User            Failure Count
ge-0/0/17.0   00:37:00:00:00:00    003700000000        28
ge-0/0/20.0   00:04:10:00:00:00    000410000000        32
ge-0/0/18.0   00:00:03:00:0a:00    000003000a00        4
ge-0/0/19.0   00:00:03:00:0b:00    000003000b00        18
```

show captive-portal firewall

Syntax

```
show captive-portal firewall
<brief | detail>
<interface-name>
<interface-name detail>
```

Release Information

Command introduced in Junos OS Release 10.1 for EX Series switches.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description

Display information about the firewall filters for each user that is authenticated on each captive portal interface.

Options

none—Display all the firewall filters on all captive portal interfaces.

brief | detail—(Optional) Display the specified level of output.

interface-name—(Optional) Display all the terms of the firewall filters for the specified interface.

***interface-name* detail**—(Optional) Display all of the terms of the firewall filters for the specified interface.

Required Privilege Level

view

Related Documentation

- show captive-portal authentication-failed-users on page 1727
- show captive-portal interface on page 1731
- clear captive-portal on page 1638
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

List of Sample Output

show captive-portal firewall brief on page 1730
show captive-portal firewall (Specific Interface) on page 1730
show captive-portal firewall on page 1730

Output Fields

Output fields for the **show captive-portal firewall** command include any action modifier specified in firewall filters except policers. Policers are not supported in the terms of the internally generated dynamic firewall filters that are created when multiple supplicants authenticate on 802.1X-enabled interfaces.

Sample Output

show captive-portal firewall brief

```
user@switch> show captive-portal firewall brief
```

```
Captive Portal Information:
Interface      State           MAC address          User
ge-0/0/1.0     Connecting
ge-0/0/10.0    Connecting      00:30:48:8c:66:bd    No User
```

show captive-portal firewall (Specific Interface)

```
user@switch> show captive-portal firewall ge-0/0/10.0
```

```
Filter name: dot1x_ge-0/0/10
Counters:
Name                            Bytes              Packets
dot1x_ge-0/0/10_CP_arp           7616                  119
dot1x_ge-0/0/10_CP_dhcp             0                    0
dot1x_ge-0/0/10_CP_http             0                    0
dot1x_ge-0/0/10_CP_https            0                    0
dot1x_ge-0/0/10_CP_t_dns            0                    0
dot1x_ge-0/0/10_CP_u_dns            0                    0
```

show captive-portal firewall

```
user@switch> show captive-portal firewall
```

```
Filter name: dot1x_ge-0/0/0
Counters:
Name                                  Bytes              Packets
dot1x_ge-0/0/0_CP_arp                     0                    0
dot1x_ge-0/0/0_CP_dhcp                    0                    0
dot1x_ge-0/0/0_CP_http                    0                    0
dot1x_ge-0/0/0_CP_https                   0                    0
dot1x_ge-0/0/0_CP_t_dns                   0                    0
dot1x_ge-0/0/0_CP_u_dns                   0                    0
Filter name: dot1x_ge-0/0/1
Counters:
Name                                  Bytes              Packets
dot1x_ge-0/0/1_CP_arp                     0                    0
dot1x_ge-0/0/1_CP_dhcp                    0                    0
dot1x_ge-0/0/1_CP_http                    0                    0
dot1x_ge-0/0/1_CP_https                   0                    0
dot1x_ge-0/0/1_CP_t_dns                   0                    0
dot1x_ge-0/0/1_CP_u_dns                   0                    0
Filter name: dot1x_ge-0/0/10
Counters:
Name                                  Bytes              Packets
dot1x_ge-0/0/10_CP_arp                 7616                  119
dot1x_ge-0/0/10_CP_dhcp                   0                    0
dot1x_ge-0/0/10_CP_http                   0                    0
dot1x_ge-0/0/10_CP_https                  0                    0
dot1x_ge-0/0/10_CP_t_dns                  0                    0
dot1x_ge-0/0/10_CP_u_dns                  0                    0
Filter name: dot1x_ge-0/0/11
```

show captive-portal interface

Syntax

```
show captive-portal interface
<interface-name>
detail
```

Release Information

Command introduced in Junos OS Release 10.1 for EX Series switches.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description

Display the current operational state of all captive portal interfaces with the list of connected users and the configured values of captive portal attributes on the interfaces.

Options

none—Display all captive portal interfaces.

interface-name—(Optional) Display the state for the specified captive portal interface and lists the MAC address and user names of any clients authenticated on the interface.

***interface-name* detail**—(Optional) Display the configured values of captive portal attributes on the specified captive portal interface.

Required Privilege Level

view

Related Documentation

- show captive-portal authentication-failed-users on page 1727
- show captive-portal firewall on page 1729
- captive-portal on page 920
- clear captive-portal on page 1638
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 373
- Configuring Captive Portal Authentication (CLI Procedure) on page 378

List of Sample Output

show captive-portal interface (Only Captive Portal Enabled) on page 1733
show captive-portal interface (802.1X Authentication and Captive Portal Enabled) on page 1733
show captive-portal interface detail (Only Captive Portal Enabled) on page 1733
show captive-portal interface detail (802.1X Authentication and Captive Portal Enabled) on page 1734

Output Fields

Table 61 on page 1732 lists the output fields for the **show captive-portal interface** command. Output fields are listed in the approximate order in which they appear.

Table 61: show captive-portal interface Output Fields

Field Name	Field Description	Level of Output
Interface	Interface on which captive portal has been configured.	All levels
State	The state of the interface: • **Authenticated**—The client has been authenticated through the RADIUS server or has been permitted access through server fail fallback. • **Authenticating**—The client is authenticating through the RADIUS server. • **Connecting**—Switch is attempting to contact the RADIUS server. • **Initialize**—The interface link is down. • **Held**—An action has been triggered through server fail fallback during a RADIUS server timeout. A supplicant is denied access, permitted access through a specified VLAN, or maintains the authenticated state granted to it before the RADIUS server timeout occurred.	All levels
MAC address	The MAC address of the connected client on the interface..	brief
User	Users connected to the captive portal interface.	brief
Fallen back	Indicates when 802.1X authentication and captive portal are both enabled on an interface: • If 802.1X authentication and captive portal are both enabled, **CP fallen back** status is **Yes**. • If 802.1X authentication and captive portal are not both enabled, **CP fallen back** status is **No**.	
Supplicant mode	Mode used to authenticate clients—multiple, single, or single-supplicant.	detail
Number of retries	Number of times the user can attempt to submit authentication information.	detail
Quiet period	Time, in seconds, after a user exceeds the maximum number of retries before they can attempt to authenticate.	detail
Configured CP session timeout	Time, in seconds, that a client can be idle before the session expires.	detail
Server timeout	Time, in seconds, that an interface will wait for a reply when relaying a response from the client to the authentication server before timing out and invoking the server-fail action.	detail
Configured CP User-keepalive timeout	Time, in minutes, that a captive portal authentication session is extended after the MAC aging timer expires.	detail

Table 61: show captive-portal interface Output Fields (continued)

Field Name	Field Description	Level of Output
Number of connected supplicants	Number of users connecting through the captive portal interface. Information for each user includes: • **Supplicant**—User name and MAC address. • **Operational state**—See State (above). • **Dynamic CP session timeout**—Timeout value dynamically downloaded from the RADIUS server for this user, if any. • **CP Session expiration due in**—Time remaining in session. • **Eapol-Block**—Shows whether EAPOL block is in effect or not. • **CP Session User-keepalive Expiration due in**—Time, in seconds, remaining in the keep-alive period.	detail

Sample Output

show captive-portal interface (Only Captive Portal Enabled)

```
user@switch> show captive-portal interface

Captive Portal Information:
Interface      State           MAC address          User          Fallen back
ge-0/0/1.0     Connecting
ge-0/0/10.0    Connecting      00:30:48:8c:66:bd    No User
ge-6/0/5.0     Authenticated   00:30:48:8d:7a:9b    abcdeX      No
```

show captive-portal interface (802.1X Authentication and Captive Portal Enabled)

```
user@switch> show captive-portal interface

Captive Portal Information:
Interface      State           MAC address          User          Fallen back
ge-0/0/1.0     Connecting
ge-0/0/10.0    Connecting      00:30:48:8c:66:bd    No User
ge-6/0/5.0     Authenticated   00:30:48:8d:7a:9b    abcdeX      Yes
```

show captive-portal interface detail (Only Captive Portal Enabled)

```
user@switch> show captive-portal interface detail ge-6/0/5.0

 Supplicant mode: Multiple
 Number of retries: 3
 Quiet period: 60 seconds
 Configured CP session timeout: 3600 seconds
 Server timeout: 15 seconds
 Configured CP User-keepalive timeout: 7 minutes
 CP fallen back: No
 Number of connected supplicants: 1
     Supplicant: abcdeX, 00:30:48:8d:7a:9b
         Operational state: Authenticated
         Dynamic CP Session Timeout: 3600 seconds
         CP Session Expiration due in: 3583 seconds
             Eapol-Block: In Effect
         CP session User-keepalive Expiration due in: 420 seconds
```

show captive-portal interface detail (802.1X Authentication and Captive Portal Enabled)

```
user@switch> show captive-portal interface detail ge-6/0/5.0
Supplicant mode: Multiple
 Number of retries: 3
 Quiet period: 60 seconds
 Configured CP session timeout: 3600 seconds
 Server timeout: 15 seconds
 CP fallen back: Yes
 Number of connected supplicants: 1
     Supplicant: abcdeX, 00:30:48:8d:7a:9b
         Operational state: Authenticated
         Dynamic CP Session Timeout: 3600 seconds
         CP Session Expiration due in: 3583 seconds
             Eapol-Block: In Effect
```

show ethernet-switching interfaces

Syntax

```
show ethernet-switching interfaces
<brief | detail | summary>
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
In Junos OS Release 9.6 for EX Series switches, the following updates were made:

- **Blocking** field output was updated.
- The default view was updated to include information about 802.1Q tags.
- The **detail** view was updated to include information on VLAN mapping.

Command introduced in Junos OS Release 11.1 for the QFX Series.
In Junos OS Release 11.1 for EX Series switches, the **detail** view was updated to include reflective relay information.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Display information about switched Ethernet interfaces.

Options

none—(Optional) Display brief information for Ethernet-switching interfaces.

brief | detail | summary—(Optional) Display the specified level of output.

interface *interface-name*—(Optional) Display Ethernet-switching information for a specific interface.

Required Privilege Level

view

Related Documentation

- *Troubleshooting Ethernet SwitchingUnderstanding Bridging and VLANs on Switches*
- *Example: Setting Up Basic Bridging and a VLAN on Switches*
- *Example: Setting Up Bridging with Multiple VLANs*
- *Understanding FCoE*
- *Interfaces Overview for Switches*
- *show ethernet-switching mac-learning-log*
- *show ethernet-switching table*
- *Configuring Autorecovery for Port Security Events*

List of Sample Output

show ethernet-switching interfaces on page 1738
show ethernet-switching interfaces summary on page 1739
show ethernet-switching interfaces brief on page 1739

show ethernet-switching interfaces detail on page 1739
show ethernet-switching interfaces interface-name on page 1740
show ethernet-switching interfaces on page 1740
show ethernet-switching interfaces ge-0/0/15 brief on page 1741
show ethernet-switching interfaces ge-0/0/2 detail (Blocked by RTG rtggroup) on page 1741
show ethernet-switching interfaces ge-0/0/15 detail (Blocked by STP) on page 1741
show ethernet-switching interfaces ge-0/0/17 detail (Disabled by bpdu-control) on page 1741
show ethernet-switching interfaces detail (C-VLAN to S-VLAN Mapping) on page 1741
show ethernet-switching interfaces detail (Reflective Relay Is Configured) on page 1741

Output Fields For QFX Series, QFabric, NFX Series, EX4600 and OCX1100:

Table 62 on page 1736 lists the output fields for the **show ethernet-switching interfaces** command on QFX Series, QFabric, NFX Series, EX4600 and OCX1100. Output fields are listed in the approximate order in which they appear.

Table 62: show ethernet-switching interfaces Output Fields

Field Name	Field Description	Level of Output
Interface	Name of a switching interface.	All levels
State	Interface state. Values are **up** or **down**.	none, **brief**, **detail**, **summary**
VLAN members	Name of a VLAN.	none, **brief**, **detail**, **summary**
Blocking	Forwarding state of the interface: • **blocked**—Traffic is not being forwarded on the interface. • **unblocked**—Traffic is forwarded on the interface. • **MAC limit exceeded**—The interface is temporarily disabled because of a MAC limiting error. The disabled interface is automatically restored to service when the disable timeout expires. • **MAC move limit exceeded**—The interface is temporarily disabled because of a MAC move limiting error. The disabled interface is automatically restored to service when the disable timeout expires. • **Storm control in effect** —The interface is temporarily disabled because of a storm control error. The disabled interface is automatically restored to service when the disable timeout expires. • **Storm control shutdown in effect** —The interface is temporarily disabled because of a storm control shutdown error. The disabled interface is automatically restored to service when the disable timeout expires.	none, **brief**, **detail**, **summary**
Index	VLAN index internal to Junos OS software.	**detail**
untagged | tagged	Specifies whether the interface forwards IEEE802.1Q-tagged or untagged traffic.	**detail**

Output fields for EX Series:

Table 63 on page 1737 lists the output fields for the **show ethernet-switching interfaces** command on EX Series switches. Output fields are listed in the approximate order in which they appear.

Table 63: show ethernet-switching interfaces Output Fields

Field Name	Field Description	Level of Output
Interface	Name of a switching interface.	none, **brief**, **detail**, **summary**
Index	VLAN index internal to Junos OS.	**detail**
State	Interface state. Values are **up** and **down**.	none, **brief**, **detail**
Port mode	The **access** mode is the port mode default and works with a single VLAN. Port mode can also be **trunk**, which accepts tagged packets from multiple VLANs on other switches. The third port mode value is **tagged-access**, which accepts tagged packets from access devices.	**detail**
Reflective Relay Status	Reflective relay allows packets to use the same interface for both upstream and downstream traffic. When reflective relay has been configured, the status displayed is always **enabled** . When reflective relay is not configured, this entry does not appear in the command output.	**detail**
Ether type for the interface	Ether type is a two-octet field in an Ethernet frame used to indicate which protocol is encapsulated in the payload of an incoming Ethernet packet. Both 802.1Q packets and Q-in-Q packets use this field. The output displayed for this particular field indicates the interface's Ether type, which is used to match the Ether type of incoming 802.1Q packets and Q-in-Q packets. The indicated Ether type field is also added to the interface's outgoing 802.1Q and Q-in-Q packets.	**detail**
VLAN membership	Names of VLANs that belong to this interface.	none, **brief**, **detail**,
Tag	Number of the 802.1Q tag.	none, **brief**, **detail**,
Tagging	Specifies whether the interface forwards 802.1Q **tagged** or **untagged** traffic.	none, **brief**, **detail**,

Table 63: show ethernet-switching interfaces Output Fields (continued)

Field Name	Field Description	Level of Output
Blocking	The forwarding state of the interface: • **unblocked**—Traffic is forwarded on the interface. • **blocked**—Traffic is not being forwarded on the interface. • **Disabled by bpdu control**—The interface is disabled due to receiving BPDUs on a protected interface. If the **disable-timeout** statement has been included in the BPDU configuration, the interface automatically returns to service after the timer expires. • **blocked by RTG**—The specified redundant trunk group is disabled. • **blocked by STP**—The interface is disabled due to a spanning-tree protocol error. • **MAC limit exceeded**—The interface is temporarily disabled due to a MAC limit error. The disabled interface is automatically restored to service when the disable timeout expires. • **MAC move limit exceeded**—The interface is temporarily disabled due to a MAC move limit error. The disabled interface is automatically restored to service when the disable timeout expires. • **Storm control in effect**—The interface is temporarily disabled due to a storm control error. The disabled interface is automatically restored to service when the disable timeout expires.	none, **brief**, **detail**,
Number of MACs learned on IFL	Number of MAC addresses learned by this interface.	**detail**
mapping	When mapping is configured, the status is one of the following C-VLAN to S-VLAN mapping types: • **dot1q-tunneled**—The interface maps all traffic to the S-VLAN (all-in-one bundling). • **native**—The interface maps untagged and priority tagged packets to the S-VLAN. • **push**—The interface maps packets to a firewall filter to an S-VLAN. • **policy-mapped**—The interface maps packets to a specifically defined S-VLAN. • *integer*—The interface maps packets to the specified S-VLAN. When mapping is not configured, this entry does not appear in the command output.	**detail**

Sample Output for QFX Series Switches, QFabric, NFX Series, EX4600 and OCX1100

show ethernet-switching interfaces

```
user@switch> show ethernet-switching interfaces

Interface   State    VLAN members          Blocking
xe-0/0/0.0  up       T1122                 unblocked
xe-0/0/1.0  down     default               – MAC limit exceeded
xe-0/0/2.0  down     default               – MAC move limit exceeded
xe-0/0/3.0  down     default               – Storm control in effect
xe-0/0/4.0  down     default               unblocked
```

```
xe-0/0/5.0  down     default               unblocked
xe-0/0/6.0  down     default               unblocked
xe-0/0/7.0  down     default               unblocked
xe-0/0/8.0  down     default               unblocked
xe-0/0/9.0  up       T111                  unblocked
xe-0/0/10.0 down     default               unblocked
xe-0/0/11.0 down     default               unblocked
xe-0/0/12.0 down     default               unblocked
xe-0/0/13.0 down     default               unblocked
xe-0/0/14.0 down     default               unblocked
xe-0/0/15.0 down     default               unblocked
xe-0/0/16.0 down     default               unblocked
xe-0/0/17.0 down     default               unblocked
xe-0/0/18.0 down     default               unblocked
xe-0/0/19.0 up       T111                  unblocked
xe-0/1/0.0  down     default               unblocked
xe-0/1/1.0  down     default               unblocked
xe-0/1/2.0  down     default               unblocked
xe-0/1/3.0  down     default               unblocked
```

show ethernet-switching interfaces summary

```
user@switch> show ethernet-switching interfaces summary
```

```
xe-0/0/0.0
xe-0/0/1.0
xe-0/0/2.0
xe-0/0/3.0
xe-0/0/8.0
xe-0/0/10.0
xe-0/0/11.0
```

show ethernet-switching interfaces brief

```
user@switch> show ethernet-switching interfaces brief
```

```
Interface   State    VLAN members          Blocking
xe-0/0/0.0  down     default               unblocked
xe-0/0/1.0  down     employee-vlan         unblocked
xe-0/0/2.0  down     employee-vlan         unblocked
xe-0/0/3.0  down     employee-vlan         unblocked
xe-0/0/8.0  down     employee-vlan         unblocked
xe-0/0/10.0 down     default               unblocked
xe-0/0/11.0 down     employee-vlan         unblocked
```

show ethernet-switching interfaces detail

```
user@switch> show ethernet-switching interfaces detail
```

```
Interface: xe-0/0/0.0 Index: 65
  State: down
  VLANs:
    default               untagged     unblocked

Interface: xe-0/0/1.0 Index: 66
  State: down
  VLANs:
    employee-vlan         untagged     unblocked
```

```
Interface: xe-0/0/2.0 Index: 67
  State: down
  VLANs:
    employee-vlan          untagged     unblocked

Interface: xe-0/0/3.0 Index: 68
  State: down
  VLANs:
    employee-vlan          untagged     unblocked

Interface: xe-0/0/8.0 Index: 69
  State: down
  VLANs:
    employee-vlan          untagged     unblocked

Interface: xe-0/0/10.0 Index: 70
  State: down
  VLANs:
    default                untagged     unblocked

Interface: xe-0/0/11.0 Index: 71
  State: down
  VLANs:
    employee-vlan          tagged       unblocked
```

show ethernet-switching interfaces interface-name

```
user@switch> show ethernet-switching interfaces xe-0/0/0.0
```

```
 Interface   State    VLAN members           Blocking
xe-0/0/0.0  down     default                unblocked
```

Sample Output for EX Series Switches

show ethernet-switching interfaces

```
user@switch> show ethernet-switching interfaces
```

```
Interface    State  VLAN members        Tag   Tagging  Blocking

ae0.0        up     default                    untagged unblocked
ge-0/0/2.0   up     vlan300           300    untagged blocked by RTG (rtggroup)
ge-0/0/3.0   up     default                             blocked by STP
ge-0/0/4.0   down   default                             MAC limit exceeded
ge-0/0/5.0   down   default                             MAC move limit exceeded
ge-0/0/6.0   down   default                             Storm control in effect
ge-0/0/7.0   down   default                             unblocked
ge-0/0/13.0  up     default                    untagged unblocked
ge-0/0/14.0  up     vlan100             100    tagged   unblocked
                    vlan200             200    tagged   unblocked
ge-0/0/15.0  up     vlan100             100    tagged   blocked by STP
                    vlan200             200    tagged   blocked by STP
ge-0/0/16.0  down   default                    untagged unblocked
ge-0/0/17.0  down   vlan100             100    tagged   Disabled by bpdu-control

                    vlan200             200    tagged   Disabled by bpdu-control
```

show ethernet-switching interfaces ge-0/0/15 brief

```
user@switch> show ethernet-switching interfaces ge-0/0/15 brief
Interface   State  VLAN members   Tag   Tagging        Blocking

ge-0/0/15.0  up     vlan100        100   tagged         blocked by STP
                    vlan200        200   tagged         blocked by STP
```

show ethernet-switching interfaces ge-0/0/2 detail (Blocked by RTG rtggroup)

```
user@switch> show ethernet-switching interfaces ge-0/0/2 detail

Interface: ge-0/0/2.0, Index: 65, State: up, Port mode: Access
Ether type for the interface: 0X8100
VLAN membership:
    vlan300, 802.1Q Tag: 300, untagged, msti-id: 0, blocked by RTG(rtggroup)
Number of MACs learned on IFL: 0
```

show ethernet-switching interfaces ge-0/0/15 detail (Blocked by STP)

```
user@switch> show ethernet-switching interfaces ge-0/0/15 detail

Interface: ge-0/0/15.0, Index: 70, State: up, Port mode: Trunk
Ether type for the interface: 0X8100
VLAN membership:
    vlan100, 802.1Q Tag: 100, tagged, msti-id: 0, blocked by STP
    vlan200, 802.1Q Tag: 200, tagged, msti-id: 0, blocked by STP

Number of MACs learned on IFL: 0
```

show ethernet-switching interfaces ge-0/0/17 detail (Disabled by bpdu-control)

```
user@switch> show ethernet-switching interfaces ge-0/0/17 detail

Interface: ge-0/0/17.0, Index: 71, State: down, Port mode: Trunk
Ether type for the interface: 0X8100
VLAN membership:
    vlan100, 802.1Q Tag: 100, tagged, msti-id: 1, Disabled by bpdu-control
    vlan200, 802.1Q Tag: 200, tagged, msti-id: 2, Disabled by bpdu-control
Number of MACs learned on IFL: 0
```

show ethernet-switching interfaces detail (C-VLAN to S-VLAN Mapping)

```
user@switch>show ethernet-switching interfaces ge-0/0/6.0 detail
Interface: ge-0/0/6.0, Index: 73, State: up, Port mode: Access
Ether type for the interface: 0X8100
VLAN membership:
    map, 802.1Q Tag: 134, Mapped Tag: native, push, dot1q-tunneled, unblocked
    map, 802.1Q Tag: 134, Mapped Tag: 20, push, dot1q-tunneled, unblocked
```

show ethernet-switching interfaces detail (Reflective Relay Is Configured)

```
user@switch1> show ethernet-switching interfaces ge-7/0/2 detail
```

```
Interface: ge-7/0/2, Index: 66, State: down, Port mode: Tagged-access
Ether type for the interface: 0X8100
Reflective Relay Status: Enabled
Ether type for the interface: 0x8100
VLAN membership:
    VLAN_Purple VLAN_Orange VLAN_Blue, 802.1Q Tag: 450, tagged, unblocked
Number of MACs learned on IFL: 0
```

show chassis routing-engine (View)

Syntax show chassis routing-engine

Release Information Command introduced in Junos OS Release 9.5.

Description Display the Routing Engine status of the chassis cluster.

Required Privilege Level view

Related Documentation
- *cluster (Chassis)*
- request system snapshot (Maintenance) on page 1716

List of Sample Output
show chassis routing-engine (Sample 1 - SRX550M) on page 1744
show chassis routing-engine (Sample 2 - vSRX) on page 1744

Output Fields Table 64 on page 1743 lists the output fields for the **show chassis routing-engine** command. Output fields are listed in the approximate order in which they appear.

Table 64: show chassis routing-engine Output Fields

Field Name	Field Description
Temperature	Routing Engine temperature. (Not available for vSRX deployments.)
CPU temperature	CPU temperature. (Not available for vSRX deployments.)
Total memory	Total memory available on the system. NOTE: Starting with Junos OS Release 15.1x49-D70 and Junos OS Release 17.3R1, there is a change in the method for calculating the memory utilization by a Routing Engine. The inactive memory is now subtracted from the total available memory. There is thus, a decrease in the reported value for used memory; as the inactive memory is now considered as free.
Control plane memory	Memory available for the control plane.
Data plane memory	Memory reserved for data plane processing.
CPU utilization	Current CPU utilization statistics on the control plane core.
User	Current CPU utilization in user mode on the control plane core.
Background	Current CPU utilization in nice mode on the control plane core.
Kernel	Current CPU utilization in kernel mode on the control plane core.

Table 64: show chassis routing-engine Output Fields (continued)

Field Name	Field Description
Interrupt	Current CPU utilization in interrupt mode on the control plane core.
Idle	Current CPU utilization in idle mode on the control plane core.
Model	Routing Engine model.
Start time	Routing Engine start time.
Uptime	Length of time the Routing Engine has been up (running) since the last start.
Last reboot reason	Reason for the last reboot of the Routing Engine.
Load averages	The average number of threads waiting in the run queue or currently executing over 1-, 5-, and 15-minute periods.

Sample Output

show chassis routing-engine (Sample 1 - SRX550M)

```
user@host> show chassis routing-engine
Routing Engine status:
    Temperature                 38 degrees C / 100 degrees F
    CPU temperature             36 degrees C / 96 degrees F
    Total memory               512 MB Max   435 MB used ( 85 percent)
      Control plane memory     344 MB Max   296 MB used ( 86 percent)
      Data plane memory        168 MB Max   138 MB used ( 82 percent)
    CPU utilization:
      User                       8 percent
      Background                 0 percent
      Kernel                     4 percent
      Interrupt                  0 percent
      Idle                      88 percent
    Model                          RE-SRX5500-LOWMEM
    Serial ID                      AAAP8652
    Start time                     2009-09-21 00:04:54 PDT
    Uptime                         52 minutes, 47 seconds
    Last reboot reason             0x200:chassis control reset
    Load averages:                 1 minute   5 minute  15 minute
                                       0.12       0.15       0.10
```

Sample Output

show chassis routing-engine (Sample 2 - vSRX)

```
user@host> show chassis routing-engine
Routing Engine status:
    Total memory              1024 MB Max   358 MB used ( 35 percent)
      Control plane memory    1024 MB Max   358 MB used ( 35 percent)
    5 sec CPU utilization:
      User                       2 percent
```

```
  Background                0 percent
  Kernel                    4 percent
  Interrupt                 6 percent
  Idle                     88 percent
Model                       VSRX RE
Start time                  2015-03-03 07:04:18 UTC
Uptime                      2 days, 11 hours, 51 minutes, 11 seconds
Last reboot reason          Router rebooted after a normal shutdown.
Load averages:              1 minute   5 minute  15 minute
                                0.07       0.04       0.06
```

show dhcp client binding

Syntax

```
show dhcp client binding
[<address> |interface <interface-name>]
routing-instance <routing-instance name>
[brief | detail | summary ]
logical-system
tenant
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.
The **logical-system** and **tenant** options are introduced in Junos OS Release 18.4R1.

Description

Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.

Options

address—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:

- ip-address—The specified IP address.
- mac-address—The specified MAC address.

routing-instance <routing-instance name>—(Optional) Display DHCP binding information for DHCP clients on the specified routing instance.

interface <interface-name>—(Optional) Perform this operation on the specified interface.

brief—(Optional) Display brief information about the active client bindings.

detail—(Optional) Display detailed client binding information.

summary—(Optional) Display a summary of DHCP client information.

logical-system—(Optional) Displays the DHCP binding information for DHCP clients on the specified logical system.

tenant—(Optional) Displays the DHCP binding information for DHCP clients on the specified tenant system.

Required Privilege Level

view

Related Documentation

- clear dhcp client binding on page 1640

List of Sample Output

show dhcp client binding on page 1747

Output Fields Table 65 on page 1747 lists the output fields for the **show dhcp client binding** command. Output fields are listed in the approximate order in which they appear.

Table 65: show dhcp client binding Output Fields

Field Name	Field Description
IP address	IP address of the DHCP client.
Hardware address	Hardware address of the DHCP client.
Server	IP address of the DHCP server.
Expires	Number of seconds in which the lease expires.
State	State of the address binding table on the DHCP local server.
Interface	Interface on which the request was received.
Lease Expires	Date and time at which the client's IP address lease expires.
Lease Expires in	Number of seconds in which the lease expires.
Lease Start	Date and time at which the client's IP address lease started.
Vendor Identifier	Vendor identifier.
Server Identifier	IP address of the DHCP server.
Client IP Address	IP address of the DHCP client.

Sample Output

show dhcp client binding

```
user@host> show dhcp client binding
2 clients, (2 bound,  0 init, 0 discover, 0 renew, 0 rebind)

             IP address      Hardware address     Server      Expires     State
    Interface
             10.1.1.89       00:0a:12:00:12:12    10.1.1.1    348         BOUND
    fe-0/0/1.0
             20.1.1.90       00:0a:12:00:12:34    20.1.1.1    568         BOUND
    fe-0/0/2.0
```

```
user@host> show dhcp client binding interface fe-0/0/1.0 detail
Client Interface: fe-0/0/1.0
               Hardware address:       00:0a:12:00:12:12
               State:                  BOUND
               Lease Expires:          2010-09-16 14:45:41 UTC
               Lease Expires in:       528 seconds
```

```
              Lease Start:            2010-09-16 14:35:41 UTC
              Vendor Identifier:      ether
              Server Identifier:      10.1.1.1
              Client IP Address:      10.1.1.89
              update server           enabled

          DHCP Options :
            Name: name-server, Value: [ 10.209.194.131, 198.51.110.2, 192.0.2.3
]
              Name: server-identifier, Value: 10.1.1.1
              Name: router, Value: [ 10.1.1.80 ]
              Name: domain-name, Value: example-50
```

user@host> **show dhcp client binding 10.1.1.89**

```
IP address      Hardware address     Server      Expires     State      Interface

        10.1.1.89       00:0a:12:00:12:12    10.1.1.1    348         BOUND
fe-0/0/1.0
```

user@host> **show dhcp client binding tenant TSYS1 routing-instance R1**

```
IP address        Hardware address   Expires     State      Interface
       33.33.33.3        00:50:56:b0:b8:21  1628        BOUND      ge-0/0/3.0
```

user@host> **show dhcp client binding detail tenant TSYS1 routing-instance R1**

```
Client Interface/Id: ge-0/0/3.0
     Hardware Address:             00:50:56:b0:b8:21
     State:                        BOUND(LOCAL_CLIENT_STATE_BOUND)
     Lease Expires:                2018-04-26 16:24:34 UTC
     Lease Expires in:             1626 seconds
     Lease Start:                  2018-04-26 15:51:14 UTC
     Server Identifier:            11.11.11.1
     Client IP Address:            33.33.33.3
     Update Server                 No

    DHCP options:
    Name: dhcp-lease-time, Value: 33 minutes, 20 seconds
    Name: server-identifier, Value: 11.11.11.1
    Name: router, Value: [ 33.33.33.1 ]
    Name: subnet-mask, Value: 255.255.255.0
```

show dhcp client statistics

Syntax

```
show dhcp client statistics
<routing-instance routing-instance-name >
logical-system
tenant
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.
The **logical-system** and **tenant** option is introduced in Junos OS Release 18.4R1.

Description

Displays the DHCP client statistics.

Options

routing-instance routing-instance-name—(Optional) Display the statistics for DHCP clients on the specified routing instance.

logical-system—(Optional) Displays the DHCP statistics information for DHCP clients on the specified logical system.

tenant—(Optional) Displays the DHCP statistics information for DHCP clients on the specified tenant system.

Required Privilege Level

view

Related Documentation

- clear dhcp client statistics on page 1641

List of Sample Output

show dhcp client statistics on page 1750
show dhcp client statistics tenant TSYS1 routing-instance R1 on page 1751

Output Fields

Table 66 on page 1749 lists the output fields for the **show dhcp client statistics** command. Output fields are listed in the approximate order in which they appear.

Table 66: show dhcp client statistics

Field Name	Field Description
Packets dropped	Number of packets discarded by the DHCP local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.

Table 66: show dhcp client statistics (continued)

Field Name	Field Description
Messages received	Number of DHCP messages received. • BOOTREPLY—Number of BOOTP protocol data units (PDUs) received • DHCPOFFER—Number of DHCP PDUs of type OFFER received • DHCPACK—Number of DHCP PDUs of type ACK received • DHCPNACK—Number of DHCP PDUs of type NACK received • DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW received
Messages sent	Number of DHCP messages sent. • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) transmitted • DHCPDECLINE—Number of DHCP PDUs of type DECLINE transmitted • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER transmitted • DHCPREQUEST—Number of DHCP PDUs of type REQUEST transmitted • DHCPINFORM—Number of DHCP PDUs of type INFORM transmitted • DHCPRELEASE—Number of DHCP PDUs of type RELEASE transmitted • DHCPRENEW—Number of DHCP PDUs of type RENEW transmitted • DHCPREBIND—Number of DHCP PDUs of type REBIND transmitted

Sample Output

show dhcp client statistics

```
user@host> show dhcp client statistics
Packets dropped:
    Total                     0
Messages received:
    BOOTREPLY                 0
    DHCPOFFER                 0
    DHCPACK                   0
    DHCPNAK                   0
    DHCPFORCERENEW            0
Messages sent:
    BOOTREQUEST               0
    DHCPDECLINE               0
    DHCPDISCOVER              0
    DHCPREQUEST               0
    DHCPINFORM                0
    DHCPRELEASE               0
```

```
    DHCPRENEW                 0
    DHCPREBIND                0
```

show dhcp client statistics tenant TSYS1 routing-instance R1

```
user@host> show dhcp client statistics tenant TSYS1 routing-instance R1
```

```
Packets dropped:
    Total                     0

   Messages received:
    BOOTREPLY                 14
    DHCPOFFER                 4
    DHCPACK                   10
    DHCPNAK                   0
    DHCPFORCERENEW            0

  Messages sent:
    BOOTREQUEST               17
    DHCPDECLINE               0
    DHCPDISCOVER              4
    DHCPREQUEST               10
    DHCPINFORM                0
    DHCPRELEASE               3
    DHCPRENEW                 6
    DHCPREBIND                0
```

show dhcp relay binding

Syntax

```
Show dhcp relay binding
[<address> |interface <interface-name>]
routing-instance <routing-instance name>
[brief | detail | summary]
```

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) relay client table.

Options

address—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:

- ip-address—The specified IP address.
- mac-address—The specified MAC address.

routing-instance <routing-instance name>—(Optional) Display DHCP binding information on the specified routing instance.

interface <interface-name>—(Optional) Perform this operation on the specified interface.

brief—(Optional) Display brief information about the active client bindings.

detail—(Optional) Display detailed client binding information.

summary—(Optional) Display a summary of DHCP client information.

Required Privilege Level view

Related Documentation

- clear dhcp relay binding on page 1642

List of Sample Output show dhcp relay binding on page 1753

Output Fields Table 67 on page 1752 lists the output fields for the **show dhcp relay binding** command. Output fields are listed in the approximate order in which they appear.

Table 67: show dhcp relay binding Output Fields

Field Name	Field Description
IP address	IP address of the DHCP client.
Hardware address	Hardware address of the DHCP client.

Table 67: show dhcp relay binding Output Fields (continued)

Field Name	Field Description
Request received on	Interface on which the request was received.
Type	Type of DHCP packet processing performed on the device.
Obtained at	Date and time at which the client's IP address lease started.
Expires at	Date and time at which the client's IP address lease expires.
State	State of the address binding table on the DHCP local server.

Sample Output

show dhcp relay binding

```
user@host> show dhcp relay binding detail
IP address       Hardware address   Type     Lease expires            State
       100.20.32.1      90:00:00:01:00:01  active   2007-01-17 11:38:47 PST
rebind
       100.20.32.3      90:00:00:02:00:01  active   2007-01-17 11:38:41 PST
rebind
       100.20.32.4      90:00:00:03:00:01  active   2007-01-17 11:38:01 PST
rebind
       100.20.32.5      90:00:00:04:00:01  active   2007-01-17 11:38:07 PST
rebind
       100.20.32.6      90:00:00:05:00:01  active   2007-01-17 11:38:47 PST
rebind
```

```
user@host> show dhcp relay binding 100.20.32.1
Active binding information:
           IP address               100.20.32.1
           Hardware address         90:00:00:01:00:01

       Lease information:
          Type               DHCP
          Obtained at        2007-01-17 11:28:47 PST
          Expires at         2007-01-17 11:38:47 PST

       > show dhcp relay binding 100.20.32.1 detail
       Active binding information:
           IP address              100.20.32.1
           Hardware address        90:00:00:01:00:01
           Request received on     fe-0/0/2.0, relayed by 100.20.32.2

       Lease information:
           Type                DHCP
           Obtained at         2007-01-17 11:28:47 PST
           Expires at          2007-01-17 11:38:47 PST
           State               rebind
```

show dhcp relay statistics

Syntax

```
show dhcp relay statistics
[<routing-instance>]
```

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Display Dynamic Host Configuration Protocol (DHCP) relay statistics.

Options **routing-instance**—(Optional) Display the DHCP relay statistics on the specified routing instance.

Required Privilege Level view

Related Documentation

- clear dhcp relay statistics on page 1643

List of Sample Output show dhcp relay statistics on page 1756

Output Fields Table 68 on page 1755 lists the output fields for the **show dhcp relay statistics** command. Output fields are listed in the approximate order in which they appear.

Table 68: show dhcp relay statistics

Field Name	Field Description
Messages received	Number of DHCP messages sent. • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received • DHCPDECLINE—Number of DHCP PDUs of type DECLINE received • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received • DHCPREQUEST—Number of DHCP PDUs of type REQUEST received • DHCPINFORM—Number of DHCP PDUs of type INFORM received • DHCPRELEASE—Number of DHCP PDUs of type RELEASE received
Messages sent	Number of DHCP messages received. • BOOTREPLY—Number of BOOTP PDUs transmitted • DHCPOFFER—Number of DHCP PDUs of type OFFER transmitted • DHCPACK—Number of DHCP PDUs of type ACK transmitted • DHCPNACK—Number of DHCP PDUs of type NACK transmitted • DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW transmitted

Sample Output

show dhcp relay statistics

```
user@host> show dhcp relay statistics

Messages received:
    BOOTREQUEST                0
    DHCPDECLINE                0
    DHCPDISCOVER               0
    DHCPINFORM                 0
    DHCPRELEASE                0
    DHCPREQUEST                0

Messages sent:
    BOOTREPLY                  0
    DHCPOFFER                  0
    DHCPACK                    0
    DHCPNAK                    0
    DHCPFORCERENEW             0
```

show dhcp server binding

Syntax

```
show dhcp server binding
[interface <interface name>]
<brief | detail | summary | verbose>
<ip-address | MAC address>
<routing-instance routing-instance-name>
```

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Display the address bindings in the client table on the Dynamic Host Configuration Protocol (DHCP) local server.

Options

interface <interface name>—(Optional) Display information about active client bindings on the specified interface.

brief | detail | summary—(Optional) Display the specified level of output about active client bindings. The default is brief, which produces the same output as **show dhcp server binding**.

ip-address—Display DHCP binding information for a specific client identified by the specified IP address.

MAC address—Display DHCP binding information for a specific client identified by the specified MAC address.

routing-instance routing-instance-name—(Optional) Display information about active client bindings for DHCP clients on the specified routing instance.

Required Privilege Level view

Related Documentation

- clear dhcp server binding on page 1644

List of Sample Output show dhcp server binding on page 1758

Output Fields Table 69 on page 1757 lists the output fields for the show dhcp server binding command. Output fields are listed in the approximate order in which they appear.

Table 69: show dhcp server binding Output Fields

Field Name	Field Description
IP address	IP address of the DHCP client.
Hardware address	Hardware address of the DHCP client.

Table 69: show dhcp server binding Output Fields (continued)

Field Name	Field Description
Request received on	Interface on which the request was received.
Type	Type of DHCP packet processing performed on the device.
Obtained at	Date and time at which the client's IP address lease started.
Expires at	Date and time at which the client's IP address lease expires.
State	State of the address binding table on the DHCP local server.

Sample Output

show dhcp server binding

```
user@host> show dhcp server binding 100.20.32.1 detail

Active binding information:
               IP address            100.20.32.1
               Hardware address      90:00:00:01:00:01
               Request received on   fe-0/0/2.0, relayed by 100.20.32.2

           Lease information:
               Type                  DHCP
               Obtained at           2007-01-17 11:28:47 PST
               Expires at            2007-01-17 11:38:47 PST
               State                 rebind
```

show dhcp server statistics

Syntax

```
show dhcp server statistics
<routing-instance>
```

Release Information Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Display Dynamic Host Configuration Protocol (DHCP) local server statistics.

Options

routing-instance—(Optional) Display information about DHCP local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.

Required Privilege Level view

Related Documentation

- clear dhcp server statistics on page 1645

List of Sample Output show dhcp server statistics on page 1760

Output Fields Table 70 on page 1759 lists the output fields for the **show dhcp server statistics** command. Output fields are listed in the approximate order in which they appear.

Table 70: show dhcp server statistics

Field Name	Field Description
Packets dropped	Number of packets discarded by the DHCP local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.
Messages received	Number of DHCP messages sent. • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received • DHCPDECLINE—Number of DHCP PDUs of type DECLINE received • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received • DHCPREQUEST—Number of DHCP PDUs of type REQUEST received • DHCPINFORM—Number of DHCP PDUs of type INFORM received • DHCPRELEASE—Number of DHCP PDUs of type RELEASE received

Table 70: show dhcp server statistics (continued)

Field Name	Field Description
Messages sent	Number of DHCP messages received. • BOOTREPLY—Number of BOOTP PDUs transmitted • DHCPOFFER—Number of DHCP PDUs of type OFFER transmitted • DHCPACK—Number of DHCP PDUs of type ACK transmitted • DHCPNACK—Number of DHCP PDUs of type NACK transmitted • DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW transmitted

Sample Output

show dhcp server statistics

```
user@host> show dhcp server statistics
Packets dropped:
    Total                     0

Messages received:
    BOOTREQUEST               0
    DHCPDECLINE               0
    DHCPDISCOVER              0
    DHCPINFORM                0
    DHCPRELEASE               0
    DHCPREQUEST               0

Messages sent:
    BOOTREPLY                 0
    DHCPOFFER                 0
    DHCPACK                   0
    DHCPNAK                   0
    DHCPFORCERENEW            0
```

show dhcpv6 client binding

Syntax

```
show dhcpv6 client binding
interface interface-name
routing-instance <routing-instance-name>
[brief | detail | summary]
```

Release Information Statement introduced in Junos OS Release 12.1X45-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Display the address bindings in the Dynamic Host Configuration Protocol version 6 (DHCPv6) client table.

Options

interface *interface-name*—(Optional) Perform this operation on the specified interface.

routing-instance *routing-instance-name*—(Optional) Display DHCPv6 binding information for DHCPv6 clients on the specified routing instance.

brief—(Optional) Display brief information about the active client bindings.

detail—(Optional) Display detailed client binding information.

summary—(Optional) Display a summary of DHCPv6 client information.

Required Privilege Level view

Related Documentation

- clear dhcpv6 client binding on page 1646

List of Sample Output show dhcpv6 client binding on page 1762

Output Fields Table 71 on page 1761 lists the output fields for the **show dhcpv6 client binding** command. Output fields are listed in the approximate order in which they appear.

Table 71: show dhcpv6 client binding Output Fields

Field Name	Field Description
Hardware Address	Hardware address of the DHCPv6 client.
State	State of the address-binding table on the DHCPv6 local server.
Lease Expires	Date and time at which the client's IP address lease expires.
Lease Expires in	Number of seconds until the lease expires.
Lease Start	Date and time at which the client's IP address lease started.

Table 71: show dhcpv6 client binding Output Fields (continued)

Field Name	Field Description
Client DUID	The DHCPv6 client's unique identifier.
Bind type	The bind type.
Client Type	The type of DHCPv6 client. The client type can be autoconfig or stateful.
Rapid Commit	Two-message exchange option for address assignment.
Server IP Address	IP address of the DHCPv6 server.
Client IP Address	IP address of the DHCPv6 client.

Sample Output

show dhcpv6 client binding

```
user@host> show dhcpv6 client binding
IP prefix           Expires      ClientType  State  Interface       Client DUID
 2001:db8::b2b7:8631:d968:8d5e/128  96        STATEFUL   BOUND ge-0/0/1.0
LL_TIME0x3-0x0-2c:6b:f5:62:39:c1
```

```
user@host> show dhcpv6 client binding detail
Client Interface: ge-0/0/1.0
       Hardware Address:             2c:6b:f5:62:39:c1
       State:                        BOUND(DHCPV6_CLIENT_STATE_BOUND)
       Lease Expires:                2012-08-07 15:52:19 UTC
       Lease Expires in:             116 seconds
    Lease Start:                    2012-08-07 15:50:19 UTC
       Client DUID                   VENDOR0x00000583-0x3000103f
    Bind Type:                     IA_NA
    ClientType :                  STATEFUL
       Rapid Commit                  Off
       Server Ip Address:            fe80::230:48ff:fe5d:5bf7
       Client IP Address:            2001:db8::655b:3c80:2deb:1a3/128

     DHCP options:
      Name: server-identifier, Value: LL_TIME0x1-0x17acddab-00:30:48:5d:5b:f7
      Name: vendor-opts, Value: 000005830002aaaa
      Name: sip-server-list, Value: 2000::300 2000::302 2000::303 2000::304
      Name: dns-recursive-server, Value: 2000::ff2000::fe
      Name: domain-search-list, Value: 076578616d706c6503636f6d00
```

show dhcpv6 client statistics

Syntax

```
show dhcpv6 client statistics
routing-instance<routing-instance-name>
```

Release Information Statement introduced in Junos OS Release 12.1X45-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description Display Dynamic Host Configuration Protocol (DHCPv6) client statistics.

Options

routing-instance <routing-instance-name>—(Optional) Display the statistics for DHCPv6 clients on the specified routing instance.

Required Privilege Level view

Related Documentation

- clear dhcpv6 client statistics on page 1647

List of Sample Output show dhcpv6 client statistics on page 1764

Output Fields Table 72 on page 1763 lists the output fields for the **show dhcpv6 client statistics** command. Output fields are listed in the approximate order in which they appear.

Table 72: show dhcpv6 client statistics Output Fields

Field Name	Field Description
Dhcpv6 Packets dropped	Number of packets discarded by the DHCPv6 local server because of errors. Only nonzero statistics appear in the DHCPv6 Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.

Table 72: show dhcpv6 client statistics Output Fields (continued)

Field Name	Field Description
Messages sent	Number of DHCPv6 messages sent. • DHCPV6_DECLINE—Number of DHCPv6 PDUs of type DECLINE transmitted • DHCPV6_SOLICIT—Number of DHCPv6 PDUs of type SOLICIT transmitted • DHCPV6_INFORMATION_REQUEST—Number of DHCPv6 PDUs of type INFORMATION REQUEST transmitted • DHCPV6_RELEASE—Number of DHCPv6 PDUs of type RELEASE transmitted • DHCPV6_REQUEST—Number of DHCPv6 PDUs of type REQUEST transmitted • DHCPV6_CONFIRM—Number of DHCPv6 PDUs of type CONFIRM transmitted • DHCPV6_RENEW—Number of DHCPv6 PDUs of type RENEW transmitted • DHCPV6_REBIND—Number of DHCPv6 PDUs of type REBIND transmitted
Messages received	Number of DHCPv6 messages received. • DHCPV6_ADVERTISE—Number of DHCPv6 PDUs of type ADVERTISE received • DHCPV6_REPLY—Number of DHCPv6 PDUs of type REPLY received • DHCPV6_RECONFIGURE—Number of DHCPv6 PDUs of type RECONFIGURE received

Sample Output

show dhcpv6 client statistics

```
user@host> show dhcpv6 client statistics
Dhcpv6 Packets dropped:
      Total               0

   Messages sent:
      DHCPV6_DECLINE             0
      DHCPV6_SOLICIT             3
      DHCPV6_INFORMATION_REQUEST 6
      DHCPV6_RELEASE             1
      DHCPV6_REQUEST             2
      DHCPV6_CONFIRM             0
      DHCPV6_RENEW               0
      DHCPV6_REBIND              0

   Messages received:
      DHCPV6_ADVERTISE           3
      DHCPV6_REPLY               3
      DHCPV6_RECONFIGURE         0
```

show dhcpv6 relay binding

Syntax

```
show dhcpv6 relay binding
<address>
<brief>
<detail>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
<summary>
```

Release Information Command introduced in Junos OS Release 11.4.
interfaces-vlan and *interfaces-wildcard* options introduced in Junos OS Release 12.1.

Description Display the DHCPv6 address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.

Options ***address***—(Optional) One of the following identifiers for the DHCPv6 client whose binding state you want to show:

- *CID*—The specified Client ID (CID).
- *ipv6-prefix*—The specified IPv6 prefix.
- *session-id*—The specified session ID.

brief—(Optional) Display brief information about the active client bindings. This is the default, and produces the same output as **show dhcpv6 relay binding**.

detail—(Optional) Display detailed client binding information.

interface *interface-name*—(Optional) Perform this operation on the specified interface. You can optionally filter on VLAN ID and S-VLAN ID.

interfaces-vlan—(Optional) Interface VLAN ID or S-VLAN ID interface on which to show binding state information.

interfaces-wildcard—(Optional) Set of interfaces on which to show binding state information. This option supports the use of the wildcard character (*).

logical-system *logical-system-name*—(Optional) Perform this operation on the specified logical system.

routing-instance *routing-instance-name*—(Optional) Perform this operation on the specified routing instance.

summary—(Optional) Display a summary of DHCPv6 client information.

Required Privilege Level view

Related Documentation
- *Viewing and Clearing DHCP Bindings*
- clear dhcpv6 relay binding on page 1648

List of Sample Output
show dhcpv6 relay binding on page 1769
show dhcpv6 relay binding (Address) on page 1769
show dhcpv6 relay binding detail (Client ID) on page 1770
show dhcpv6 relay binding detail on page 1770
show dhcpv6 relay binding detail (Dual-Stack) on page 1771
show dhcpv6 relay binding detail (Multi-Relay Topology) on page 1771
show dhcpv6 relay binding (Session ID) on page 1771
show dhcpv6 relay binding (Subscriber with Multiple Addresses) on page 1771
show dhcpv6 relay binding detail (Subscriber with Multiple Addresses) on page 1772
show dhcpv6 relay binding (Interfaces VLAN) on page 1773
show dhcpv6 relay binding (Interfaces Wildcard) on page 1773
show dhcpv6 relay binding (Interfaces Wildcard) on page 1774
show dhcpv6 relay binding summary on page 1774

Output Fields Table 73 on page 1767 lists the output fields for the **show dhcpv6 relay binding** command. Output fields are listed in the approximate order in which they appear.

Table 73: show dhcpv6 relay binding Output Fields

Field Name	Field Description	Level of Output
number **clients, (*number* init, *number* bound, *number* selecting, *number* requesting, *number* renewing, *number* rebinding, *number* releasing)**	Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state.	**summary**
Client IPv6 Prefix	Prefix of the DHCPv6 client.	**brief detail**
Client IPv6 Excluded Prefix	IPv6 Prefix of the DHCP client excluded.	**detail**
Client DUID	DHCP for IPv6 Unique Identifier (DUID) of the client.	**brief detail**
Client IPv6 Address	IPv6 address assigned to the subscriber.	**detail**
Session Id	Session ID of the subscriber session.	**brief detail**
Expires	Number of seconds in which the lease expires.	**brief detail**

Table 73: show dhcpv6 relay binding Output Fields (continued)

Field Name	Field Description	Level of Output
State	State of the DHCPv6 relay address binding table on the DHCPv6 client: • **BOUND**—Client has an active IP address lease. • **INIT**—Initial state. • **REBINDING**—Client is broadcasting a request to renew the IP address lease. • **RECONFIGURE**—Client is broadcasting a request to reconfigure the IP address lease. • **RELEASE**—Client is releasing the IP address lease. • **RENEWING**—Client is sending a request to renew the IP address lease. • **REQUESTING**—Client is requesting a DHCPv6 server. • **SELECTING**—Client is receiving offers from DHCPv6 servers.	**brief detail**
Interface	Incoming client interface.	**brief**
Lease Expires	Date and time at which the client's IP address lease expires.	**detail**
Lease Expires in	Number of seconds in which the lease expires.	**detail**
Preferred Lease Expires	Date and UTC time at which the client's IPv6 prefix expires.	**detail**
Preferred Lease Expires in	Number of seconds at which the client's IPv6 prefix expires.	**detail**
Lease Start	Date and time at which the client's IP address lease started.	**detail**
Lease time violated	Lease time violation has occurred.	**detail**
Incoming Client Interface	Client's incoming interface.	**detail**
Server Address	IP address of the DHCPv6 server. Displays **unknown** for a DHCPv6 relay agent in a multi-relay topology that is not directly adjacent to the DHCPv6 server and does not detect the IP address of the server. In that case, the output instead displays the **Next Hop Server Facing Relay** field.	**detail**
Next Hop Server Facing Relay	Next-hop address in the direction of the DHCPv6 server.	**detail**
Server Interface	Interface of the DHCPv6 server.	**detail**
Relay Address	IP address of the relay.	**detail**
Client Pool Name	Address pool that granted the client lease.	**detail**
Client ID Length	Length of client ID.	All levels

Table 73: show dhcpv6 relay binding Output Fields (continued)

Field Name	Field Description	Level of Output
Client Id	Client ID.	All levels
Generated Circuit ID	Circuit ID generated by the DHCPv6 Interface-ID option (option 18)	**detail**
Generated Remote ID Enterprise Number	The Juniper Networks IANA private enterprise number	**detail**
Generated Remote ID	Remote ID generated by the DHCPv6 Remote-ID option (option 37)	**detail**
Dual Stack Group	Name of the dual-stack group for the DHCPv6 binding.	**detail**
Dual Stack Peer Address	Address of the dual-stack DHCPv4 peer.	**detail**

Sample Output

show dhcpv6 relay binding

```
user@host> show dhcpv6 relay binding
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:db8:3c4d:15::/64   1           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
2001:db8:3c4d:16::/64   2           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02
2001:db8:3c4d:17::/64   3           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03
2001:db8:3c4d:18::/64   4           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04
2001:db8:3c4d:19::/64   5           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05
2001:db8:3c4d:20::/64   6           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06
```

show dhcpv6 relay binding (Address)

```
user@host> show dhcp6 relay binding 2001:db8:1111:2222::/64 detail
Session Id:  1
     Client IPv6 Prefix:                    2001:db8:3c4d:15::/64
    Client DUID:                          LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01

     State:                                 BOUND(RELAY_STATE_BOUND)
     Lease Expires:                         2011-05-25 07:12:09 PDT
     Lease Expires in:                      77115 seconds
     Preferred Lease Expires:               2012-07-24 00:18:14 UTC
     Preferred Lease Expires in:            600 seconds
     Lease Start:                           2011-05-24 07:12:09 PDT
     Incoming Client Interface:             ge-1/0/0.0
     Server Address:                        2001:db8:aaaa:bbbb::1
     Server Interface:                      none
```

```
    Relay Address:                          2001:db8:1111:2222::
    Client Pool Name:                       pool-25
    Client Id Length:                       14
    Client Id:
/0x00010001/0x4bfa26af/0x00109400/0x0001
```

show dhcpv6 relay binding detail (Client ID)

```
user@host> show dhcpv6 relay binding 14/0x00010001/0x4bfa26af/0x00109400/0x0001
detail
```

```
Session Id:  1
     Client IPv6 Prefix:                   2001:db8:3c4d:15::/64
    Client DUID:                          LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01

     State:                                BOUND(RELAY_STATE_BOUND)
     Lease Expires:                        2011-05-25 07:12:09 PDT
     Lease Expires in:                     77115 seconds
     Preferred Lease Expires:              2012-07-24 00:18:14 UTC
     Preferred Lease Expires in:           600 seconds
     Lease Start:                          2011-05-24 07:12:09 PDT
     Lease time violated:                  yes
     Incoming Client Interface:            ge-1/0/0.0
     Server Address:                       2001:db8:aaaa:bbbb::1
     Server Interface:                     none
     Relay Address:                        2001:db8:1111:2222::
     Client Pool Name:                     pool-25
     Client Id Length:                     14
     Client Id:
/0x00010001/0x4bfa26af/0x00109400/0x0001
```

show dhcpv6 relay binding detail

```
user@host> show dhcpv6 relay binding detail
```

```
Session Id:  1
     Client IPv6 Prefix:                   2001:db8:3c4d:15::/64
    Client DUID:                          LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01

     State:                                BOUND(RELAY_STATE_BOUND)
     Lease Expires:                        2011-05-25 07:12:09 PDT
     Lease Expires in:                     77115 seconds
     Preferred Lease Expires:              2012-07-24 00:18:14 UTC
     Preferred Lease Expires in:           600 seconds
     Lease Start:                          2011-05-24 07:12:09 PDT
     Lease time violated:                  yes
     Incoming Client Interface:            ge-1/0/0.0
     Server Address:                       2001:db8:aaaa:bbbb::1
     Server Interface:                     none
     Relay Address:                        2001:db8:1111:2222::
     Client Pool Name:                     pool-25
     Client Id Length:                     14
     Client Id:
/0x00010001/0x4bfa26af/0x00109400/0x0001
     Generated Remote ID Enterprise Number: 1411
     Generated Remote ID:                  host:ge-1/0/0:100
```

show dhcpv6 relay binding detail (Dual-Stack)

```
user@host> show dhcpv6 relay binding detail
```

```
Session Id:  2
     Client IPv6 Prefix:                    2001:db8:ffff:0:4::/64
     Client IPv6 Address:                   2001:db8:3000:8003::1/128
     Client DUID:                           LL0x1-00:00:64:01:01:02
     State:                                 BOUND(DHCPV6_RELAY_STATE_BOUND)
     Lease Expires:                         2016-10-17 07:39:25 PDT
     Lease Expires in:                      3450 seconds
     Lease Start:                           2016-10-17 06:39:25 PDT
     Last Packet Received:                  2016-10-17 06:39:25 PDT
     Incoming Client Interface:             ae0.3221225472
     Client Interface Svlan Id:             2000
     Client Interface Vlan Id:              1
     Server Ip Address:                     2001:db8:3000::2
     Server Interface:                      none
     Client Profile Name:                   my-dual-stack
     Client Id Length:                      10
     Client Id:                             /0x00030001/0x00006401/0x0102
     Dual Stack Group:                      group1
     Dual Stack Peer Address:               192.0.2.4
```

show dhcpv6 relay binding detail (Multi-Relay Topology)

```
user@host > show dhcpv6 relay binding detail
```

```
Session Id:  13
     Client IPv6 Prefix:                    2001:db8:3000:0:8001::5/128
     Client DUID:                           LL0x1-00:00:65:03:01:02
     State:                                 BOUND(DHCPV6_RELAY_STATE_BOUND)
     Lease Expires:                         2011-11-21 06:14:50 PST
     Lease Expires in:                      293 seconds
     Preferred Lease Expires:               2012-07-24 00:18:14 UTC
     Preferred Lease Expires in:            600 seconds
     Lease Start:                           2011-11-21 06:09:50 PST
     Incoming Client Interface:             ge-1/0/0.0
     Server Address:                        unknown
     Next Hop Server Facing Relay:          2001:db8:4000::2
     Server Interface:                      none
     Client Id Length:                      10
     Client Id:                             /0x00030001/0x00006503/0x0102
```

show dhcpv6 relay binding (Session ID)

```
user@host> show dhcpv6 relay binding 41
```

```
Prefix                 Session Id   Expires   State   Interface    Client DUID
2001:db8:3c4d:15::/64   41           78837     BOUND   ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
```

show dhcpv6 relay binding (Subscriber with Multiple Addresses)

```
user@host> show dhcpv6 relay binding
```

```
Prefix                 Session Id  Expires  State    Interface    Client DUID
2001:db8:1001::1:24/128          23          593      BOUND    ge-9/0/9.0
LL_TIME0x1-0x55306754-00:10:94:00:00:02
2001:db8:1001::1:1c/128          23          393      BOUND    ge-9/0/9.0
```

```
LL_TIME0x1-0x55306754-00:10:94:00:00:02
2001:db8:1001::1:14/128          23          193      BOUND    ge-9/0/9.0
LL_TIME0x1-0x55306754-00:10:94:00:00:02
2001:db8:3001::300/120           23          293      BOUND    ge-9/0/9.0
LL_TIME0x1-0x55306754-00:10:94:00:00:02
2001:db8:3001::200/120           23          193      BOUND    ge-9/0/9.0
LL_TIME0x1-0x55306754-00:10:94:00:00:02
2001:db8:3001::100/120           23          93       BOUND    ge-9/0/9.0
LL_TIME0x1-0x55306754-00:10:94:00:00:02
```

When DHCPv6 relay binding is configured with prefix exclude option, we get the following output:

```
user@host> show dhcpv6 relay binding detail
```

```
Session Id:  6
     Hardware Address:                      00:10:94:00:00:01
     Client IPv6 Address:                   7001:2:3::d/128
     Lease Expires:                         2017-12-11 07:45:27 IST
     Lease Expires in:                      9999952 seconds
     Preferred Lease Expires:               2017-12-11 07:45:27 IST
     Preferred Lease Expires in:            9999952 seconds
     Client IPv6 Prefix:                    7001::1000:0:0:0/68
     Client IPv6 Excluded Prefix:           7001::1fff:ffff:ffff:ff00/120
     Lease Expires:                         2017-12-11 07:45:27 IST
     Lease Expires in:                      9999952 seconds
     Preferred Lease Expires:               2017-12-11 07:45:27 IST
     Preferred Lease Expires in:            9999952 seconds
    Client DUID:                          LL_TIME0x1-0x599553b0-00:10:94:00:00:01

     State:                                 BOUND(DHCPV6_RELAY_STATE_BOUND)
     Lease Start:                           2017-08-17 13:58:33 IST
     Last Packet Received:                  2017-08-17 13:58:48 IST
     Incoming Client Interface:             ge-0/0/0.100
     Client Interface Vlan Id:              100
     Server Ip Address:                     7002::1
     Server Interface:                      none
     Client Id Length:                      14
     Client Id:
/0x00010001/0x599553b0/0x00109400/0x0001
     Generated Circuit ID:                  ge-0/0/0:100
```

show dhcpv6 relay binding detail (Subscriber with Multiple Addresses)

```
user@host> show dhcpv6 relay binding detail
```

```
Session Id:  3
     Client IPv6 Address:                   2001:db8:1001::1:2/128
     Lease Expires:                         2015-05-15 02:34:51 PDT
     Lease Expires in:                      24 seconds
     Preferred Lease Expires:               2015-05-15 02:34:51 PDT
     Preferred Lease Expires in:            24 seconds
     Client IPv6 Address:                   2001:db8:1001::1:12/128
     Lease Expires:                         2015-05-15 02:41:31 PDT
     Lease Expires in:                      424 seconds
     Preferred Lease Expires:               2015-05-15 02:41:31 PDT
     Preferred Lease Expires in:            424 seconds
     Client IPv6 Address:                   2001:db8:1001::1:a/128
     Lease Expires:                         2015-05-15 02:38:11 PDT
     Lease Expires in:                      224 seconds
```

```
    Preferred Lease Expires:              2015-05-15 02:38:11 PDT
    Preferred Lease Expires in:           224 seconds
    Client IPv6 Prefix:                   2001:db8:3001::/120
    Lease Expires:                        2015-05-15 02:34:51 PDT
    Lease Expires in:                     24 seconds
    Preferred Lease Expires:              2015-05-15 02:34:51 PDT
    Preferred Lease Expires in:           24 seconds
    Client IPv6 Prefix:                   2001:db8:3001::200/120
    Lease Expires:                        2015-05-15 02:38:11 PDT
    Lease Expires in:                     224 seconds
    Preferred Lease Expires:              2015-05-15 02:38:11 PDT
    Preferred Lease Expires in:           224 seconds
    Client IPv6 Prefix:                   2001:db8:3001::100/120
    Lease Expires:                        2015-05-15 02:36:31 PDT
    Lease Expires in:                     124 seconds
    Preferred Lease Expires:              2015-05-15 02:36:31 PDT
    Preferred Lease Expires in:           124 seconds
   Client DUID:                         LL_TIME0x1-0x55554c6e-00:10:94:00:00:02

    State:                                BOUND(DHCPV6_RELAY_STATE_BOUND)
    Lease Start:                          2015-05-15 02:34:21 PDT
    Last Packet Received:                 2015-05-15 02:34:22 PDT
    Incoming Client Interface:            ge-9/0/9.0
    Client Interface Vlan Id:             111
    Demux Interface:                      demux0.3221225475
    Server Ip Address:                    2001:db8:5001::1
    Server Interface:                     none
    Client Profile Name:                  DHCP-IPDEMUX-PROF
    Client Id Length:                     14
    Client Id:
/0x00010001/0x55554c6e/0x00109400/0x0002
    Generated Circuit ID:                 ge-9/0/9:111
    Generated Remote ID Enterprise Number: 1411
    Generated Remote ID:                  ge-9/0/9:111
```

show dhcpv6 relay binding (Interfaces VLAN)

```
user@host> show dhcpv6 relay binding ge-1/0/0:100-200
Prefix           Session Id  Expires  State    Interface            Client DUID
2001:DB8::/32        11        87583    BOUND    ge-1/0/0.1073741827
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB8:19::/32     12       87583    BOUND    ge-1/0/0.1073741827
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
```

show dhcpv6 relay binding (Interfaces Wildcard)

```
user@host> show dhcpv6 relay binding demux0
Prefix            Session Id  Expires  State    Interface           Client DUID
2001:DB8::/32        30       79681    BOUND    demux0.1073741824
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB8:19::/32     31       79681    BOUND    demux0.1073741825
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB8:C9::/32     32       79681    BOUND    demux0.1073741826
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
```

show dhcpv6 relay binding (Interfaces Wildcard)

```
user@host> show dhcpv6 relay binding ge-1/3/*
Prefix            Session Id  Expires  State    Interface      Client DUID
2001:DB8::/32        22       79681    BOUND    ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB8:19::/32     33       79681    BOUND    ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB8:C9::/32     24       79681    BOUND    ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
```

show dhcpv6 relay binding summary

```
user@host> show dhcpv6 relay binding summary
5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
```

show dhcpv6 relay statistics

Syntax

```
show dhcpv6 relay statistics
<bulk-leasequery-connections>
<leasequery>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Release Information

Command introduced in Junos OS Release 11.4.
Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Switches.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.
bulk-leasequery-connections option introduced in Junos OS Release 16.1.

Description

Display Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay statistics.

Options

bulk-leasequery-connections—(Optional) Display DHCPv6 relay bulk leasequery statistics.

leasequery—(Optional) Display information about DHCPv6 relay individual leasequery statistics.

logical-system *logical-system-name*—(Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are displayed for the default logical system.

routing-instance *routing-instance-name*—(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are displayed for the default routing instance.

Required Privilege Level

view

Related Documentation

- clear dhcpv6 relay statistics on page 1651
- *DHCPv6 Client MAC Address Validation to Prevent Session Hijacking*

List of Sample Output

show dhcpv6 relay statistics on page 1777
show dhcpv6 relay statistics bulk-leasequery-connections on page 1778

Output Fields

Table 74 on page 1776 lists the output fields for the **show dhcpv6 relay statistics** command. Output fields are listed in the approximate order in which they appear.

Table 74: show dhcpv6 relay statistics Output Fields

Field Name	Field Description
DHCPv6 Packets dropped	Number of packets discarded by the extended DHCPv6 relay agent application due to errors. Only nonzero statistics appear in the **Packets dropped** output. When all of the Packets dropped statistics are 0 (zero), only the **Total** field appears. • **Total**—Total number of packets discarded by the DHCPV6 relay agent application. • **Bad options**—Number of packets discarded because invalid options were specified. • **Bad send**—Number of packets that the extended DHCP relay application could not send. • **Bad src address**—Number of packets discarded because the family type was not AF_INET6. • **Client MAC validation**—Number of packets discarded because validation of the client MAC address failed. • **No client id**—Number of packets discarded because they could not be matched to a client. • **Lease Time Violation**—Number of packets discarded because of a lease time violation • **No safd**—Number of packets discarded because they arrived on an unconfigured interface. • **Short packet**—Number of packets discarded because they were too short. • **Relay hop count**—Number of packets discarded because the hop count in the packet exceeded 32.
Messages received	Number of DHCPv6 messages received. • **DHCPv6_DECLINE**—Number of DHCPv6 PDUs of type DECLINE received • **DHCPV6_SOLICIT**—Number of DHCPv6 PDUs of type SOLICIT received • **DHCPV6_INFORMATION_REQUEST**—Number of DHCPv6 PDUs of type INFORMATION-REQUEST received • **DHCPV6_RELEASE**—Number of DHCPv6 PDUs of type RELEASE received • **DHCPV6_REQUEST**—Number of DHCPv6 PDUs of type REQUEST received • **DHCPV6_CONFIRM**—Number of DHCPv6 PDUs of type CONFIRM received **DHCPV6_RENEW**—Number of DHCPv6 PDUs of type RENEW received **DHCPV6_REBIND**—Number of DHCPv6 PDUs of type REBIND received **DHCPV6_RELAY_REPL**—Number of DHCPv6 PDUs of type RELAY-REPL received • **DHCPV6_RELAY_FORW**—Number of DHCPv6 RELAY-FORW PDUs received. • **DHCPV6_LEASEQUERY_REPLY**—Number of DHCPv6 replies received from the DHCPv6 sever • **DHCPV6_LEASEQUERY_DATA**—xxxx • **DHCPV6_LEASEQUERY_DONE**—The leasequery is complete
Messages sent	Number of DHCPv6 messages sent. • **DHCPV6_ADVERTISE**—Number of DHCPv6 ADVERTISE PDUs transmitted • **DHCP_REPLY**—Number of DHCPv6 REPLY PDUs transmitted • **DHCP_RECONFIGURE**—Number of DHCPv6 RECONFIGURE PDUs transmitted • **DHCP_RELAY_FORW**—Number of DHCPv6 RELAY-FORW PDUs transmitted • **DHCPV6_RELAY_REPL**—Number of DHCPv6 RELAY-REPL PDUs transmitted. • **DHCP6_LEASEQUERY**—Number of DHCP leasequery messages transmitted
Packets forwarded	Number of packets forwarded by the extended DHCPv6 relay agent application. • **FWD REQUEST**—Number of DHCPv6 REQUEST packets forwarded • **FWD REPLY**—Number of DHCPv6 REPLY packets forwarded

Table 74: show dhcpv6 relay statistics Output Fields (continued)

Field Name	Field Description
External Server Response	State of the external DHCP server responsiveness.
Total Requested Servers	Total number of servers with which the DHCP relay agent has requested a bulk leasequery connection.
Total Attempted Servers	Total number of servers with which the DHCP relay agent has attempted to create a bulk leasequery connection.
Total Connected	Total number of servers that have formed a bulk leasequery connection with the DHCP relay agent.
Total Terminated by Server	Total number of servers that have terminated a bulk leasequery connection with the DHCP relay agent.
Total Max Attempted	Total number of servers where the DHCP relay agent reached the maximum retry limit when it attempted to create a bulk leasequery connection.
Total Closed due to Errors	Total number of bulk leasequery connections that closed due to an internal error on the DHCP relay agent.
In-Flight Connected	Number of current bulk leasequery connections on the DHCP relay agent.
Bulk Leaasequery Reply Packet Retries	Number of bulk leasequery reply packets that the DHCP relay agent has retried.

Sample Output

show dhcpv6 relay statistics

```
user@host> show dhcpv6 relay statistics

DHCPv6 Packets dropped:
    Total                       2
    Lease Time Violation        1
    Client MAC validation       1

Messages received:
    DHCPV6_DECLINE              0
    DHCPV6_SOLICIT              10
    DHCPV6_INFORMATION_REQUEST  0
    DHCPV6_RELEASE              0
    DHCPV6_REQUEST              10
    DHCPV6_CONFIRM              0
    DHCPV6_RENEW                0
    DHCPV6_REBIND               0
    DHCPV6_RELAY_FORW           0
    DHCPV6_LEASEQUERY_REPLY     0
    DHCPV6_LEASEQUERY_DATA      0
    DHCPV6_LEASEQUERY_DONE      0

Messages sent:
```

```
    DHCPV6_ADVERTISE            0
    DHCPV6_REPLY                0
    DHCPV6_RECONFIGURE          0
    DHCPV6_RELAY_REPL           0
    DHCPV6_LEASEQUERY           0

Packets forwarded:
    Total                       4
    FWD REQUEST                 2
    FWD REPLY                   2

External Server Response:
    State                      Responding
```

show dhcpv6 relay statistics bulk-leasequery-connections

```
user@host> show dhcpv6 relay statistics bulk-leasequery-connections

Total Requested Servers:    0
Total Attempted Servers:    0
Total Connected:            0
Total Terminated by Server: 0
Total Max Attempted:        0
Total Closed due to Errors: 0
In-Flight Connected:        0
Bulk Leasequery Reply Packet Retries:   0
```

show dhcpv6 server binding

Syntax

```
show dhcpv6 server binding
<address>
<brief | detail | summary>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Release Information Command introduced in Junos OS Release 9.6.
Options *interfaces-vlan* and *interfaces-wildcard* added in Junos OS Release 12.1.

Description Display the address bindings in the client table on the extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server.

Options

address—(Optional) One of the following identifiers for the DHCPv6 client whose binding state you want to show:

- *CID*—The specified Client ID (CID).
- *ipv6-prefix*—The specified IPv6 prefix.
- *session-id*—The specified session ID.

brief | detail | summary—(Optional) Display the specified level of output about active client bindings. The default is **brief**, which produces the same output as **show dhcpv6 server binding**.

interface *interface-name*—(Optional) Display information about active client bindings on the specified interface. You can optionally filter on VLAN ID and SVLAN ID.

interfaces-vlan—(Optional) Interface VLAN ID or S-VLAN ID interface on which to show binding state information.

interfaces-wildcard—(Optional) Set of interfaces on which to show binding state information. This option supports the use of the wildcard character (*).

logical-system *logical-system-name*—(Optional) Display information about active client bindings for DHCPv6 clients on the specified logical system.

routing-instance *routing-instance-name*—(Optional) Display information about active client bindings for DHCPv6 clients on the specified routing instance.

Required Privilege Level view

Related Documentation

- *Viewing and Clearing DHCP Bindings*
- clear dhcpv6 server binding on page 1653

List of Sample Output

Output Fields

Table 75 on page 1780 lists the output fields for the **show dhcpv6 server binding** command. Output fields are listed in the approximate order in which they appear.

Table 75: show dhcpv6 server binding Output Fields

Field Name	Field Description	Level of Output
number clients, (*number* init, *number* bound, *number* selecting, *number* requesting, *number* renewing, *number* releasing)	Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state.	summary
Prefix	Client's DHCPv6 prefix, or prefix used to support multiple address assignment.	brief detail
Session Id	Session ID of the subscriber session.	brief detail
Expires	Number of seconds in which lease expires.	brief detail
State	State of the address binding table on the extended DHCPv6 local server: • **BOUND**—Client has active IP address lease. • **INIT**—Initial state. • **RECONFIGURE**—Server has sent reconfigure message to client. • **RELEASE**—Client is releasing IP address lease. • **RENEWING**—Client sending request to renew IP address lease. • **REQUESTING**—Client requesting a DHCPv6 server. • **SELECTING**—Client receiving offers from DHCPv6 servers.	brief detail
Interface	Interface on which the DHCPv6 request was received.	brief
Client IPv6 Address	Client's IPv6 address.	detail
Client IPv6 Prefix	Client's IPv6 prefix.	detail

Table 75: show dhcpv6 server binding Output Fields (continued)

Field Name	Field Description	Level of Output
Client IPv6 Excluded Prefix	IPv6 Prefix of the DHCP client excluded.	**detail**
Client DUID	Client's DHCP Unique Identifier (DUID).	**brief detail**
Lease expires	Date and time at which the client's IP address lease expires.	**detail**
Lease expires in	Number of seconds in which lease expires.	**detail**
Preferred Lease Expires	Date and UTC time at which the client's IPv6 prefix expires.	**detail**
Preferred Lease Expires in	Number of seconds at which client's IPv6 prefix expires.	**detail**
Lease Start	Date and time at which the client's address lease was obtained.	**detail**
Lease time violated	Lease time violation has occurred.	**detail**
Incoming Client Interface	Client's incoming interface.	**detail**
Server IP Address	IP address of DHCPv6 server.	**detail**
Server Interface	Interface of DHCPv6 server.	**detail**
Client Pool Name	Address pool used to assign IPv6 address.	**detail**
Client Prefix Pool Name	Address pool used to assign IPv6 prefix.	**detail**
Client Id length	Length of the DHCPv6 client ID, in bytes.	**detail**
Client Id	ID of the DHCPv6 client.	**detail**
Server Id	DHCP unique identifier (DUID) for the DHCPv6 server.	**detail**
Client Interface Svlan Id	S-VLAN ID of the client's incoming interface.	**detail**
Client Interface Vlan Id	VLAN ID of the client's incoming interface.	**detail**
Dual Stack Group	DHCPv6 server profile name.	**detail**
Dual Stack Peer Address	DHCPv6 Peer IP address.	**detail**

Sample Output

show dhcpv6 server binding

```
user@host> show dhcpv6 server binding
```

```
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:db8:1111:2222::/64 6           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:01
2001:db8:1111:2222::/64 7           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
2001:db8:1111:2222::/64 8           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
2001:db8:1111:2222::/64 9           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:04
2001:db8:1111:2222::/64 10          86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:05
2001:db8:2002::1/74 11              86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:06
```

show dhcpv6 server binding detail

```
user@host> show dhcpv6 server binding detail
```

```
Session Id:  2
     Client IPv6 Prefix:                    2001:db8:ffff:0:4::/64
     Client IPv6 Address:                   2001:db8:0:8003::1/128
     Client DUID:                           LL0x1-00:00:64:01:01:02
     State:                                BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)

     Lease Expires:                         2016-11-07 08:30:39 PST
     Lease Expires in:                      43706 seconds
     Preferred Lease Expires:               2016-11-07 08:30:39 PST
     Preferred Lease Expires in:            43706 seconds
     Lease Start:                           2016-11-04 11:00:37 PDT
     Last Packet Received:                  2016-11-06 09:00:39 PST
     Incoming Client Interface:             ae0.3221225472
     Client Interface Svlan Id:             2000
     Client Interface Vlan Id:              1
     Server Ip Address:                     2001:db8::2
     Server Interface:                      none
     Client Profile Name:                   my-dual-stack
     Client Id Length:                      10
     Client Id:                             /0x00030001/0x00006401/0x0102
     Dual Stack Group:                      my-dual-stack
     Dual Stack Peer Address:               192.0.2.10
```

When DHCPv6 binding is configured with prefix exclude option, we get the following output:

```
user@host> show dhcpv6 server binding detail
```

```
Session Id:  5
     Client IPv6 Address:                   2001:db8:2:3::d/128
     Lease Expires:                         2017-12-11 07:45:15 IST
     Lease Expires in:                      9999995 seconds
     Preferred Lease Expires:               2017-12-11 07:45:15 IST
     Preferred Lease Expires in:            9999995 seconds
     Client IPv6 Prefix:                    2001:db8::1000:0:0/68
```

```
   Client IPv6 Excluded Prefix:           2001:db8::1fff:ffff:ff00/120
    Lease Expires:                         2017-12-11 07:45:15 IST
    Lease Expires in:                      9999995 seconds
    Preferred Lease Expires:               2017-12-11 07:45:15 IST
    Preferred Lease Expires in:            9999995 seconds
   Client DUID:                          LL_TIME0x1-0x599553b0-00:10:94:00:00:01

    State:                                BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)

    Lease Start:                           2017-08-17 13:58:32 IST
    Last Packet Received:                  2017-08-17 13:58:36 IST
    Incoming Client Interface:             ge-0/0/0.0
    Client Interface Vlan Id:              100
    Client Pool Name:                      ia_na_pool
    Client Prefix Pool Name:               prefix_delegate_pool
    Client Id Length:                      14
    Client Id:
/0x00010001/0x599553b0/0x00109400/0x0001
    Relay Id Length:                       31
    Relay Id:
/0x00020000/0x05830130/0x303a3035/0x3a38363a
    Relay Id:
/0x34343a65/0x323a6330/0x00000000/0x000000
```

show dhcpv6 server binding interface

user@host> **show dhcpv6 server binding interface ge-1/0/0:10-101**

```
Prefix                 Session Id  Expires  State    Interface    Client DUID
2001:db8:1111:2222::/64 1          86055    BOUND    ge-1/0/0.100
LL_TIME0x1-0x4b0a53b9-00:10:94:00:00:01
```

show dhcpv6 server binding interface detail

user@host> **show dhcpv6 server binding interface ge-1/0/0:10-101 detail**

```
Session Id:  7
    Client IPv6 Prefix:                    2001:db8:1111:2222::/64
   Client DUID:                          LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

    State:                                 BOUND(bound)
    Lease Expires:                         2009-07-21 10:41:15 PDT
    Lease Expires in:                      86136 seconds
    Preferred Lease Expires:               2012-07-24 00:18:14 UTC
    Preferred Lease Expires in:            600 seconds
    Lease Start:                           2009-07-20 10:41:15 PDT
    Incoming Client Interface:             ge-1/0/0.0
    Server Ip Address:                     0.0.0.0
    Server Interface:                      none
    Client Id Length:                      14
    Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002
```

show dhcpv6 server binding (IPv6 Prefix)

user@host> **show dhcpv6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005 detail**

```
Session Id:  7
     Client IPv6 Prefix:                    2001:db8:1111:2222::/64
     Client DUID:                          LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

     State:                                 BOUND(bound)
     Lease Expires:                         2009-07-21 10:41:15 PDT
     Lease Expires in:                      86136 seconds
     Preferred Lease Expires:               2012-07-24 00:18:14 UTC
     Preferred Lease Expires in:            600 seconds
     Lease Start:                           2009-07-20 10:41:15 PDT
     Incoming Client Interface:             ge-1/0/0.0
     Server Ip Address:                     0.0.0.0
     Server Interface:                      none
     Client Id Length:                      14
     Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002
```

show dhcpv6 server binding (Session ID)

```
user@host> show dhcpv6 server binding 8
```

```
Prefix           Session Id  Expires  State    Interface    Client DUID
2001:db8::/32    8           86235    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
```

show dhcpv6 server binding (Interfaces VLAN)

```
user@host> show dhcpv6 server binding ge-1/0/0:100-200
```

```
Prefix            Session Id  Expires  State    Interface             Client DUID
2001:db8::/32     11          87583    BOUND    ge-1/0/0.1073741827
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:db8:19::/32     12       87583    BOUND    ge-1/0/0.1073741827
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
```

show dhcpv6 server binding (Interfaces Wildcard)

```
user@host> show dhcpv6 server binding demux0
```

```
Prefix            Session Id  Expires  State    Interface           Client DUID
2001:db8::/32     30          79681    BOUND    demux0.1073741824
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:db8:19::/32     31       79681    BOUND    demux0.1073741825
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:db8:C9::/32     32       79681    BOUND    demux0.1073741826
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
```

show dhcpv6 server binding (Interfaces Wildcard)

```
user@host> show dhcpv6 server binding ge-1/3/*
```

```
Prefix            Session Id  Expires  State    Interface      Client DUID
2001:db8::/32     22          79681    BOUND    ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:db8:19::/32     33       79681    BOUND    ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:db8:C9::/32     24       79681    BOUND    ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
```

show dhcpv6 server binding summary

```
user@host> show dhcpv6 server binding summary
5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
```

show dhcpv6 server binding (View)

Syntax

```
show dhcpv6 server binding
<brief | detail | summary>
<interface interface-name>
<routing-instance routing-instance-name>
```

Release Information Command introduced in Junos OS Release 10.4.

Description Display the address bindings in the client table for DCHPv6 local server.

Options

- brief | detail | summary—(Optional) Display the specified level of output about active client bindings. The default is **brief**, which produces the same output as **show dhcpv6 server binding**.
- interface *interface-name*—(Optional) Display information about active client bindings on the specified interface.
- routing-instance *routing-instance-name*—(Optional) Display information about active client bindings for DHCPv6 clients on the specified routing instance.

Required Privilege Level view

Related Documentation

- clear dhcpv6 server binding (Local Server) on page 1656

List of Sample Output

show dhcpv6 server binding on page 1787
show dhcpv6 server binding detail on page 1788
show dhcpv6 server binding interface on page 1788
show dhcpv6 server binding interface detail on page 1789
show dhcpv6 server binding prefix on page 1789
show dhcpv6 server binding session-id on page 1789
show dhcpv6 server binding summary on page 1789

Output Fields Table 75 on page 1780 lists the output fields for the **show dhcpv6 server binding** command. Output fields are listed in the approximate order in which they appear.

Table 76: show dhcv6p server binding Output Fields

Field Name	Field Description	Level of Output
number clients, (*number* init, *number* bound, *number* selecting, *number* requesting, *number* renewing, *number* releasing)	Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state.	**summary**

Table 76: show dhcv6p server binding Output Fields (continued)

Field Name	Field Description	Level of Output
Prefix	Client's DHCPv6 prefix.	**brief** **detail**
Session Id	Session ID of the subscriber session.	**brief** **detail**
Expires	Number of seconds in which lease expires.	**brief** **detail**
State	State of the address binding table on the DHCPv6 local server: • **BOUND**—Client has active IP address lease. • **INIT**—Initial state. • **RELEASE**—Client is releasing IP address lease. • **RECONFIGURE**—Client has received reconfigure message from server. • **RENEWING**—Client sending request to renew IP address lease. • **REQUESTING**—Client requesting a DHCPv6 server. • **SELECTING**—Client receiving offers from DHCPv6 servers.	**brief** **detail**
Interface	Interface on which the DHCPv6 request was received.	**brief**
Client DUID	Client's DHCP Unique Identifier (DUID).	**brief**
Lease expires	Date and time at which the client's IP address lease expires.	**detail**
Lease expires in	Number of seconds in which lease expires.	**detail**
Lease Start	Date and time at which the client's address lease was obtained.	**detail**
Incoming Client Interface	Client's incoming interface.	**detail**
Server IP Address	IP address of DHCPv6 server.	**detail**
Server Interface	Interface of DHCPv6 server.	**detail**
Client Id length	Length of the DHCPv6 client ID, in bytes.	**detail**
Client Id	ID of the DHCPv6 client.	**detail**
Server Id	ID type and ID of the DHCPv6 server.	**detail**

Sample Output

show dhcpv6 server binding

```
user@host> show dhcpv6 server binding
```

```
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:bd8:1111:2222::/64 6           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:01
2001:bd8:1111:2222::/64 7           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
2001:bd8:1111:2222::/64 8           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
2001:bd8:1111:2222::/64 9           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:04
2001:bd8:1111:2222::/64 10          86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:05
```

show dhcpv6 server binding detail

```
user@host> show dhcpv6 server binding detail
```

```
Session Id:  6
     Client IPv6 Prefix:                   2001:bd8:1111:2222::/64
     Client DUID:                         LL_TIME0x1-0x2e159c0-00:10:94:00:00:01

     State:                                BOUND(bound)
     Lease Expires:                        2009-07-21 10:41:15 PDT
     Lease Expires in:                     86308 seconds
     Lease Start:                          2009-07-20 10:41:15 PDT
     Incoming Client Interface:            ge-1/0/0.0
     Server Ip Address:                    0.0.0.0
     Server Interface:                     none
     Client Id Length:                     14
     Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0001      Server Id:
     <VENDOR 2198142976/4a4e3131324143433741464300000000000000000>

Session Id:  7
     Client IPv6 Prefix:                   2001:bd8:1111:2222::/64
     Client DUID:                         LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

     State:                                BOUND(bound)
     Lease Expires:                        2009-07-21 10:41:15 PDT
     Lease Expires in:                     86308 seconds
     Lease Start:                          2009-07-20 10:41:15 PDT
     Incoming Client Interface:            ge-1/0/0.0
     Server Ip Address:                    0.0.0.0
     Server Interface:                     none
     Client Id Length:                     14
     Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002      Server Id:
     <VENDOR 2198142976/4a4e3131324143433741464300000000000000000>
```

show dhcpv6 server binding interface

```
user@host> show dhcp6 server binding interface ge-1/0/0:10-101
```

```
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:bd8:1111:2222::/64 1           86055    BOUND    ge-1/0/0.100
LL_TIME0x1-0x4b0a53b9-00:10:94:00:00:01
```

show dhcpv6 server binding interface detail

user@host> **show dhcp6 server binding interface ge-1/0/0:10-101 detail**

```
Session Id:  7
     Client IPv6 Prefix:                   2001:bd8:1111:2222::/64
     Client DUID:                         LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

     State:                                BOUND(bound)
     Lease Expires:                        2009-07-21 10:41:15 PDT
     Lease Expires in:                     86136 seconds
     Lease Start:                          2009-07-20 10:41:15 PDT
     Incoming Client Interface:            ge-1/0/0.0
     Server Ip Address:                    0.0.0.0
     Server Interface:                     none
     Client Id Length:                     14
     Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002      Server Id:
     <VENDOR 2198142976/4a4e3131324143433741464300000000000000000>
```

show dhcpv6 server binding prefix

user@host> **show dhcp6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005 detail**

```
Session Id:  7
     Client IPv6 Prefix:                   2001:bd8:1111:2222::/64
     Client DUID:                         LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

     State:                                BOUND(bound)
     Lease Expires:                        2009-07-21 10:41:15 PDT
     Lease Expires in:                     86136 seconds
     Lease Start:                          2009-07-20 10:41:15 PDT
     Incoming Client Interface:            ge-1/0/0.0
     Server Ip Address:                    0.0.0.0
     Server Interface:                     none
     Client Id Length:                     14
     Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002
```

show dhcpv6 server binding session-id

user@host> **show dhcpv6 server binding 8**

```
Prefix                 Session Id  Expires  State    Interface    Client DUID
2001:bd8:1111:2222::/64 8          86235    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
```

show dhcpv6 server binding summary

user@host> **show dhcpv6 server binding summary**

```

5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)

```

show dhcpv6 server statistics

Syntax

```
show dhcpv6 server statistics
<bulk-leasequery-connections>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Release Information

Command introduced in Junos OS Release 9.6.
bulk-leasequery-connections option introduced in Junos OS Release 16.1.

Description

Display extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.

Options

bulk-leasequery-connections—(Optional) Display information about DHCPv6 local server bulk leasequery statistics.

logical-system *logical-system-name*—(Optional) Display information about extended DHCPv6 local server statistics on the specified logical system. If you do not specify a logical system, statistics are displayed for the default logical system.

routing-instance *routing-instance-name*—(Optional) Display information about extended DHCPv6 local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.

Required Privilege Level

view

Related Documentation

- clear dhcpv6 server statistics on page 1657
- *DHCPv6 Client MAC Address Validation to Prevent Session Hijacking*

List of Sample Output

show dhcpv6 server statistics on page 1792
show dhcpv6 server statistics bulk-leasequery-connections on page 1793

Output Fields

Table 77 on page 1791 lists the output fields for the **show dhcpv6 server statistics** command. Output fields are listed in the approximate order in which they appear.

Table 77: show dhcpv6 server statistics Output Fields

Field Name	Field Description
Packets dropped	Number of packets discarded by the extended DHCPv6 local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears. • **Total**—Total number of packets discarded by the extended DHCPv6 local server • **Strict Reconfigure**—Number of solicit messages discarded because the client does not support reconfiguration • **Bad hardware address**—Number of packets discarded because an invalid hardware address was specified • **Bad opcode**—Number of packets discarded because an invalid operation code was specified • **Bad options**—Number of packets discarded because invalid options were specified • **Client MAC validation**—Number of packets discarded because validation of the client MAC address failed. • **Invalid server address**—Number of packets discarded because an invalid server address was specified • **Lease Time Violation**—Number of packets discarded because of a lease time violation • **No available addresses**—Number of packets discarded because there were no addresses available for assignment • **No interface match**—Number of packets discarded because they did not belong to a configured interface • **No routing instance match**—Number of packets discarded because they did not belong to a configured routing instance • **No valid local address**—Number of packets discarded because there was no valid local address • **Packet too short**—Number of packets discarded because they were too short • **Read error**—Number of packets discarded because of a system read error • **Send error**—Number of packets that the extended DHCPv6 local server could not send
Advertise Delay	Number of DHCP advertise messages delayed. • **DELAYED**—Number of DHCPv6 advertise packets that have been sent after being delayed. • **INPROGRESS**—Number of DHCPv6 advertise packets that are in the delay queue. • **TOTAL**—Total number of delayed DHCPv6 advertise messages; sum of **DELAYED** and **INPROGRESS**.
Messages received	Number of DHCPv6 messages received. • **DHCPV6_CONFIRM**—Number of DHCPv6 CONFIRM PDUs received. • **DHCPV6_DECLINE**—Number of DHCPv6 DECLINE PDUs received. • **DHCPV6_INFORMATION_REQUEST**—Number of DHCPv6 INFORMATION-REQUEST PDUs received. • **DHCPV6_REBIND**—Number of DHCPv6 REBIND PDUs received. • **DHCPV6_RELAY_FORW**—Number of DHCPv6 RELAY-FORW PDUs received. • **DHCPV6_RELAY_REPL**—Number of DHCPv6 RELAY-REPL PDUs received. • **DHCPV6_RELEASE**—Number of DHCPv6 RELEASE PDUs received. • **DHCPV6_RENEW**—Number of DHCPv6 RENEW PDUs received. • **DHCPV6_REQUEST**—Number of DHCPv6 REQUEST PDUs received. • **DHCPV6_SOLICIT**—Number of DHCPv6 SOLICIT PDUs received. • **DHCPV6_LEASEQUERY**—Number of DHCPv6 leasequery messages received.

Table 77: show dhcpv6 server statistics Output Fields (continued)

Field Name	Field Description
Messages sent	Number of DHCPv6 messages sent. • **DHCPV6_ADVERTISE**—Number of DHCPv6 ADVERTISE PDUs transmitted. • **DHCPV6_REPLY**—Number of DHCPv6 ADVERTISE PDUs transmitted. • **DHCPV6_LOGICAL_NAK**—Number of logical NAK messages sent, signifying T1 and T2 timers with values of zero; subset of **DHCPV6_REPLY** counter. (Displays only at **verbose** level. • **DHC6_RECONFIGURE**—Number of DHCPv6 RECONFIGURE PDUs transmitted. • **DHCPV6_RELAY_REPL**—Number of DHCPv6 RELAY-REPL PDUs transmitted. • **DHCPV6_RELAY_FORW**—Number of DHCPv6 RELAY-FORW PDUs transmitted. • **DHCPV6_LEASEQUERY_REPLY**—Number of DHCPv6 leasequery replies transmitted to the DHCPv6 relay agent. • **DHCPV6_LEASEQUERY_DATA**—Number of DHCPv6 LEASEQUERY-DATA packets transmitted. • **DHCPV6_LEASEQUERY_DONE**—Number of DHCPv6 LEASEQUERY-DONE packets sent.

Sample Output

show dhcpv6 server statistics

```
user@host> show dhcpv6 server statistics

Dhcpv6 Packets dropped:
    Total                     2
    Lease Time Violation      1
    Client MAC validation     1

Advertise Delay:
    DELAYED                   3
    INPROGRESS                9
    TOTAL                    12

Messages received:
    DHCPV6_DECLINE            0
    DHCPV6_SOLICIT            9
    DHCPV6_INFORMATION_REQUEST 0
    DHCPV6_RELEASE            0
    DHCPV6_REQUEST            5
    DHCPV6_CONFIRM            0
    DHCPV6_RENEW              0
    DHCPV6_REBIND             0
    DHCPV6_RELAY_FORW         0

    DHCPV^_LEASEQUERY         0

Messages sent:
    DHCPV6_ADVERTISE          9
    DHCPV6_REPLY              5
    DHCPV6_RECONFIGURE        0
    DHCPV6_RELAY_REPL         0
    DHCPV6_LEASEQUERY_REPLY   0
    DHCPV6_LEASEQUERY_DATA    0
    DHCPV6_LEASEQUERY_DONE    0
```

show dhcpv6 server statistics bulk-leasequery-connections

```
user@host> show dhcpv6 server statistics bulk-leasequery-connections

Total Accepted Connections:                    0
Total Not-Accepted Connections:                0
Connections Closed due to Errors:              0
Connections Closed due to max-empty-replies:   0
In-flight Connections:                         0
```

show dhcpv6 server statistics (View)

Syntax

```
show dhcpv6 server statistics
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Release Information Command introduced in Junos OS Release 10.4.

Description Display DHCPv6 local server statistics.

Options

logical-system *logical-system-name*—(Optional) Display information about extended DHCPv6 local server statistics on the specified logical system. If you do not specify a logical system, statistics are displayed for the default logical system.

routing-instance *routing-instance-name*—(Optional) Display information about DHCPv6 local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.

Required Privilege Level view

Related Documentation

- clear dhcpv6 server statistics (Local Server) on page 1658

List of Sample Output show dhcpv6 server statistics on page 1796

Output Fields Table 78 on page 1795 lists the output fields for the **show dhcpv6 server statistics** command. Output fields are listed in the approximate order in which they appear.

Table 78: show dhcpv6 server statistics Output Fields

Field Name	Field Description
Dhcpv6 Packets dropped	Number of packets discarded by the DHCPv6 local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears. • **Total**—Total number of packets discarded by the DHCPv6 local server • **Authentication**—Number of packets discarded because they could not be authenticated • **Strict Reconfigure**—Number of solicit messages discarded because the client does not support reconfiguration • **Bad hardware address**—Number of packets discarded because an invalid hardware address was specified • **Bad opcode**—Number of packets discarded because an invalid operation code was specified • **Bad options**—Number of packets discarded because invalid options were specified • **Invalid server address**—Number of packets discarded because an invalid server address was specified • **No available addresses**—Number of packets discarded because there were no addresses available for assignment • **No interface match**—Number of packets discarded because they did not belong to a configured interface • **No routing instance match**—Number of packets discarded because they did not belong to a configured routing instance • **No valid local address**—Number of packets discarded because there was no valid local address • **Packet too short**—Number of packets discarded because they were too short • **Read error**—Number of packets discarded because of a system read error • **Send error**—Number of packets that the DHCPv6 local server could not send
Messages received	Number of DHCPv6 messages received. • **DHCPV6_CONFIRM**—Number of DHCPv6 CONFIRM PDUs received. • **DHCPV6_DECLINE**—Number of DHCPv6 DECLINE PDUs received. • **DHCPV6_INFORMATION_REQUEST**—Number of DHCPv6 INFORMATION-REQUEST PDUs received. • **DHCPV6_REBIND**—Number of DHCPv6 REBIND PDUs received. • **DHCPV6_RELAY_FORW**—Number of DHCPv6 RELAY-FORW PDUs received from a relay by the DHCPv6 server. • **DHCPV6_RELEASE**—Number of DHCPv6 RELEASE PDUs received. • **DHCPV6_RENEW**—Number of DHCPv6 RENEW PDUs received. • **DHCPV6_REQUEST**—Number of DHCPv6 REQUEST PDUs received. • **DHCPV6_SOLICIT**—Number of DHCPv6 SOLICIT PDUs received.
Messages sent	Number of DHCPv6 messages sent. • **DHCPV6_ADVERTISE**—Number of DHCPv6 ADVERTISE PDUs transmitted. • **DHCPV6_REPLY**—Number of DHCPv6 ADVERTISE PDUs transmitted. • **DHC6_RECONFIGURE**—Number of DHCPv6 RECONFIGURE PDUs transmitted. • **DHCPV6_RELAY_REPL**—Number of DHCPv6 RELAY-REPL PDUs sent from DHCPv6 server to DHCPv6 relay.

Sample Output

show dhcpv6 server statistics

```
user@host> show dhcpv6 server statistics
Dhcpv6 Packets dropped:
    Total               0

Messages received:
    DHCPV6_DECLINE             0
    DHCPV6_SOLICIT             9
    DHCPV6_INFORMATION_REQUEST 0
    DHCPV6_RELEASE             0
    DHCPV6_REQUEST             5
    DHCPV6_CONFIRM             0
    DHCPV6_RENEW               0
    DHCPV6_REBIND              0
    DHCPV6_RELAY_FORW          0
   Messages sent:
    DHCPV6_ADVERTISE           9
    DHCPV6_REPLY               5
    DHCPV6_RECONFIGURE         0
    DHCPV6_RELAY_REPL          0
```

show firewall (View)

Syntax

```
show firewall
<filter filter-name>
<counter counter-name>
<log>
<prefix-action-stats>
<terse>
```

Release Information Command introduced before Junos OS Release 10.0 .

Description Display statistics about configured firewall filters.

Options

none—Display statistics about configured firewall filters.

filter *filter-name*—Name of a configured filter.

counter *counter-name*—Name of a filter counter.

log—Display log entries for firewall filters.

prefix-action-stats—Display prefix action statistics for firewall filters.

terse—Display firewall filter names only.

Required Privilege Level view

Related Documentation

- *firewall*

List of Sample Output show firewall on page 1798

Output Fields Table 79 on page 1797 lists the output fields for the **show firewall** command. Output fields are listed in the approximate order in which they appear.

Table 79: show firewall Output Fields

Field Name	Field Description
Filter	Name of a filter that has been configured with the **filter** at the **[edit firewall]** hierarchy level. When an interface-specific filter is displayed, the name of the filter is followed by the full interface name and by either **-i** for an input filter or **-o** for an output filter. When dynamic filters are displayed, the name of the filter is followed by the full interface name and by either **-in** for an input filter or **-out** for an output filter. When a logical system–specific filter is displayed, the name of the filter is prefixed with two underscore (__) characters and the name of the logical system (for example, **__ls1/filter1**).

Table 79: show firewall Output Fields (continued)

Field Name	Field Description
Counters	Display filter counter information: • **Name**—Name of a filter counter that has been configured with the **counter** firewall filter action. • **Bytes**—Number of bytes that match the filter term under which the **counter** action is specified. • **Packets**—Number of packets that matched the filter term under which the **counter** action is specified.
Policers	Display policer information: • **Name**—Name of policer. • **Bytes**—Number of bytes that match the filter term under which the policer action is specified. This is only the number out-of-specification (out-of-spec) byte counts, not all the bytes in all packets policed by the policer. • **Packets**—Number of packets that matched the filter term under which the policer action is specified. This is only the number of out-of-specification (out-of-spec) packet counts, not all packets policed by the policer.

Sample Output

show firewall

```
user@host> show firewall
Filter: ef_path
Counters:
Name                                            Bytes              Packets
def-count                                       0                    0
video-count                                     0                    0
voice-count                                     0                    0

Filter: __default_bpdu_filter__

Filter: deep
Counters:
Name                                            Bytes              Packets
deep2                                           302076               5031

Filter: deep-flood
Counters:
Name                                            Bytes              Packets
deep_flood_def                                  302136               5032
deep1                                           0                    0
Policers:
Name                                                        Packets
deep-pol-op-first                                             0
```

show dot1x

Syntax

```
show dot1x
<brief | detail>
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description

Display the current operational state of all ports with the list of connected users.

This command displays the list of connected supplicants received from the RADIUS authentication server regardless of the session state—that is, for both authenticated supplicants and for supplicants that attempted authentication.

Options

none—Display information for all authenticator ports.

brief | detail—(Optional) Display the specified level of output.

interface *interface-name*—(Optional) Display information for the specified port with a list of connected supplicants.

Required Privilege Level

view

Related Documentation

- clear dot1x on page 1659
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 309
- Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 315
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 297
- Verifying 802.1X Authentication on page 321

List of Sample Output

show dot1x interface brief on page 1803
show dot1x interface detail on page 1803

Output Fields

Table 80 on page 1800 lists the output fields for the **show dot1x** command. Output fields are listed in the approximate order in which they appear.

Table 80: show dot1x Output Fields

Field Name	Field Description	Level of Output
Interface	Name of a port.	All levels
MAC address	The MAC address of the connected supplicant on the port.	All levels
Role	The 802.1X authentication role of the interface. When 802.1X is enabled on an interface, the role is **Authenticator**. As **Authenticator**, the interface blocks LAN access until a supplicant is authenticated through 802.1X or MAC RADIUS authentication.	**brief**, **detail**
State	The state of the port: • **Authenticated**—The supplicant has been authenticated through the RADIUS server or has been permitted access through server fail fallback. • **Authenticating**—The supplicant is authenticating through the RADIUS server. • **Held**—An action has been triggered through server fail fallback during a RADIUS server timeout. A supplicant is denied access, permitted access through a specified VLAN, or maintains the authenticated state granted to it before the RADIUS server timeout occurred.	**brief**
User	The username of the connected supplicant.	**brief**
Administrative state	The administrative state of the port: • **auto**—Traffic is allowed through the port based on the authentication result (by default). • **force-authorize**—All traffic flows through the port irrespective of the authentication result. This state is not allowed on an interface whose VLAN membership has been set to **dynamic**. • **force-unauthorize**—All traffic drops on the port irrespective of the authentication result. This state is not allowed on an interface whose VLAN membership has been set to **dynamic**.	**detail**
Supplicant	The mode for the supplicant: • **single**—Only the first supplicant is authenticated. All other supplicants who connect later to the port are allowed full access without any further authentication. They effectively “piggyback” on the first supplicant’s authentication. • **single-secure**—Only one supplicant is allowed to connect to the port. No other supplicant is allowed to connect until the first supplicant logs out. • **multiple**—Multiple supplicants are allowed to connect to the port. Each supplicant is authenticated individually.	**detail**
Quiet period	The number of seconds the port waits following a failed authentication exchange with the supplicant before reattempting the authentication. The default value is 60 seconds. The range is 0 through 65,535 seconds.	**detail**
Transmit period	The number of seconds the port waits before retransmitting the initial EAPOL PDUs to the supplicant. The default value is 30 seconds. The range is 1 through 65,535 seconds.	**detail**

Table 80: show dot1x Output Fields (continued)

Field Name	Field Description	Level of Output
MAC radius	MAC RADIUS authentication: • **enabled**—The switch sends an EAPOL request to the connecting host to attempt 802.1X authentication and if the connecting host is unresponsive, the switch tries to authenticate the host by using the MAC address. • **disabled**—The default. The switch does not attempt to authenticate the MAC address of the connecting host.	**detail**
MAC radius authentication protocol	MAC RADIUS authentication protocol: • **EAP-MD5**—The EAP-MD5 protocol is used for MAC RADIUS authentication. EAP-MD5 is an authentication method belonging to the Extensible Authentication Protocol (EAP) authentication framework. EAP-MD5 is the default authentication protocol. • **PAP**—The Password Authentication Protocol (PAP) authentication protocol is used for MAC RADIUS authentication.	**detail**
MAC radius restrict	The authentication method is restricted to MAC RADIUS only. 802.1X authentication is not enabled.	**detail**
Reauthentication	The reauthentication state: • **disable**—Periodic reauthentication of the client is disabled. • **interval**—Sets the periodic reauthentication time interval. The default value is 3600 seconds. The range is 1 through 65,535 seconds.	**detail**
Supplicant timeout	The number of seconds the port waits for a response when relaying a request from the authentication server to the supplicant before resending the request. The default value is 30 seconds. The range is 1 through 60 seconds.	**detail**
Server timeout	The number of seconds the port waits for a reply when relaying a response from the supplicant to the authentication server before timing out. The default value is 30 seconds. The range is 1 through 60 seconds.	**detail**
Maximum EAPOL requests	The maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out. The default value is 2. The range is 1 through 10.	**detail**
Number of clients bypassed because of authentication	The number of non-802.1X clients granted access to the LAN by means of static MAC bypass. The following fields are displayed: • **Client**—MAC address of the client. • **vlan** —The name of the VLAN to which the client is connected.	**detail**
Guest VLAN member	The VLAN to which a supplicant is connected when the supplicant is authenticated using a guest VLAN. If a guest VLAN is not configured on the interface, this field displays <**not configured**>.	**detail**
Multi domain data session count	The number of data sessions that have been authenticated on a multi-domain authentication interface.	**detail**

Table 80: show dot1x Output Fields (continued)

Field Name	Field Description	Level of Output
Number of connected supplicants	The number of supplicants connected to a port.	**detail**
Supplicant	The username and MAC address of the connected supplicant.	**detail**
Authentication method	The authentication method used for a supplicant: • **CWA Authentication**—A supplicant is authenticated by the central Web authentication (CWA) server. • **Fail**—Authentication failed and supplicant is in **Held** state. • **Guest VLAN**—A supplicant is connected to the LAN through the guest VLAN. • **MAC RADIUS**—A nonresponsive host is authenticated based on its MAC address. The MAC address is configured as permitted on the RADIUS server, the RADIUS server lets the switch know that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected. • **RADIUS**—A supplicant is configured on the RADIUS server, the RADIUS server communicates this to the switch, and the switch opens LAN access on the interface to which the supplicant is connected. • **Server-fail**—One of the following fallback actions is in effect because the RADIUS server is unreachable. Indicates whether EAPOL block is in effect, and the amount of time remaining for EAPOL block (in seconds). ◦ **deny**—The supplicant is denied access to the LAN, preventing traffic from flowing from the supplicant through the interface. This is the default server fail fallback action. ◦ **permit**—The supplicant is permitted access to the LAN as if the supplicant had been successfully authenticated by the RADIUS server. ◦ **use-cache**—In the event that the RADIUS server times out when the supplicant is attempting reauthentication, the supplicant is reauthenticated only if it was previously authenticated; otherwise, the supplicant is denied LAN access. ◦ **VLAN**—The supplicant is configured to be moved to a specified VLAN if the RADIUS server is unavailable to reauthenticate the supplicant. (The VLAN must already exist on the switch.) • **Server-reject VLAN**—The supplicant received a RADIUS access-reject message from the authentication server and was moved to a server-reject VLAN, a specified VLAN already configured on the switch.	**detail**
Authenticated VLAN	The VLAN to which the supplicant is connected.	**detail**
Dynamic filter	User policy filter sent by the RADIUS server.	**detail**
Session Reauth interval	The configured reauthentication interval.	**detail**
Reauthentication due in	The number of seconds in which reauthentication will occur again for the connected supplicant.	**detail**
Session Accounting Interim Interval	The number of seconds between interim RADIUS accounting messages.	**detail**

Table 80: show dot1x Output Fields (continued)

Field Name	Field Description	Level of Output
Accounting Update due in	The number of seconds until the next interim RADIUS accounting update is due.	**detail**
CWA Redirect URL	The URL used to redirect the supplicant to a central Web server for authentication.	**detail**
Eapol Block	Shows whether EAPOL block is in effect or not in effect.	**detail**

Sample Output

show dot1x interface brief

```
user@switch> show dot1x interface brief
802.1X Information:
Interface     Role           State           MAC address          User
ge-0/0/1      Authenticator  Authenticated   00:a0:d2:18:1a:c8    user1
ge-0/0/2      Authenticator  Connecting
ge-0/0/3      Authenticator  Held            00:a6:55:f2:94:ae    user3
```

show dot1x interface detail

```
user@switch> show dot1x interface ge-0/0/16.0 detail

ge-0/0/16.0
 Role: Authenticator
 Administrative state: Auto
 Supplicant mode: Single
 Number of retries: 3
 Quiet period: 60 seconds
 Transmit period: 30 seconds
 Mac Radius: Enabled
 Mac Radius Restrict: Disabled
 Mac Radius Authentication Protocol: PAP
 Reauthentication: Enabled
 Configured Reauthentication interval: 3600 seconds
 Supplicant timeout: 30 seconds
 Server timeout: 30 seconds
 Maximum EAPOL requests: 2
 Guest VLAN member: <not configured>
 Number of connected supplicants: 2
   Supplicant: abc, 00:30:48:8C:66:BD
     Operational state: Authenticated
     Authentication method: Radius
     Authenticated VLAN: v200
     Session Reauth interval: 3600 seconds
     Reauthentication due in 3587 seconds
     Eapol-Block: Not In Effect
  Supplicant: 000303030303, 00:03:03:03:03:03
     Operational state: Authenticated
     Backend Authentication state: Idle
     Authentication method: Mac Radius
     Authenticated VLAN: dyn_vlan2
```

```
    Session Reauth interval: 3600 seconds
    Reauthentication due in 3587 seconds
    Eapol-Block: In Effect
```

show dot1x accounting attribute

Syntax **show dot1x accounting attribute**

Release Information Command introduced in JUNOS Release 16.1 for EX Series switches.

Description Display the RADIUS accounting attributes sent by the switch, operating as the network access server (NAS), to the RADIUS accounting server. RADIUS accounting attributes convey information that is used to account for a service provided to an authenticated user. The user session statistics are recorded by the accounting server in an accounting log file.

RADIUS accounting attributes are included in Accounting-Request messages sent from the switch to the accounting server. Attribute information is created only if the data for the attribute is available.

Required Privilege Level view

Related Documentation

- show dot1x on page 1799
- clear dot1x on page 1659
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 368
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 297

List of Sample Output show dot1x accounting-attributes on page 1806

Output Fields Table 81 on page 1806 lists the output fields for the **show dot1x accounting-attributes** command. Output fields are listed in the approximate order in which they appear.

Table 81: show dot1x accounting attribute Output Fields

Field Name	Field Description
Accounting attributes	Shows the value for the RADIUS accounting attributes sent from the NAS to the server. An attribute is displayed only if data is available for that attribute value. The following RADIUS accounting attributes are supported: • User-Name—The name of the authenticated user. • NAS-Port—The physical port number of the NAS which is authenticating the user. • Framed-IP-Address—The IP address of the authenticated user. • Filter-ID—The name of the filter list for the authenticated user. • Framed-MTU—The maximum transmission unit that can be configured for user. • Client-System-Name—This is a vendor-specific attribute (VSA) used to indicate the client host name. Supported for LLDP-capable devices only. • Session-Timeout—The maximum number of seconds that a session will stay active before termination of the session or prompt. • Called-Station-ID—Allows the NAS to send the phone number that the user called, using Dialed Number Identification (DNIS) or similar technology. • Calling-Station-ID—Allows the NAS to send the phone number that the call came from, using Dialed Number Identification (DNIS) or similar technology. • NAS-Identifier—Contains a string identifying the NAS originating the Accounting-Request. • Acct-Status-Type—Indicates whether this Accounting-Request marks the beginning of the user session (Start) or the end (Stop). Can also be used for an interim update (Interim-Update). • Acct-Authentic—Indicates whether the user was authenticated locally (Local), by the RADIUS server (RADIUS), or by another remote authentication protocol (Remote). • Acct-Session-ID—A unique ID for a specific accounting session that can be used to match start and stop records for a session in the log file. • Event-Timestamp—Records the time an event occurred. • NAS-Port-ID—The port of the NAS that is authenticating the user. • Framed-IPv6-Address—The IPv6 address of the authenticated user.

Sample Output

show dot1x accounting-attributes

```
user@switch> show dot1x accounting-attributes

Accounting Attribute:
      Calling Station Id:               88-e0-f3-1f-c5-e0
      Called station Id:                00-10-94-00-00-02
      Framed Ipv6 Address               :2001:db8:0:1:2a0:a514:0:24d
      Accounting Session ID:            802.1x812f00250002dcc6
      Client System Name:               AVX149485
      Session-Timeout:                  120s
      Framed-MTU:                       492
      Acct-Authentic:                   RADIUS
      Nas-Port-ID                       ge-0/0/5.0
```

show dot1x authentication-failed-users

Syntax show dot1x authentication-failed-users

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description Display the supplicants (users) that have failed 802.1X authentication.

Required Privilege Level view

Related Documentation
- clear dot1x on page 1659
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 368
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292

List of Sample Output show dot1x authentication-failed-users on page 1807

Output Fields Table 82 on page 1807 lists the output fields for the **show dot1x authentication-failed-users** command. Output fields are listed in the approximate order in which they appear.

Table 82: show dot1x authentication-failed-users Output Fields

Field Name	Field Description	Level of Output
Interface	The MAC address configured to bypass 802.1X authentication.	**all**
MAC address	The MAC address configured statically on the interface.	**all**
User	The user that is configured on the RADIUS server and that has failed 802.1X authentication.	**all**
Failure Count	The number of times that 802.1X authentication has failed on the interface.	**all**

Sample Output

show dot1x authentication-failed-users

```
user@switch> show dot1x authentication-failed-users

Interface     MAC address          User            Failure Count
ge-0/0/17.0   00:37:00:00:00:00    003700000000        28
ge-0/0/20.0   00:04:10:00:00:00    000410000000        32
```

```
ge-0/0/18.0    00:00:03:00:0a:00     000003000a00          4
ge-0/0/19.0    00:00:03:00:0b:00     000003000b00          18
```

show dot1x firewall

Syntax show dot1x firewall <interface *interface-name*>

Release Information Command introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description Display information about the firewall filters for each user or nonresponsive host that is authenticated on each 802.1X-enabled interface that is configured for multiple supplicants. For example, if the firewall filter is configured with a term for counters, the command shows the count for each user.

Options **none**—Display information for all interfaces.

interface *interface-names*—(Optional) Display information for the specified interface.

Required Privilege Level view

Related Documentation
- clear dot1x on page 1659

List of Sample Output
show dot1x firewall on page 1809
show dot1x firewall on page 1809

Output Fields Output fields include any action modifier that is specified in firewall filters.

Sample Output

show dot1x firewall

(Showing counter action)

```
user@switch> show dot1x firewall
Filter: dot1x-filter-ge-0/0/3
Counters
 counter1_dot1x_ge-0/0/3_user1   342
 counter1_dot1x_ge-0/0/3_user2   857
```

show dot1x firewall

(Showing policer action)

```
user@switch> show dot1x firewall
Filter: dot1x_ge-0/0/0
Counters
```

```
p1-t1   494946
```

show dot1x static-mac-address

Syntax

```
show dot1x static-mac-address <(interface [interface-name])>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description

Display all the static MAC addresses that are configured to bypass 802.1X authentication on the switch.

Options

none—Display static MAC addresses for all interfaces.

interface ***interface-name***—(Optional) Display static MAC addresses for a specific interface.

Required Privilege Level

view

Related Documentation

- clear dot1x on page 1659
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 368
- *Adding a Static MAC Address Entry to the Ethernet Switching Table on a Switch with ELS Support*
- Configuring 802.1X Interface Settings (CLI Procedure) on page 292
- Understanding Authentication on Switches on page 268

List of Sample Output

show dot1x static-mac-address on page 1812
show dot1x static-mac-address interface (Specific Interface) on page 1812

Output Fields

Table 83 on page 1811 lists the output fields for the **show dot1x static-mac-address** command. Output fields are listed in the approximate order in which they appear.

Table 83: show dot1x static-mac-address Output Fields

Field Name	Field Description	Level of Output
MAC address	The MAC address of the device that is configured to bypass 802.1X authentication.	**all**
VLAN-Assignment	The name of the VLAN to which the device is assigned.	**all**
Interface	The name of the interface on which authentication is bypassed for a given MAC address.	**all**

Sample Output

show dot1x static-mac-address

```
user@switch> show dot1x static-mac-address

MAC address           VLAN-Assignment           Interface
00:00:00:11:22:33
00:00:00:00:12:12                               ge-0/0/3.0
00:00:00:02:34:56      facilities               ge-0/0/1.0
```

show dot1x static-mac-address interface (Specific Interface)

```
user@switch> show dot1x static-mac-address interface ge-0/0/0.1

MAC address           VLAN-Assignment           Interface
00:00:00:12:24:12     support                   ge-0/0/1.0
00:00:00:72:30:58     support                   ge-0/0/1.0
```

show dot1x statistics

Syntax

```
show dot1x statistics
<interface interface>
```

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.

Description Display the number of EAPOL messages transmitted or received on all interfaces or specific interfaces.

Options

none—Displays statistical information for all interfaces.

interface *interface-name*—(Optional) Displays statistical information for the specified interface.

Required Privilege Level view

Related Documentation

- show dot1x on page 1799
- clear dot1x on page 1659
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 337
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 297

List of Sample Output show dot1x statistics interface on page 1814

Output Fields Table 81 on page 1806 lists the output fields for the **show dot1x statistics** command. Output fields are listed in the approximate order in which they appear.

Table 84: show dot1x statistics Output Fields

Field Name	Field Description
TxReqId	The number of EAP-Request/Identity messages transmitted on the interface.
TxReq	The number of transmitted EAP-Request frames that were not EAP-Request/Identity.
TxTotal	The total number of EAPOL messages transmitted on the interface.
RxStart	The number of EAPOL-Start messages received on the interface.
RxLogoff	The number of EAP-Logoff messages received on the interface.
RxRespId	The number of EAP-Response/Identity frames received on the interface.

Table 84: show dot1x statistics Output Fields (continued)

Field Name	Field Description
RxResp	The number of EAP-Response messages received that were not EAP-Response/Identity.
CoA-Request	The number of Change of Authorization (CoA) Request messages received on the interface.
CoA-Ack	The number of CoA-Ack messages transmitted on the interface.
CoA-Nak	The number of CoA-Nak messages transmitted on the interface.
RxInvalid	The number of invalid EAPOL messages received on the interface.
RxLenErr	The number of EAPOL messages with incorrect length received on the interface.
RxTotal	The total number of EAPOL messages creceived on the interface.
LastRxVersion	The version number of the last EAPOL message received on the interface.
LastRxSrcMac	The source MAC address in the last EAPOL message received on the interface.
PortBounceReqRx	The number of port bounce requests received on the port.

Sample Output

show dot1x statistics interface

```
user@host> show dot1x statistics interface ge-0/0/0

Interface: ge-0/0/0.0
  TxReqId = 4 TxReq = 0 TxTotal = 4
  RxStart = 0 RxLogoff = 0 RxRespId = 0 RxResp = 0
  CoA-Request = 0 CoA-Ack = 0 CoA-Nak = 0
  RxInvalid = 0 RxLenErr = 0 RxTotal = 0
  LastRxVersion = 0 LastRxSrcMac = 00:50:56:85:66:0f
  PortBounceReqRx = 0
```

show ethernet-switching interfaces

Syntax

```
show ethernet-switching interfaces
<brief | detail | summary>
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
In Junos OS Release 9.6 for EX Series switches, the following updates were made:

- **Blocking** field output was updated.
- The default view was updated to include information about 802.1Q tags.
- The **detail** view was updated to include information on VLAN mapping.

Command introduced in Junos OS Release 11.1 for the QFX Series.
In Junos OS Release 11.1 for EX Series switches, the **detail** view was updated to include reflective relay information.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Display information about switched Ethernet interfaces.

Options

none—(Optional) Display brief information for Ethernet-switching interfaces.

brief | detail | summary—(Optional) Display the specified level of output.

interface *interface-name*—(Optional) Display Ethernet-switching information for a specific interface.

Required Privilege Level

view

Related Documentation

- *Troubleshooting Ethernet SwitchingUnderstanding Bridging and VLANs on Switches*
- *Example: Setting Up Basic Bridging and a VLAN on Switches*
- *Example: Setting Up Bridging with Multiple VLANs*
- *Understanding FCoE*
- *Interfaces Overview for Switches*
- *show ethernet-switching mac-learning-log*
- *show ethernet-switching table*
- *Configuring Autorecovery for Port Security Events*

List of Sample Output

show ethernet-switching interfaces on page 1818
show ethernet-switching interfaces summary on page 1819
show ethernet-switching interfaces brief on page 1819

show ethernet-switching interfaces detail on page 1819
show ethernet-switching interfaces interface-name on page 1820
show ethernet-switching interfaces on page 1820
show ethernet-switching interfaces ge-0/0/15 brief on page 1821
show ethernet-switching interfaces ge-0/0/2 detail (Blocked by RTG rtggroup) on page 1821
show ethernet-switching interfaces ge-0/0/15 detail (Blocked by STP) on page 1821
show ethernet-switching interfaces ge-0/0/17 detail (Disabled by bpdu-control) on page 1821
show ethernet-switching interfaces detail (C-VLAN to S-VLAN Mapping) on page 1821
show ethernet-switching interfaces detail (Reflective Relay Is Configured) on page 1821

Output Fields For QFX Series, QFabric, NFX Series, EX4600 and OCX1100:

Table 62 on page 1736 lists the output fields for the **show ethernet-switching interfaces** command on QFX Series, QFabric, NFX Series, EX4600 and OCX1100. Output fields are listed in the approximate order in which they appear.

Table 85: show ethernet-switching interfaces Output Fields

Field Name	Field Description	Level of Output
Interface	Name of a switching interface.	All levels
State	Interface state. Values are **up** or **down**.	none, **brief**, **detail**, **summary**
VLAN members	Name of a VLAN.	none, **brief**, **detail**, **summary**
Blocking	Forwarding state of the interface: • **blocked**—Traffic is not being forwarded on the interface. • **unblocked**—Traffic is forwarded on the interface. • **MAC limit exceeded**—The interface is temporarily disabled because of a MAC limiting error. The disabled interface is automatically restored to service when the disable timeout expires. • **MAC move limit exceeded**—The interface is temporarily disabled because of a MAC move limiting error. The disabled interface is automatically restored to service when the disable timeout expires. • **Storm control in effect** —The interface is temporarily disabled because of a storm control error. The disabled interface is automatically restored to service when the disable timeout expires. • **Storm control shutdown in effect** —The interface is temporarily disabled because of a storm control shutdown error. The disabled interface is automatically restored to service when the disable timeout expires.	none, **brief**, **detail**, **summary**
Index	VLAN index internal to Junos OS software.	**detail**
untagged | tagged	Specifies whether the interface forwards IEEE802.1Q-tagged or untagged traffic.	**detail**

Output fields for EX Series:

Table 63 on page 1737 lists the output fields for the **show ethernet-switching interfaces** command on EX Series switches. Output fields are listed in the approximate order in which they appear.

Table 86: show ethernet-switching interfaces Output Fields

Field Name	Field Description	Level of Output
Interface	Name of a switching interface.	none, **brief**, **detail**, **summary**
Index	VLAN index internal to Junos OS.	**detail**
State	Interface state. Values are **up** and **down**.	none, **brief**, **detail**
Port mode	The **access** mode is the port mode default and works with a single VLAN. Port mode can also be **trunk**, which accepts tagged packets from multiple VLANs on other switches. The third port mode value is **tagged-access**, which accepts tagged packets from access devices.	**detail**
Reflective Relay Status	Reflective relay allows packets to use the same interface for both upstream and downstream traffic. When reflective relay has been configured, the status displayed is always **enabled** . When reflective relay is not configured, this entry does not appear in the command output.	**detail**
Ether type for the interface	Ether type is a two-octet field in an Ethernet frame used to indicate which protocol is encapsulated in the payload of an incoming Ethernet packet. Both 802.1Q packets and Q-in-Q packets use this field. The output displayed for this particular field indicates the interface's Ether type, which is used to match the Ether type of incoming 802.1Q packets and Q-in-Q packets. The indicated Ether type field is also added to the interface's outgoing 802.1Q and Q-in-Q packets.	**detail**
VLAN membership	Names of VLANs that belong to this interface.	none, **brief**, **detail**,
Tag	Number of the 802.1Q tag.	none, **brief**, **detail**,
Tagging	Specifies whether the interface forwards 802.1Q **tagged** or **untagged** traffic.	none, **brief**, **detail**,

Table 86: show ethernet-switching interfaces Output Fields (continued)

Field Name	Field Description	Level of Output
Blocking	The forwarding state of the interface: • **unblocked**—Traffic is forwarded on the interface. • **blocked**—Traffic is not being forwarded on the interface. • **Disabled by bpdu control**—The interface is disabled due to receiving BPDUs on a protected interface. If the **disable-timeout** statement has been included in the BPDU configuration, the interface automatically returns to service after the timer expires. • **blocked by RTG**—The specified redundant trunk group is disabled. • **blocked by STP**—The interface is disabled due to a spanning-tree protocol error. • **MAC limit exceeded**—The interface is temporarily disabled due to a MAC limit error. The disabled interface is automatically restored to service when the disable timeout expires. • **MAC move limit exceeded**—The interface is temporarily disabled due to a MAC move limit error. The disabled interface is automatically restored to service when the disable timeout expires. • **Storm control in effect**—The interface is temporarily disabled due to a storm control error. The disabled interface is automatically restored to service when the disable timeout expires.	none, **brief**, **detail**,
Number of MACs learned on IFL	Number of MAC addresses learned by this interface.	**detail**
mapping	When mapping is configured, the status is one of the following C-VLAN to S-VLAN mapping types: • **dot1q-tunneled**—The interface maps all traffic to the S-VLAN (all-in-one bundling). • **native**—The interface maps untagged and priority tagged packets to the S-VLAN. • **push**—The interface maps packets to a firewall filter to an S-VLAN. • **policy-mapped**—The interface maps packets to a specifically defined S-VLAN. • *integer*—The interface maps packets to the specified S-VLAN. When mapping is not configured, this entry does not appear in the command output.	**detail**

Sample Output for QFX Series Switches, QFabric, NFX Series, EX4600 and OCX1100

show ethernet-switching interfaces

```
user@switch> show ethernet-switching interfaces

Interface   State    VLAN members          Blocking
xe-0/0/0.0  up       T1122                 unblocked
xe-0/0/1.0  down     default               – MAC limit exceeded
xe-0/0/2.0  down     default               – MAC move limit exceeded
xe-0/0/3.0  down     default               – Storm control in effect
xe-0/0/4.0  down     default               unblocked
```

```
xe-0/0/5.0  down     default               unblocked
xe-0/0/6.0  down     default               unblocked
xe-0/0/7.0  down     default               unblocked
xe-0/0/8.0  down     default               unblocked
xe-0/0/9.0  up       T111                  unblocked
xe-0/0/10.0 down     default               unblocked
xe-0/0/11.0 down     default               unblocked
xe-0/0/12.0 down     default               unblocked
xe-0/0/13.0 down     default               unblocked
xe-0/0/14.0 down     default               unblocked
xe-0/0/15.0 down     default               unblocked
xe-0/0/16.0 down     default               unblocked
xe-0/0/17.0 down     default               unblocked
xe-0/0/18.0 down     default               unblocked
xe-0/0/19.0 up       T111                  unblocked
xe-0/1/0.0  down     default               unblocked
xe-0/1/1.0  down     default               unblocked
xe-0/1/2.0  down     default               unblocked
xe-0/1/3.0  down     default               unblocked
```

show ethernet-switching interfaces summary

```
user@switch> show ethernet-switching interfaces summary
```

```
xe-0/0/0.0
xe-0/0/1.0
xe-0/0/2.0
xe-0/0/3.0
xe-0/0/8.0
xe-0/0/10.0
xe-0/0/11.0
```

show ethernet-switching interfaces brief

```
user@switch> show ethernet-switching interfaces brief
```

```
Interface   State    VLAN members          Blocking
xe-0/0/0.0  down     default               unblocked
xe-0/0/1.0  down     employee-vlan         unblocked
xe-0/0/2.0  down     employee-vlan         unblocked
xe-0/0/3.0  down     employee-vlan         unblocked
xe-0/0/8.0  down     employee-vlan         unblocked
xe-0/0/10.0 down     default               unblocked
xe-0/0/11.0 down     employee-vlan         unblocked
```

show ethernet-switching interfaces detail

```
user@switch> show ethernet-switching interfaces detail
```

```
Interface: xe-0/0/0.0 Index: 65
  State: down
  VLANs:
    default               untagged     unblocked

Interface: xe-0/0/1.0 Index: 66
  State: down
  VLANs:
    employee-vlan         untagged     unblocked
```

```
Interface: xe-0/0/2.0 Index: 67
  State: down
  VLANs:
    employee-vlan          untagged     unblocked

Interface: xe-0/0/3.0 Index: 68
  State: down
  VLANs:
    employee-vlan          untagged     unblocked

Interface: xe-0/0/8.0 Index: 69
  State: down
  VLANs:
    employee-vlan          untagged     unblocked

Interface: xe-0/0/10.0 Index: 70
  State: down
  VLANs:
    default                untagged     unblocked

Interface: xe-0/0/11.0 Index: 71
  State: down
  VLANs:
    employee-vlan          tagged       unblocked
```

show ethernet-switching interfaces interface-name

```
user@switch> show ethernet-switching interfaces xe-0/0/0.0
```

```
 Interface   State    VLAN members           Blocking
xe-0/0/0.0  down     default                unblocked
```

Sample Output for EX Series Switches

show ethernet-switching interfaces

```
user@switch> show ethernet-switching interfaces
```

```
Interface    State  VLAN members        Tag   Tagging  Blocking

ae0.0        up     default                   untagged unblocked
ge-0/0/2.0   up     vlan300           300     untagged blocked by RTG (rtggroup)
ge-0/0/3.0   up     default                            blocked by STP
ge-0/0/4.0   down   default                            MAC limit exceeded
ge-0/0/5.0   down   default                            MAC move limit exceeded
ge-0/0/6.0   down   default                            Storm control in effect
ge-0/0/7.0   down   default                            unblocked
ge-0/0/13.0  up     default                   untagged unblocked
ge-0/0/14.0  up     vlan100             100   tagged   unblocked
                    vlan200             200   tagged   unblocked
ge-0/0/15.0  up     vlan100             100   tagged   blocked by STP
                    vlan200             200   tagged   blocked by STP
ge-0/0/16.0  down   default                   untagged unblocked
ge-0/0/17.0  down   vlan100             100   tagged   Disabled by bpdu-control

                    vlan200             200   tagged   Disabled by bpdu-control
```

show ethernet-switching interfaces ge-0/0/15 brief

```
user@switch> show ethernet-switching interfaces ge-0/0/15 brief
Interface   State  VLAN members   Tag   Tagging        Blocking

ge-0/0/15.0  up     vlan100        100   tagged         blocked by STP
                    vlan200        200   tagged         blocked by STP
```

show ethernet-switching interfaces ge-0/0/2 detail (Blocked by RTG rtggroup)

```
user@switch> show ethernet-switching interfaces ge-0/0/2 detail

Interface: ge-0/0/2.0, Index: 65, State: up, Port mode: Access
Ether type for the interface: 0X8100
VLAN membership:
    vlan300, 802.1Q Tag: 300, untagged, msti-id: 0, blocked by RTG(rtggroup)
Number of MACs learned on IFL: 0
```

show ethernet-switching interfaces ge-0/0/15 detail (Blocked by STP)

```
user@switch> show ethernet-switching interfaces ge-0/0/15 detail

Interface: ge-0/0/15.0, Index: 70, State: up, Port mode: Trunk
Ether type for the interface: 0X8100
VLAN membership:
    vlan100, 802.1Q Tag: 100, tagged, msti-id: 0, blocked by STP
    vlan200, 802.1Q Tag: 200, tagged, msti-id: 0, blocked by STP

Number of MACs learned on IFL: 0
```

show ethernet-switching interfaces ge-0/0/17 detail (Disabled by bpdu-control)

```
user@switch> show ethernet-switching interfaces ge-0/0/17 detail

Interface: ge-0/0/17.0, Index: 71, State: down, Port mode: Trunk
Ether type for the interface: 0X8100
VLAN membership:
    vlan100, 802.1Q Tag: 100, tagged, msti-id: 1, Disabled by bpdu-control
    vlan200, 802.1Q Tag: 200, tagged, msti-id: 2, Disabled by bpdu-control
Number of MACs learned on IFL: 0
```

show ethernet-switching interfaces detail (C-VLAN to S-VLAN Mapping)

```
user@switch>show ethernet-switching interfaces ge-0/0/6.0 detail
Interface: ge-0/0/6.0, Index: 73, State: up, Port mode: Access
Ether type for the interface: 0X8100
VLAN membership:
    map, 802.1Q Tag: 134, Mapped Tag: native, push, dot1q-tunneled, unblocked
    map, 802.1Q Tag: 134, Mapped Tag: 20, push, dot1q-tunneled, unblocked
```

show ethernet-switching interfaces detail (Reflective Relay Is Configured)

```
user@switch1> show ethernet-switching interfaces ge-7/0/2 detail
```

```
Interface: ge-7/0/2, Index: 66, State: down, Port mode: Tagged-access
Ether type for the interface: 0X8100
Reflective Relay Status: Enabled
Ether type for the interface: 0x8100
VLAN membership:
    VLAN_Purple VLAN_Orange VLAN_Blue, 802.1Q Tag: 450, tagged, unblocked
Number of MACs learned on IFL: 0
```

show ethernet-switching interface

Syntax

```
show ethernet-switching interface
<brief | detail | extensive>
<interface-name>
```

Release Information

Command introduced in Junos OS Release 12.3R2.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Command introduced in Junos OS Release 13.2x51 for QFX Series switches.

Description

Display Layer 2 learning information for all the interfaces.

Options

none—Display Ethernet-switching information for all interfaces.

brief | detail | extensive—(Optional) Display the specified level of output.

interface-name—(Optional) Display Ethernet-switching information for the specified interface.

Required Privilege Level

view

Related Documentation

List of Sample Output

show ethernet switching interface (Specific Interface) on page 1824
show ethernet-switching interface detail on page 1825

Output Fields

Table 87 on page 1823 describes the output fields for the **show ethernet-switching interface** command. Output fields are listed in the approximate order in which they appear.

Table 87: show ethernet-switching interface Output Fields

Field Name	Field Description
Logical interface	Name of the logical interface.
VLAN members	VLANs associated with this interface.
Tag	VLAN ID.
MAC limit	Number of MAC addresses that can be associated with the interface.
STP state	Spanning Tree protocol (STP) state.

Table 87: show ethernet-switching interface Output Fields (continued)

Field Name	Field Description
Logical interface flags	Status of Layer 2 learning properties for each interface: • **DL**—MAC learning is disabled. • **LH**—MAC interface limit has been reached. • **AD**—Packets are dropped after the MAC interface limit is reached. • **DN**—The MAC interface is down. • **MMAS**—The MAC interface is disabled after a MAC address move. • **SCTL**—The MAC interface is disabled after a configured storm-control level is exceeded.
Tagging	Tagging state of the VLAN.

Sample Output

show ethernet switching interface (Specific Interface)

```
user@host> show ethernet-switching inerface ae10.0

Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down)

Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ae10.0                        8192                                  tagged
             VLAN70..   701   1024     Forwarding

             VLAN70..   702   1024     Forwarding

             VLAN70..   703   1024     Forwarding

             VLAN70..   704   1024     Forwarding

             VLAN70..   705   1024     Forwarding

             VLAN70..   706   1024     Forwarding

             VLAN70..   707   1024     Forwarding

             VLAN70..   708   1024     Forwarding

             VLAN70..   709   1024     Forwarding

             VLAN71..   710   1024     Forwarding

             VLAN71..   711   1024     Forwarding

             VLAN71..   712   1024     Forwarding

             VLAN71..   713   1024     Forwarding

             VLAN71..   714   1024     Forwarding

             VLAN71..   715
```

```
[...output truncated...]
```

show ethernet-switching interface detail

```
user@host> show ethernet-switching interface detail
Information for interface family:
Name: ge-1/0/3.0
  Type: IFF                              Handle: 0x8bba280
  Index: 331                             Generation: 159
                                         Flags: UP,
  IFD index: 141                         Routing/Vlan index: 4
  IFL index: 331                         Address family: 50
  Sequence number: 0                     MAC sequence number: 0
  MAC limit: 65535                       MACs learned: 0
  Static MACs learned: 0                 Non configured static MACs learned: 0
Name: ge-1/0/3.0
  Type: IFBD (static)                    Handle: 0x8bb6e00
  Index:                                 Generation: 129
  Trunk id: 0                            Flags: UP,
  IFD index:                             Routing/Vlan index: 2
  IFL index:                             Address family:
  Sequence number: 1                     MAC sequence number: 1
  MAC limit: 65535                       MACs learned: 0
  Static MACs learned: 0                 Non configured static MACs learned: 0
  VSTP index: 11                         Rewrite op:
Name: ge-1/0/3.0
  Type: IFBD (static)                    Handle: 0x8bb6f00
  Index:                                 Generation: 130
  Trunk id: 0                            Flags: UP,
  IFD index:                             Routing/Vlan index: 3
  IFL index:                             Address family:
  Sequence number: 1                     MAC sequence number: 1
  MAC limit: 65535                       MACs learned: 0
  Static MACs learned: 0                 Non configured static MACs learned: 0
  VSTP index: 11                         Rewrite op:
```

show lldp

Syntax

```
show lldp
<detail>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display information about Link Layer Discovery Protocol (LLDP) and Link Level Discovery Protocol–Media Endpoint Discovery (LLDP-MED) configuration and capabilities on the switch. LLDP and LLDP-MED are used to learn about and to distribute device information on network links.

NOTE: LLDP-MED is not available on the QFX Series.

Options

none—Display LLDP information for all interfaces.

detail—(Optional) Display detailed LLDP information for all interfaces.

Required Privilege Level

view

Related Documentation

- Configuring LLDP (CLI Procedure) on page 512
- Configuring LLDP-MED (CLI Procedure) on page 521
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518
- Understanding LLDP on page 511

List of Sample Output

show lldp (EX3200 switches) on page 1829
show lldp (EX4300 switches) on page 1830
show lldp detail (EX4300 switches) on page 1830
show lldp detail (EX3400 switches with VLAN name TLV) on page 1831

Output Fields

Table 88 on page 1827 lists the output fields for the **show lldp** command. Output fields are listed in the approximate order in which they appear.

Table 88: show lldp Output Fields

Field Name	Field Description	Level of Output
LLDP	LLDP operating state. The state can be **enabled** or **disabled**. NOTE: If a VLAN that has been configured for untagged packets on an interface also has Layer 2 protocol tunneling (L2PT) enabled for LLDP, the LLDP operating state for that interface is displayed as **disabled**.	All levels
Advertisement interval	Frequency, in seconds, at which LLDP advertisements are sent. This value is set by the advertisement-interval configuration statement.	All levels
Transmit delay	Seconds of delay before advertisements are sent to neighbors following a change to a TLV (type, length, or value) element in the LLDP protocol or to the state of the local system, such as a change in hostname or management address. You can set this value to reduce the delay in notifying neighbors of a change in the local system. This value is set by the transmit-delay configuration statement.	All levels
Hold timer	On EX4300 switches, the hold timer shows the length of time LLDP information is held before it is discarded. The hold timer value is equal to the advertisement interval multiplied by the hold multiplier. On all other switches, the hold timer shows the value of the hold multiplier. The hold multipler value is set by the hold-multiplier configuration statement.	All levels
Notification interval	How often LLDP trap notifications are generated as a result of LLDP database changes. If the interval value is 0, LLDP trap notifications on database changes are disabled. This value is set by the lldp-configuration-notification-interval configuration statement.	All levels
Config Trap Interval	How often LLDP trap notifications are generated as a result of changes in topology—for example, when an endpoint connects or disconnects. If the interval value is 0, LLDP trap notifications on topology changes are disabled. This value is set by the ptopo-configuration-trap-interval configuration statement.	All levels
Connection Hold timer	Amount of time the system maintains dynamic topology entries. This value is set by the ptopo-configuration-maximum-hold-time configuration statement.	All levels
LLDP-MED	LLDP-MED operating state. The state can be **Enabled** or **Disabled**.	All levels
MED fast start count	Number of advertisements sent from a switch to a device, such as a VoIP telephone, when the device is first detected by the switch. These increased advertisements are temporary. After a device and a switch exchange information and can communicate, advertisements are reduced to one per second. This value is set by using the fast-start configuration statement. NOTE: **fast-start**is not available on the QFX Series.	All levels

Table 88: show lldp Output Fields (continued)

Field Name	Field Description	Level of Output
Interface	Name of the interface for which LLDP configuration information is being reported.	All levels
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs.	All levels
LLDP	LLDP operating state. The state can be **Enabled** or **Disabled**.	All levels
Power Negotiation	LLDP power negotiation operating state. The state can be **Enabled** or **Disabled**.	All levels
Neighbor count	Total number of new LLDP neighbors detected since the last switch reboot.	**detail**
Interface	Name of the interface that is advertising VLAN information.	All levels
Vlan-id	VLAN tag associated with the interface sending LLDP frames. If the interface is not a member of a VLAN, the VLAN ID is advertised as 0.	**detail**
Vlan-name	VLAN name associated with the VLAN ID. For switches running Junos OS releases with Enhanced Layer 2 Software (ELS), this column displays the string **vlan-*vlan-id*** by default. Starting in Junos OS Release 15.1X53-D59 and 18.2R1, you can configure the **vlan-name-tlv-option name** option at the **[edit protocols lldp]** hierarchy level to transmit the VLAN name in the LLDP VLAN name TLV in place of the VLAN ID, and display the actual VLAN name in this output field instead.	**detail**
LLDP basic TLVs supported	Basic TLVs supported on the switch: • **Chassis identifier**—TLV that advertises the MAC address associated with the local system. • **Port identifier**—TLV that advertises the port identification for the specified port in the local system. • **Port description**—Interface name for the port. • **System name**—TLV that advertises the user-configured name of the local system. • **System description**—TLV that advertises the system description containing information about the software and current image running on the system. This information is taken from the software and is not configurable. • **System capabilities**—TLV that advertises the primary functions performed by the system—for example, bridge or router. • **Management address**—TLV that advertises the IP management address of the local system.	**detail**

Table 88: show lldp Output Fields (continued)

Field Name	Field Description	Level of Output
Supported LLDP 802 TLVs	802.3 TLVs supported on the switch: • **MAC/PHY configuration status**—TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information is based on the physical interface structure and is not configurable. • **Power via MDI**—TLV that advertises MDI power support, PSE power pair, and power class information. • **Link aggregation**—TLV that advertises if the interface is aggregated and its aggregated interface ID. • **Maximum frame size**—TLV that advertises the maximum transmission unit (MTU) of the interface sending LLDP frames. • **Port VLAN tag**—TLV that advertises the VLAN tag configured on the interface. • **Port VLAN name**—TLV that advertises the VLAN name configured on the interface.	**detail**
Supported LLDP MED TLVs	LLDP-MED TLVs supported on the switch: • **LLDP MED capabilities**—TLV that advertises the primary function of the port. The capabilities values range from 0 through 15: ◦ **0**—Capabilities ◦ **1**—Network Policy ◦ **2**—Location Identification ◦ **3**—Extended Power via MDI-PSE ◦ **4**—Inventory ◦ **5–15**—Reserved • **Network policy**—TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types—such as voice or streaming video—802.1Q VLAN tagging, and 802.1p priority bits and DiffServ code points. • **Endpoint location**—TLV that advertises the physical location of the endpoint. • **Extended power Via MDI**—TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.	**detail**

Sample Output

show lldp (EX3200 switches)

```
user@switch> show lldp

LLDP                      : Enabled
Advertisement interval    : 30 seconds
Transmit delay            : 2 seconds
Hold timer                : 4 seconds
Notification interval     : 0 Second(s)
Config Trap Interval      : 0 seconds
Connection Hold timer     : 300 seconds

LLDP MED                  : Disabled
```

```
MED fast start count   : 3 Packets


Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
all            -                   Enabled     Enabled      Enabled
```

show lldp (EX4300 switches)

```
user@switch> show lldp
```

```
LLDP                    : Enabled
Advertisement interval  : 30 seconds
Transmit delay          : 2 seconds
Hold timer              : 120 seconds
Notification interval   : 0 Second(s)
Config Trap Interval    : 0 seconds
Connection Hold timer   : 300 seconds

LLDP MED                : Disabled
MED fast start count    : 3 Packets


Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
all            -                   Enabled     Enabled      Enabled
```

show lldp detail (EX4300 switches)

```
user@switch> show lldp detail
```

```
LLDP                    : Enabled
Advertisement interval  : 30 seconds
Transmit delay          : 2 seconds
Hold timer              : 120 seconds
Notification interval   : 0 Second(s)
Config Trap Interval    : 0 seconds
Connection Hold timer   : 300 seconds

LLDP MED                : Disabled
MED fast start count    : 3 Packets


Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation     Neighbor count
all            -                   Enabled     Enabled      Enabled               8

Interface      Parent Interface    Vlan-id     Vlan-name
xe-3/0/0.0     ae31.0              100         vlan-100
xe-3/0/0.0     ae31.0              101         vlan-101
xe-3/0/0.0     ae31.0              4000        vlan-4000
xe-3/0/1.0     ae31.0              100         vlan-100
xe-3/0/1.0     ae31.0              101         vlan-101
xe-3/0/1.0     ae31.0              4000        vlan-4000
xe-3/0/2.0     ae31.0              100         vlan-100
xe-3/0/2.0     ae31.0              101         vlan-101
xe-3/0/2.0     ae31.0              4000        vlan-4000

LLDP basic TLVs supported:
Chassis identifier, Port identifier, Port description, System name, System
description, System capabilities, Management address.
```

```
Supported LLDP 802 TLVs:
MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum frame
size, Port VLAN tag, Port VLAN name.

Supported LLDP MED TLVs:
LLDP MED capabilities, Network policy, Endpoint location, Extended power
Via MDI.
```

show lldp detail (EX3400 switches with VLAN name TLV)

```
user@switch> show lldp detail
```

```
LLDP                      : Enabled
Advertisement interval    : 30 seconds
Transmit delay            : 2 seconds
Hold timer                : 120 seconds
Notification interval     : 5 Second(s)
Config Trap Interval      : 0 seconds
Connection Hold timer     : 300 seconds

LLDP MED                  : Enabled
MED fast start count      : 3 Packets

Port ID TLV subtype       : locally-assigned
Port Description TLV type : interface-alias (ifAlias)


Interface   Parent Interface    LLDP      LLDP-MED    Power Negotiation   Neighbor count
all         -                   -         Enabled     -                   5

Interface   Parent Interface    Vlan-id   Vlan-name
ge-0/0/0    -                   2         dc-vlan
ge-0/0/1    -                   2         dc-vlan
ge-0/0/2    -                   2         dc-vlan
ge-0/0/3    -                   2         dc-vlan
ge-0/0/4    -                   2         dc-vlan
ge-0/0/5    -                   2         dc-vlan
```

show lldp local-information

Syntax

```
show lldp local-information
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display the information that the switch provides in Link Layer Discovery Protocol (LLDP) advertisements to its neighbors.

Required Privilege Level

view

Related Documentation

- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518
- **management-address on page 1221**
- Understanding LLDP on page 511

List of Sample Output

show lldp local-information (EX Series Switch) on page 1833

Output Fields

Table 89 on page 1832 lists the output fields for the **show lldp local-information** command. Output fields are listed in the approximate order in which they appear.

Table 89: show lldp local-information Output Fields

Field Name	Field Description
LLDP Local Information details	Information about the local system (the switch): • **Chassis ID**—MAC address associated with the switch. • **System name**—User-configured name of the switch. • **System descr**—System description containing information about the switch model and the current software image running on the switch. This information is taken from the software and is not configurable.
System Capabilities	Capabilities (such as **bridge** or **router**) that are supported or enabled on the system.

Table 89: show lldp local-information Output Fields (continued)

Field Name	Field Description
Management Information	Details of the management information: **Port Name**, **Port Address** (such as **10.204.34.35**), **Address Type** (such as **ipv4** or **ipv6**), **Port ID** (SNMP interface index), **Port ID Subtype**, and **Port Subtype**. The **Port Subtype** displays: • **ifIndex(2)**— IP address of the switch's management Ethernet interface (**me0**) or virtual management Ethernet (**VME**) interface address (for a virtual chassis) is used to manage the switch. • **unknown(1)**—IP management address has been configured with set **protocols lldp management-address**.
Interface name	Name of the local interface which is configured for either LLDP or LLDP-MED.
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the local interface belongs.
SNMP Index	SNMP interface index.
Interface description	User-configured port description.
Status	Administrative status of the interface: either **up** or **down**.
Tunneling	Status of tunneling on the interface: either **enabled** or **disabled**.

Sample Output

show lldp local-information (EX Series Switch)

```
user@switch> show lldp local-information

LLDP Local Information details

Chassis ID   : 00:1d:b5:aa:b9:f0
System name  : switch
System descr : Juniper Networks, Inc. ex8208 , version 10.4I0 [builder] Build
               date: 2010-11-17 12:38:30 UTC

System Capabilities
    Supported       : Bridge Router
    Enabled         : Bridge Router

Management Information
    Port Name       : -
    Port Address    : 10.93.54.6
    Address Type    : IPv4
    Port ID         : 34
    Port ID Subtype : local(7)
    Port Subtype    : ifIndex(2)

Interface name Parent Interface  SNMP Index Interface description Status Tunneling
```

```
me0.0          -               34         -                   Down   Disabled
xe-3/0/0.0     ae31.0          769        xe-3/0/0.0          Up     Disabled
xe-3/0/1.0     ae31.0          770        xe-3/0/1.0          Up     Disabled
xe-3/0/2.0     ae31.0          771        xe-3/0/2.0          Up     Disabled
xe-3/0/3.0     ae31.0          772        xe-3/0/3.0          Up     Disabled
xe-3/0/4.0     ae31.0          577        xe-3/0/4.0          Up     Disabled
xe-3/0/5.0     ae31.0          578        xe-3/0/5.0          Up     Disabled
xe-3/0/6.0     ae31.0          579        xe-3/0/6.0          Up     Disabled
xe-3/0/7.0     ae31.0          581        xe-3/0/7.0          Up     Disabled
```

show lldp neighbors

Syntax

```
<show lldp neighbors>
<interface interface-ids>
```

Release Information Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description Display learned information about Link Layer Discovery Protocol (LLDP) on all neighboring interfaces or on selected interfaces.

Options

none—Display learned LLDP information on all neighboring interfaces and devices.

interface *interface-ids*—(Optional) Display learned LLDP information on the selected interfaces or devices.

NOTE: When a port with DCBX enabled begins to exchange type, length, and value (TLV) entries, optional LLDP TLVs on that port are not advertised to neighbors in order to interoperate with a wider variety of converged network adapters (CNAs). As a result, information for those ports will not be listed in the output for this command.

Required Privilege Level view

Related Documentation

- Understanding LLDP on page 511

List of Sample Output

show lldp neighbors on page 1838
show lldp neighbors interface on page 1838

Output Fields Table 90 on page 1835 lists the output fields for the **show lldp neighbors** command. Output fields are listed in the approximate order in which they appear.

Table 90: show lldp neighbors Output Fields

Field Name	Field Description
Local Interface	List of local interfaces for which neighbor information is available.
Parent Interface	List of aggregated Ethernet interfaces, if any, to which the local interfaces belong.
Chassis ID	List of chassis identifiers for neighbors.

Table 90: show lldp neighbors Output Fields (continued)

Field Name	Field Description
Port info	List of port information gathered from neighbors. This could be the port identifier or port description.
System name	List of system names gathered from neighbors.
LLDP Neighbor Information	Information about both the local system (the switch) and a neighbor system on the interface (appears when the **interface** option is used).
Local Information	Information about the local system (appears when the **interface** option is used).
Index	Local interface index (appears when the **interface** option is used).
Time to live	Number of seconds for which this information is valid (appears when the **interface** option is used).
Time mark	Date and timestamp of information (appears when the **interface** option is used).
Local Interface	Name of the local physical interface (appears when the **interface** option is used).
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the **interface** option is used).
Local Port ID	Local interface SNMP index (appears when the interface option is used).
Ageout Count	Number of times the complete set of information advertised by the neighbor has been deleted from LLDP neighbor information maintained by the local system because the information timeliness interval has expired (appears when the **interface** option is used).
Neighbor Information	Information about a neighbor system on the interface (appears when the **interface** option is used).
Chassis type	Type of chassis identifier supplied, such as **MAC address** (appears when the **interface** option is used).
Chassis ID	Chassis identifier of the chassis type listed (appears when the **interface** option is used).
Port type	Type of port identifier supplied, such as **locally assigned** (appears when the **interface** option is used).
Port ID	Port identifier of the port type listed (appears when the **interface** option is used).
Port description	Port description (appears when the **interface** option is used).

Table 90: show lldp neighbors Output Fields (continued)

Field Name	Field Description
System name	Name supplied by the system on the interface (appears when the **interface** option is used).
System Description	Description supplied by the system on the interface (appears when the **interface** option is used).
System capabilities	Capabilities (such as **Bridge**, **Router**, and **Telephone**) that are supported or enabled by the system on the interface (appears when the **interface** option is used).
Management Info	Details of management information: **Type** (such as **ipv4** or **ipv6**), **Address** (such as **10.204.34.35**), **Port ID**, **Subtype**, **Interface Subtype**, and organization identifier (**OID**) (appears when the **interface** option is used). The **Interface Subtype** displays: • **ifIndex(2)**— IP address of the neighbor's management Ethernet interface (**me0**) or virtual management Ethernet (**VME**) interface address (for a virtual chassis) is used to manage the switch. • **unknown(1)**—Neighbor's IP management address has been configured with set **protocols lldp management-address**.
Media Info	Additional details about the endpoint device appear when a device that supports LLDP-MED is attached to the interface. The specific details depend upon the capabilities of the device. Details might include **Media endpoint class** (such as Class 3 for communication devices such as IP phones), **MED Hardware revision**, **MED Firmware revision**, **MED Software revision**, **MED Serial number**, **MED Manufacturer name**, or **MED Model name**.
Organization Info	One or more entries listing remote information by organizationally unique identifier (**OUI**), **Subtype**, **Index**, and **Info** (appears when the **interface** option is used).
Age	How long the neighbor has been identified (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).
Local Interface	Name of the local physical interface (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).
Chassis ID	Chassis identifier of the chassis type listed (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).
Port description	Port description (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).
System name	NetBIOS name of the host (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).

Sample Output

show lldp neighbors

```
user@switch> show lldp neighbors

Local Interface   Parent Interface   Chassis Id          Port info    System Name
xe-3/0/4.0        ae31.0             b0:c6:9a:63:80:40   xe-0/0/0.0   newyork31
xe-3/0/5.0        ae31.0             b0:c6:9a:63:80:40   xe-0/0/1.0   newyork31
xe-3/0/6.0        ae31.0             b0:c6:9a:63:80:40   xe-0/0/2.0   newyork31
xe-3/0/7.0        ae31.0             b0:c6:9a:63:80:40   xe-0/0/3.0   newyork31
xe-3/0/0.0        ae31.0             b0:c6:9a:63:80:40   xe-0/1/0.0   newyork31
xe-3/0/1.0        ae31.0             b0:c6:9a:63:80:40   xe-0/1/1.0   newyork31
xe-3/0/2.0        ae31.0             b0:c6:9a:63:80:40   xe-0/1/2.0   newyork31
xe-3/0/3.0        ae31.0             b0:c6:9a:63:80:40   xe-0/1/3.0   newyork31
```

show lldp neighbors interface

```
user@switch> show lldp neighbors interface ge-0/0/2

LLLDP Neighbor Information:
Local Information:
Index: 1 Time to live: 240 Time mark: Wed Dec  1 10:23:24 2010 Age: 29 secs
Local Interface    : ge-0/0/2.0
Parent Interface   : -
Local Port ID      : 507
Ageout Count       : 0

Neighbour Information:
Chassis type       : Mac address
Chassis ID         : 00:1f:12:38:7f:c0
Port type          : Locally assigned
Port ID            : 507
Port description   : ge-0/0/2.0
System name        : bng-l48p5-dev


System Description : Juniper Networks, Inc. ex4200-48p , version 10.4I0 Build
date: 2010-11-30 09:32:17 UTC

System capabilities
        Supported  : Bridge Router
        Enabled    : Bridge Router

Management Info
        Type              : IPv4
        Address           : 10.204.96.235
        Port ID           : 34
        Subtype           : 1
        Interface Subtype : ifIndex(2)
        OID               : 1.3.6.1.2.1.31.1.1.1.1.34
Media endpoint class: Network Connectivity

Organization Info
       OUI      : 0.12.f
       Subtype  : 1
       Index    : 1
       Info     : 22A8360000
```

```
Organization Info
       OUI      : 0.12.f
       Subtype  : 2
       Index    : 2
       Info     : 030100
```

show lldp neighbors

Syntax

show lldp neighbors
<interface *interface*>

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display the information about neighboring devices learned by the switch by using the Link Layer Discovery Protocol (LLDP).

NOTE: The Chassis ID TLV has a subtype for Network Address Family. The supported network address families are IPv4 and IPv6. LLDP frames are validated only if the Network Address subtype of the Chassis ID TLV has a value of 1 (IPv4) or 2 (IPv6). For any other value, the transmitting device is detected by LLDP as a neighbor and displayed in the output of the **show lldp neighbors** command, but is not assigned to the VLAN.

Options

interface *interface*—(Optional) Display LLDP neighbor information for a selected interface.

Required Privilege Level

view

Related Documentation

- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

List of Sample Output

show lldp neighbors on page 1843
show lldp neighbors interface ge-0/0/8 on page 1843
show lldp neighbors interface ge-0/0/0.0 (for a VoIP AvayaTelephone with LLDP-MED Support) on page 1844
show lldp neighbors interface ge-0/0/5.0 (with NetBIOS Snooping Enabled on the Switch) on page 1845

Output Fields

Table 90 on page 1835 lists the output fields for the **show lldp neighbors** command. Output fields are listed in the approximate order in which they appear.

Table 91: show lldp neighbors Output Fields

Field Name	Field Description
Local Interface	List of local interfaces for which neighbor information is available.
Parent Interface	List of aggregated Ethernet interfaces, if any, to which the local interfaces belong.

Table 91: show lldp neighbors Output Fields (continued)

Field Name	Field Description
Chassis ID	List of chassis identifiers for neighbors.
Port info	This field displays the port information received from neighbors.
System name	List of system names gathered from neighbors. Includes the host name and the domain name.
LLDP Neighbor Information	Information about both the local system (the switch) and a neighbor system on the interface (appears when the **interface** option is used).
Local Information	Information about the local system (appears when the **interface** option is used).
Index	Local interface index (appears when the **interface** option is used).
Time to live	Number of seconds for which this information is valid (appears when the **interface** option is used).
Time mark	Date and timestamp of information (appears when the **interface** option is used).
Local Interface	Name of the local physical interface (appears when the **interface** option is used).
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the **interface** option is used).
Local Port ID	Local interface SNMP index (appears when the interface option is used).
Ageout Count	Number of times the complete set of information advertised by the neighbor has been deleted from LLDP neighbor information maintained by the local system because the information timeliness interval expired (appears when the interface option is used).
Neighbor Information	Information about a neighbor system on the interface (appears when the **interface** option is used).
Chassis type	Type of chassis identifier supplied, such as **Mac address** (appears when the **interface** option is used).
Chassis ID	Chassis identifier of the chassis type listed (appears when the **interface** option is used).
Port type	Type of port identifier supplied, such as **Locally assigned** (appears when the **interface** option is used).
Port ID	Port identifier of the port type listed (appears when the **interface** option is used).

Table 91: show lldp neighbors Output Fields (continued)

Field Name	Field Description
Port description	The port description field uses the configured port description, the port name or the SNMP ifIndex (appears when the **interface** option is used).
System name	Name supplied by the system on the interface (appears when the **interface** option is used).
System Description	Description supplied by the system on the interface (appears when the **interface** option is used).
System capabilities	Capabilities (such as **Bridge**, **Bridge Router**, and **Bridge Telephone**) that are supported or enabled by the system on the interface (appears when the **interface** option is used).
Management Info	Details of management information: **Type** (such as **IPv4** or **IPv6**), **Address** (such as **10.204.34.35**), **Port ID**, **Subtype**, **Interface Subtype**, and organization identifier (**OID**) (appears when the **interface** option is used). The **Interface Subtype** displays: • **ifIndex(2)**— IP address of the neighbor's management Ethernet interface (**me0**) or virtual management Ethernet (**VME**) interface address (for a Virtual Chassis) is used to manage the switch. • **unknown(1)**—Neighbor's IP management address has been configured with set **protocols lldp management-address**.
Media Info	Additional details about the endpoint device appear when a device that supports LLDP-MED is attached to the interface. The specific details depend upon the capabilities of the device. Details might include: **Media endpoint class** (such as Class 3 for communication devices such as IP phones), **MED Hardware revision**, **MED Firmware revision**, **MED Software revision**, **MED Serial number**, **MED Manufacturer name**, **MED Model name**.
Organization Info	One or more entries (indexed by the **Index** element) listing more remote interface information by organizationally unique identifier (**OUI**), **Subtype**, and **Info** (appears when the **interface** option is used).
Age	How long the neighbor has been identified (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).
Local Interface	Name of the local physical interface (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).
Chassis ID	Chassis identifier of the chassis type listed (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).

Sample Output

show lldp neighbors

```
user@switch> show lldp neighbors

Local Interface   Parent Interface   Chassis Id          Port info    System Name
xe-3/0/4.0        ae31.0            b0:c6:9a:63:80:40   xe-0/0/0.0   host.jnpr.net
xe-3/0/5.0        ae31.0            b0:c6:9a:63:80:40   xe-0/0/1.0   host.jnpr.net
xe-3/0/6.0        ae31.0            b0:c6:9a:63:80:40   xe-0/0/2.0   host.jnpr.net
xe-3/0/7.0        ae31.0            b0:c6:9a:63:80:40   xe-0/0/3.0   host.jnpr.net
xe-3/0/0.0        ae31.0            b0:c6:9a:63:80:40   xe-0/1/0.0   host.jnpr.net
xe-3/0/1.0        ae31.0            b0:c6:9a:63:80:40   xe-0/1/1.0   host.jnpr.net
xe-3/0/2.0        ae31.0            b0:c6:9a:63:80:40   xe-0/1/2.0   host.jnpr.net
xe-3/0/3.0        ae31.0            b0:c6:9a:63:80:40   xe-0/1/3.0   host.jnpr.net
```

show lldp neighbors interface ge-0/0/8

```
user@switch> show lldp neighbors interface ge-0/0/8

LLDP Neighbor Information:
Local Information:
Index: 1 Time to live: 120 Time mark: Thu Nov 26 06:41:24 2015 Age: 1 secs
Local Interface    : ge-0/0/8
Parent Interface   : -
Local Port ID      : 518
Ageout Count       : 0

Neighbour Information:
Chassis type       : Mac address
Chassis ID         : 88:e0:f3:1f:14:e0
Port type          : Locally assigned
Port ID            : 880
Port description   : ge-0/0/8
System name        : bng-nw6moj.juniper.net

System Description : Juniper Networks, Inc. ex4300-24p Ethernet Switch, kernel
JUNOS 14.1I20151125_0548_rajjs, Build date: 2015-11-25 06:06:58 UTC Copyright (c)
 1996-2015 Juniper Networks, Inc.

System capabilities
        Supported: Bridge Router
        Enabled  : Bridge Router

Management address
        Address Type      : IPv4(1)
        Address           : 10.204.39.232
        Interface Number  : 33
        Interface Subtype : ifIndex(2)
        OID               : 1.3.6.1.2.1.31.1.1.1.1.33.
Media endpoint class: Network Connectivity

Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
       Subtype  : MAC/PHY Configuration/Status (1)
       Info     : Autonegotiation [supported, enabled (0x3)], PMD Autonegotiation
 Capability (0x1), MAU Type (0x0)
       Index    : 1
```

```
Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
       Subtype  : MDI Power (2)
       Info     : MDI Power Support [PSE bit set, supported, disabled, CONTROL
bit not set (0x3)], MDI Power Pair [signal], MDI Power Class [Unknown (7)]
       Index    : 2

Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
       Subtype  : Link Aggregation (3)
       Info     : Aggregation Status [supported, disabled (0x1)], Aggregation
Port ID (0)
       Index    : 3

Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
       Subtype  : Maximum Frame Size (4)
       Info     : MTU Size (1514)
       Index    : 4

Organization Info
       OUI      : Juniper Specific (0x009069)
       Subtype  : Chassis Serial Type (1)
       Info     : Juniper Slot Serial [MS3112240009]
       Index    : 5
```

show lldp neighbors interface ge-0/0/0.0 (for a VoIP AvayaTelephone with LLDP-MED Support)

```
user@switch>show lldp neighbors interface ge-0/0/0.0
```

```
LLDP Neighbor Information:
Local Information:
Index: 20 Time to live: 120 Time mark: Thu Apr 15 22:26:22 2010 Age: 16 secs
Local Interface    : ge-0/0/0.0
Parent Interface   : -
Local Port ID      : 517
Ageout Count       : 0

Neighbour Information:
Chassis type       : Network address
Chassis ID         : 0.0.0.0
Port type          : Mac address
Port ID            : 00:04:0d:fc:55:48
System name        : AVAFC5548.juniper.net

System capabilities
        Supported  : Bridge Telephone
        Enabled    : Bridge

Management Info
        Type              : IPv4
        Address           : 0.0.0.0
        Port ID           : 1
        Subtype           : 1
        Interface Subtype : ifIndex(2)
        OID               : 1.3.6.1.2.1.31.1.1.1.1.1
Media endpoint class: Class III Device
```

```
MED Hardware revision : 4610D01A
MED Firmware revision : b10d01b2_9.bin
MED Software revision : a10d01b2_9.bin
MED Serial number     : 07N510103424
MED Manufacturer name : Avaya
MED Model name        : 4610

Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
       Subtype  : MAC/PHY Configuration/Status (1)
       Info     : Autonegotiation [supported, enabled (0x3)], PMD Autonegotiation
 Capability (0x1d00), MAU Type (0x0)
       Index    : 1

Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
       Subtype  : MDI Power (2)
       Info     : MDI Power Support [PSE bit set, supported, disabled, CONTROL
bit not set (0x3)], MDI Power Pair [signal], MDI Power Class [Unknown (7)]
       Index    : 2

Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
       Subtype  : Link Aggregation (3)
       Info     : Aggregation Status [supported, disabled (0x1)], Aggregation
Port ID (0)
       Index    : 3

Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
       Subtype  : Maximum Frame Size (4)
       Info     : MTU Size (1514)
       Index    : 4

Organization Info
       OUI      : Ethernet Bridged (0x0080c2)
       Subtype  : Port Vid (1)
       Info     : VLAN ID (10),
       Index    : 5

Organization Info
       OUI      : Juniper Specific (0x009069)
       Subtype  : Chassis Serial Type (1)
       Info     : Juniper Slot Serial [BQ0208211462]
       Index    : 6

Organization Info
       OUI      : Ethernet Bridged (0x0080c2)
       Subtype  : VLAN Name (3)
       Info     : VLAN ID (10), VLAN Name (vtest)
       Index    : 7
```

show lldp neighbors interface ge-0/0/5.0 (with NetBIOS Snooping Enabled on the Switch)

user@switch> **show lldp neighbors interface ge-0/0/5**

```
Age: 299999 secs
Local Interface    : ge-0/0/5.0
Parent Interface   : -
```

```
Chassis ID         : 00:10:94:00:00:02
Port description   : 192.0.2.1
System name        : host.juniper.net
```

show lldp statistics

Syntax

```
show lldp statistics
<interface interface-ids>
```

Release Information

Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Display LLDP statistics on all or selected interfaces.

Options

none—Display LLDP statistics on all interfaces and devices.

interface *interface-ids*—(Optional) Display LLDP statistics on the selected devices.

Required Privilege Level

view

Related Documentation

- Understanding LLDP on page 511

List of Sample Output

show lldp statistics on page 1848

Output Fields

Table 92 on page 1847 lists the output fields for the **show lldp statistics** command. Output fields are listed in the approximate order in which they appear.

Table 92: show lldp statistics Output Fields

Field Name	Field Description	Level of Output
Interface	Name of an interface.	All levels
Received	Total number of LLDP frames received on an interface.	All levels
Unknown-TLVs	Number of unrecognized LLDP TLVs received on an interface.	All levels
With Errors	Number of LLDP frames received that contain errors.	All levels
Discarded TLVs	Number of LLDP TLVs received and then discarded on an interface.	All levels
Transmitted	Total number of LLDP frames transmitted on an interface.	All levels
Untransmitted	Total number of LLDP frames not transmitted on an interface.	All levels

Sample Output

show lldp statistics

```
user@switch> show lldp statistics

Interface  Received  Unknown TLVs  With Errors  Discarded TLVs  Transmitted
Untransmitted
me0.0      0         0             0            0               8003         0

ge-0/0/0.0 8002      0             0            0               8003         0

ge-0/0/1.0 8002      0             0            0               8003         0
```

show lldp statistics

Syntax

show lldp statistics
<interface *interface*>

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display LLDP statistics for all interfaces or for the specified interface.

Options

none—Display LLDP statistics for all interfaces.

interface *interface*—(Optional) Display LLDP statistics for the specified interface.

Required Privilege Level

view

Related Documentation

- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

List of Sample Output

show lldp statistics on page 1850
show lldp statistics interface xe-3/0/0.0 on page 1850

Output Fields

Table 92 on page 1847 lists the output fields for the **show lldp statistics** command. Output fields are listed in the approximate order in which they appear.

Table 93: show lldp statistics Output Fields

Field Name	Field Description
Interface	Name of the interface.
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs. NOTE: Because LLDP packets are transmitted and received on member interfaces only, statistics are available only for the member interfaces, not for the aggregated interface.
Received	Total number of LLDP frames received on an interface.
Unknown TLVs	Number of unrecognized LLDP TLVs received on an interface.
With Errors	Number of invalid LLDP TLVs received on an interface.
Discarded	Number of LLDP TLVs received and then discarded on an interface.
Transmitted	Total number of LLDP frames that were transmitted on an interface.

Table 93: show lldp statistics Output Fields (continued)

Field Name	Field Description
Untransmitted	Total number of LLDP frames that were untransmitted on an interface.

Sample Output

show lldp statistics

```
user@switch> show lldp statistics

Interface    Parent Interface  Received  Unknown TLVs  With Errors
xe-3/0/0.0   ae31.0            1564      0             0
xe-3/0/1.0   ae31.0            1564      0             0
xe-3/0/2.0   ae31.0            1565      0             0
xe-3/0/3.0   ae31.0            1566      0             0
xe-3/0/4.0   ae31.0            1598      0             0
xe-3/0/5.0   ae31.0            1598      0             0
xe-3/0/6.0   ae31.0            1596      0             0
xe-3/0/7.0   ae31.0            1597      0             0
xe-5/0/6.0   -                 0         0             0
xe-5/0/7.0   -                 0         0             0

Discarded TLVs  Transmitted  Untransmitted
0               3044         1
0               3044         1
0               3044         1
0               3044         1
0               3075         1
0               3075         1
0               3075         1
0               3075         1
0               17312        0
0               17312        0
```

show lldp statistics interface xe-3/0/0.0

```
user@switch> show lldp statistics interface xe-3/0/0.0

Interface    Parent Interface  Received  Unknown TLVs  With Errors
xe-3/0/0.0   ae31.0            1566      0             0

Discarded TLVs  Transmitted  Untransmitted
0               3046         1
```

show lldp remote-global-statistics

Syntax show lldp remote-global-statistics

Release Information Command introduced in Junos OS Release 10.0 for EX Series switches.

Description Display remote Link Layer Discovery Protocol (LLDP) global statistics.

Options This command has no options.

Required Privilege Level view

Related Documentation

- Configuring LLDP (CLI Procedure) on page 512
- Understanding LLDP and LLDP-MED on EX Series Switches on page 518

List of Sample Output show lldp remote-global-statistics on page 1852

Output Fields Table 94 on page 1851 describes the output fields for the **show lldp remote-global-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 94: show lldp remote-global-statistics Output Fields

Field Name	Field Description
LLDP Remote Database Table Counters	Information about remote database table counters.
LastchangeTime	Time elapsed between LLDP agent startup and the last change to the remote database table information.
Inserts	Number of insertions made in the remote database table.
Deletes	Number of deletions made in the remote database table.
Drops	Number of LLDP frames dropped from the remote database table because of errors.
Ageouts	Number of remote database table entries that have aged out of the table.

Sample Output

show lldp remote-global-statistics

```
user@host> show lldp remote-global-statistics
```

```
user@host> show lldp remote-global-statistics
   LLDP Remote Database Table Counters
   LastchangeTime          Inserts    Deletes    Drops    Ageouts
   00:00:76 (76 sec)       192        0          0        0
```

show network-access aaa statistics accounting

Syntax show network-access aaa statistics accounting;

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for QFX Series switches.

Description Display authentication, authorization, and accounting (AAA) accounting statistics.

Required Privilege Level view

Related Documentation
- accounting-server on page 847
- accounting-stop-on-access-deny on page 848
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 335

List of Sample Output show network-access aaa statistics accounting on page 1853

Output Fields Table 95 on page 1853 lists the output fields for the **show network-access aaa statistics accounting** command. Output fields are listed in the approximate order in which they appear.

Table 95: show network-access aaa statistics accounting Output Fields

Field Name	Field Description
Requests received	The number of accounting-request packets sent from a switch to a RADIUS accounting server.
Accounting Response failures	The number of accounting-response failure packets sent from the RADIUS accounting server to the switch.
Accounting Response Success	The number of accounting-response success packets sent from the RADIUS accounting server to the switch.
Requests timedout	The number of requests-timedout packets sent from the RADIUS accounting server to the switch.

Sample Output

show network-access aaa statistics accounting

```
user@switch> show network-access aaa statistics accounting
```

```
Accounting module statistics
  Requests received: 1
  Accounting Response failures: 0
  Accounting Response Success: 1
  Requests timedout: 0
```

show network-access aaa statistics authentication

Syntax **show network-access aaa statistics authentication**

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for QFX Series switches.

Description Display authentication, authorization, and accounting (AAA) authentication statistics.

Required Privilege Level view

Related Documentation
- authentication-server on page 891
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302

List of Sample Output show network-access aaa statistics authentication on page 1855
show network-access aaa statistics authentication (in QFX Series Switches) on page 1856

Output Fields Table 96 on page 1855 lists the output fields for the **show network-access aaa statistics authentication** command. Output fields are listed in the approximate order in which they appear.

Table 96: show network-access aaa statistics authentication Output Fields

Field Name	Field Description
Requests received	The number of authentication requests received by the switch.
Accepts	The number of authentication accepts received by the RADIUS server.
Rejects	The number authentication rejects sent by the RADIUS server.
Challenges	The number of authentication challenges sent by the RADIUS server.

Sample Output

show network-access aaa statistics authentication

```
user@switch> show network-access aaa statistics authentication
Authentication module statistics
  Requests received: 2
  Accepts: 1
  Rejects: 0
  Challenges: 1
```

show network-access aaa statistics authentication (in QFX Series Switches)

```
user@switch> show network-access aaa statistics authentication
```

```
Authentication module statistics
  Requests received: 2
  Accepts: 1
  Rejects: 0
  Challenges: 1
```

show network-access aaa statistics dynamic-requests

Syntax **show network-access aaa statistics dynamic-requests;**

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for QFX Series switches.

Description Display authentication, authorization, and accounting (AAA) authentication statistics for disconnects.

Required Privilege Level view

Related Documentation
- authentication-server on page 891
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 302

List of Sample Output show network-access aaa statistics authentication on page 1857

Output Fields Table 97 on page 1857 lists the output fields for the **show network-access aaa statistics dynamic-requests** command. Output fields are listed in the approximate order in which they appear.

Table 97: show network-access aaa statistics dynamic-requests Output Fields

Field Name	Field Description
Requests received	The number of dynamic requests received by the RADIUS server.
Processed successfully	The number of dynamic requests successfully processed by the RADIUS server.
Errors during processing	The number of errors that occurred while the RADIUS server was processing the dynamic request.
Silently dropped	The number of silently dropped requests.

Sample Output

show network-access aaa statistics authentication

```
user@switch> show network-access aaa statistics dynamic-requests
Dynamic-requests module statistics
  Requests received: 0
  Processed successfully: 0
  Errors during processing: 0
  Silently dropped: 0
```

show network-access radsec local-certificate

Syntax

```
show network-access radsec local-certificate
<state>
<statistics [brief | detail | extensive]>
<certificate-name>
```

Release Information Command introduced in Junos OS Release 19.1R1.

Description Display the state and statistics of local certificate acquisition. RADSEC uses local certificates dynamically acquired from the public key infrastructure to establish a TLS connection.

If a certificate is not available, or if it was revoked, the RADSEC client will try to retrieve it every 300 seconds. Response timeout is 10 seconds, and failures are retried in 10 seconds.

Options

state—Display the state of acquisition for the local certificate.

statistics—Display acquisition statistics for the local certificate.

brief | detail | extensive—(Optional) Display the specified level of output.

certificate-name—(Optional) Display detailed information about the specified certificate.

Required Privilege Level view

Related Documentation

- RADIUS over TLS (RADSEC) on page 203

List of Sample Output

show network-access radsec local-certificate state on page 1860
show network-access radsec local-certificate statistics on page 1860
show network-access radsec local-certificate statistics detail on page 1860

Output Fields Table 98 on page 1859 lists the output fields for the **show network-access local-certificate** command. Output fields are listed in the approximate order in which they appear.

Table 98: show network-access radsec local-certificate Output Fields

Field Name	Field Description	Level of Output
Local certificate state	State of acquisition for the local certificate. • **active**—Local certificate is active. • **waiting**—Waiting to acquire local certificate.	all

Table 98: show network-access radsec local-certificate Output Fields (continued)

Field Name	Field Description	Level of Output
Local certificate general counters	Statistics for RADSEC local certificate acquisition.	all NOTE: Default output level will list only non-zero counters. Use **detail** or **extensive** to view all counters.

Sample Output

show network-access radsec local-certificate state

```
user@host> show network-access radsec local-certificate state
Local certificate state:
  cert-2                                        active
  cert-4                                        waiting
  qqq                                           waiting
```

Sample Output

show network-access radsec local-certificate statistics

```
user@host> show network-access radsec local-certificate statistics
Local certificate general counters:
  total-requests                                36
```

Sample Output

show network-access radsec local-certificate statistics detail

```
user@host> show network-access radsec local-certificate statistics detail
Local certificate general counters:
  total-requests                                36
  failed-requests                               0
  total-responses                               0
  configured-responses                           0
```

show network-access radsec statistics

Syntax

```
show network-access radsec statistics
<[brief | detail | extensive]>
<destination destination-id>
```

Release Information Command introduced in Junos OS Release 19.1R1.

Description Display the connection statistics for the RADSEC destinations.

Options

brief | detail | extensive—(Optional) Display the specified level of output. The default is **brief**, which will list only non-zero counters.

destination *destination–id*—(Optional) Display detailed information about the request specified by this RADSEC destination.

Required Privilege Level view

Related Documentation

- RADIUS over TLS (RADSEC) on page 203

List of Sample Output

show network-access radsec statistics on page 1861
show network-access radsec statistics detail on page 1862

Output Fields Table 99 on page 1861 lists the output fields for the **show network-access statistics** command. Output fields are listed in the approximate order in which they appear.

Table 99: show network-access radsec statistics Output Fields

Field Name	Field Description	Level of Output
Radsec general counters	Statistics for RADSEC syslog event counters.	all NOTE: Default output level will list only non-zero counters. Use **detail** or **extensive** to show all counters.
Destination	ID number of the RADSEC destination.	all

Sample Output

show network-access radsec statistics

```
user@host> show network-access radsec statistics
Radsec general counters:

  destination                                   895
```

```
  start-events                                1
  clear-events                                1
  timeout-events                              1
  loc-cert-acq-events                         1
  connected-events                            1
  ssl-ready-events                            1
```

Sample Output

show network-access radsec statistics detail

```
user@host> show network-access radsec statistics detail

Radsec general counters:

  destination                                 895
  start-events                                1
  clear-events                                1
  force-disconnect-events                     0
  timeout-events                              1
  loc-cert-acq-events                         1
  loc-cert-lost-events                        0
  connected-events                            1
  conn-failed-events                          0
  ssl-disconnected-events                     0
  ssl-ready-events                            1
  in-auth-reqs                                0
  in-acct-reqs                                0
  in-dyn-req-resps                            0
  tx-auth-reqs                                0
  tx-acct-reqs                                0
  tx-wd-reqs                                  9
  tx-late-auth-reqs                           0
  tx-late-acct-reqs                           0
  tx-dyn-req-resps                            0
  rx-auth-resps                               0
  rx-acct-resps                               0
  rx-dyn-reqs                                 0
  rx-dyn-req-naks                             0
  rx-dyn-req-drops                            0
  rx-wd-resps                                 9
  rx-resps                                    0
  rx-late-resps                               0
  rx-other-drops                              0
  resp-disconnect-drops                       0
  id-disconnect-drops                         0
  id-timeout-drops                            0
  tx-req-no-acct-supports                     0
  tx-req-dest-downs                           0
  tx-req-overflows                            0
  tx-req-disconnects                          0
  tx-req-bad-responses                        0
  tx-req-id-reuse-timeouts                    0
  tx-resp-dest-downs                          0
  tx-wd-reqs                                  9
  rx-wd-resps                                 9
```

show network-access radsec state

Syntax

show network-access radsec state
<destination *destination-id*>

Release Information

Command introduced in Junos OS Release 19.1R1.

Description

Display the connection state of RADSEC destinations.

Options

destination *destination–id*—(Optional) Display detailed information about the request specified by this RADSEC destination.

Required Privilege Level

view

Related Documentation

- RADIUS over TLS (RADSEC) on page 203

List of Sample Output

show network-access radsec state on page 1864

Output Fields

Table 100 on page 1863 lists the output fields for the **show network-access state** command. Output fields are listed in the approximate order in which they appear.

Table 100: show network-access radsec state Output Fields

Field Name	Field Description	Level of Output
Radsec state	State information for the RADSEC destination.	all
state	State of the RADSEC connection. • **connecting**—Establishing TCP connection. • **ssl-handshake**—SSL negotiation in progress. • **open**—RADSEC session is established for exchange of RADIUS messages. • **pause**—Pause for restart of connection process. The length of the pause is determined by the reason for restarting. • **local-cert-wait**—Connection initiated but waiting for local certificate to complete negotiation.	all
secs-in-state	Length of time in seconds of the current state.	all
remaining-secs	Length of time in seconds remaining for the current state.	all
pause-reason	The reason for restarting the connection, which triggers the pause state. The pause reason determines the length of the pause until reattempting the connection.	all

Table 100: show network-access radsec state Output Fields (continued)

Field Name	Field Description	Level of Output
acct-support	Shows whether the remote server supports accounting. • **Y**—Remote server supports accounting. This is the default value. • **N**—If the client receives a NAK response to an accounting request, all accounting requests will be dropped.	all
remote-failures	Number of consecutive failures on the remote side.	all
tx-requests	Number of RADIUS request messages transmitted.	all
tx-responses	Number of RADIUS response messages transmitted.	all

Sample Output

show network-access radsec state

```
user@host> show network-access radsec state

Radsec state:
    destination                                 895
    state                                       open
    secs-in-state                               66
    remaining-secs                              4294967295
    pause-reason                                none
    acct-support                                Y
    remote-failures                             0
    tx-requests                                 0
    tx-responses                                0
```

show route extensive

List of Syntax

Syntax on page 1865
Syntax (EX Series Switches) on page 1865

Syntax

```
show route extensive
<destination-prefix>
<logical-system (all | logical-system-name)>
```

Syntax (EX Series Switches)

```
show route extensive
<destination-prefix>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display extensive information about the active entries in the routing tables.

Options

none—Display all active entries in the routing table.

destination-prefix—(Optional) Display active entries for the specified address or range of addresses.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

view

List of Sample Output

show route extensive on page 1872
show route extensive (Access Route) on page 1879
show route extensive (BGP PIC Edge) on page 1880
show route extensive (FRR and LFA) on page 1880
show route extensive (IS-IS) on page 1881
show route extensive (Route Reflector) on page 1881
show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 1882
show route label detail (Multipoint LDP with Multicast-Only Fast Reroute) on page 1882
show route extensive (Flexible VXLAN Tunnel Profile) on page 1883

Output Fields

Table 101 on page 1865 describes the output fields for the **show route extensive** command. Output fields are listed in the approximate order in which they appear.

Table 101: show route extensive Output Fields

Field Name	Field Description
routing-table-name	Name of the routing table (for example, inet.0).

Table 101: show route extensive Output Fields (continued)

Field Name	Field Description
***number* destinations**	Number of destinations for which there are routes in the routing table.
***number* routes**	Number of routes in the routing table and total number of routes in the following states: • **active** (routes that are active). • **holddown** (routes that are in the pending state before being declared inactive). • **hidden** (routes that are not used because of a routing policy).

***route-destination* (entry, announced)**	Route destination (for example: 10.0.0.1/24). The **entry** value is the number of route for this destination, and the **announced** value is the number of routes being announced for this destination. Sometimes the route destination is presented in another format, such as:
	• ***MPLS-label*** (for example, 80001).
	• ***interface-name*** (for example, ge-1/0/2).
	• ***neighbor-address*:*control-word-status*:*encapsulation type*:*vc-id*:*source*** (Layer 2 circuit only; for example, 10.1.1.195:NoCtrlWord:1:1:Local/96).
	  ◦ ***neighbor-address***—Address of the neighbor.
	  ◦ ***control-word-status***—Whether the use of the control word has been negotiated for this virtual circuit: **NoCtrlWord** or **CtrlWord**.
	  ◦ ***encapsulation type***—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2) ATM AAL5 VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet, (6) HDLC, (7) PPP, (8) ATM VCC cell transport, (10) ATM VPC cell transport.
	  ◦ ***vc-id***—Virtual circuit identifier.
	  ◦ ***source***—Source of the advertisement: **Local** or **Remote**.

TSI	Protocol header information.
label stacking	(Next-to-the-last-hop routing device for MPLS only) Depth of the MPLS label stack, where the label-popping operation is needed to remove one or more labels from the top of the stack. A pair of routes is displayed, because the pop operation is performed only when the stack depth is two or more labels. • **S=0 route** indicates that a packet with an incoming label stack depth of two or more exits this router with one fewer label (the label-popping operation is performed). • If there is no **S=** information, the route is a normal MPLS route, which has a stack depth of 1 (the label-popping operation is not performed).
[*protocol*, *preference*]	Protocol from which the route was learned and the preference value for the route. • **+**—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table. • **-** —A hyphen indicates the last active route. • *****—An asterisk indicates that the route is both the active and the last active route. An asterisk before a **to** line indicates the best subpath to the route. In every routing metric except for the BGP **LocalPref** attribute, a lesser value is preferred. In order to use common comparison routines, Junos OS stores the 1's complement of the **LocalPref** value in the **Preference2** field. For example, if the **LocalPref** value for Route 1 is 100, the **Preference2** value is -101. If the **LocalPref** value for Route 2 is 155, the **Preference2** value is -156. Route 2 is preferred because it has a higher **LocalPref** value and a lower **Preference2** value.

Table 101: show route extensive Output Fields (continued)

Field Name	Field Description
Level	(IS-IS only). In IS-IS, a single autonomous system (AS) can be divided into smaller groups called areas. Routing between areas is organized hierarchically, allowing a domain to be administratively divided into smaller areas. This organization is accomplished by configuring Level 1 and Level 2 intermediate systems. Level 1 systems route within an area. When the destination is outside an area, they route toward a Level 2 system. Level 2 intermediate systems route between areas and toward other ASs.
Route Distinguisher	IP subnet augmented with a 64-bit prefix.
PMSI	Provider multicast service interface (MVPN routing table).
Next-hop type	Type of next hop. For a description of possible values for this field, see the Output Field table in the *show route detail* command.
Next-hop reference count	Number of references made to the next hop.
Flood nexthop branches exceed maximum message	Indicates that the number of flood next-hop branches exceeded the system limit of 32 branches, and only a subset of the flood next-hop branches were installed in the kernel.
Source	IP address of the route source.
Next hop	Network layer address of the directly reachable neighboring system.
via	Interface used to reach the next hop. If there is more than one interface available to the next hop, the name of the interface that is actually used is followed by the word **Selected**. This field can also contain the following information: • Weight—Value used to distinguish primary, secondary, and fast reroute backup routes. Weight information is available when MPLS label-switched path (LSP) link protection, node-link protection, or fast reroute is enabled, or when the standby state is enabled for secondary paths. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible. • Balance—Balance coefficient indicating how traffic of unequal cost is distributed among next hops when a routing device is performing unequal-cost load balancing. This information is available when you enable BGP multipath load balancing.
Label-switched-path *lsp-path-name*	Name of the LSP used to reach the next hop.
Label operation	MPLS label and operation occurring at this routing device. The operation can be **pop** (where a label is removed from the top of the stack), **push** (where another label is added to the label stack), or **swap** (where a label is replaced by another label).
Offset	Whether the metric has been increased or decreased by an offset value.
Interface	(Local only) Local interface name.
Protocol next hop	Network layer address of the remote routing device that advertised the prefix. This address is used to recursively derive a forwarding next hop.

Table 101: show route extensive Output Fields (continued)

Field Name	Field Description
label-operation	MPLS label and operation occurring at this routing device. The operation can be **pop** (where a label is removed from the top of the stack), **push** (where another label is added to the label stack), or **swap** (where a label is replaced by another label).
Indirect next hops	When present, a list of nodes that are used to resolve the path to the next-hop destination, in the order that they are resolved. When BGP PIC Edge is enabled, the output lines that contain **Indirect next hop: weight** follow next hops that the software can use to repair paths where a link failure occurs. The next-hop weight has one of the following values: • 0x1 indicates active next hops. • 0x4000 indicates passive next hops.
State	State of the route (a route can be in more than one state). See the Output Field table in the *show route detail* command.
Session ID	The BFD session ID number that represents the protection using MPLS fast reroute (FRR) and loop-free alternate (LFA).
Weight	Weight for the backup path. If the weight of an indirect next hop is larger than zero, the weight value is shown. For sample output, see **show route table**.

Table 101: show route extensive Output Fields (continued)

Field Name	Field Description
Inactive reason	If the route is inactive, the reason for its current state is indicated. Typical reasons include: • **Active preferred**—Currently active route was selected over this route. • **Always compare MED**—Path with a lower multiple exit discriminator (MED) is available. • **AS path**—Shorter AS path is available. • **Cisco Non-deterministic MED selection**—Cisco nondeterministic MED is enabled and a path with a lower MED is available. • **Cluster list length**—Path with a shorter cluster list length is available. • **Forwarding use only**—Path is only available for forwarding purposes. • **IGP metric**—Path through the next hop with a lower IGP metric is available. • **IGP metric type**—Path with a lower OSPF link-state advertisement type is available. • **Interior > Exterior > Exterior via Interior**—Direct, static, IGP, or EBGP path is available. • **Local preference**—Path with a higher local preference value is available. • **Next hop address**—Path with a lower metric next hop is available. • **No difference**—Path from a neighbor with a lower IP address is available. • **Not Best in its group**—Occurs when multiple peers of the same external AS advertise the same prefix and are grouped together in the selection process. When this reason is displayed, an additional reason is provided (typically one of the other reasons listed). • **Number of gateways**—Path with a higher number of next hops is available. • **Origin**—Path with a lower origin code is available. • **OSPF version**—Path does not support the indicated OSPF version. • **RIB preference**—Route from a higher-numbered routing table is available. • **Route destinguisher**—64-bit prefix added to IP subnets to make them unique. • **Route metric or MED comparison**—Route with a lower metric or MED is available. • **Route preference**—Route with a lower preference value is available. • **Router ID**—Path through a neighbor with a lower ID is available. • **Unusable path**—Path is not usable because of one of the following conditions: the route is damped, the route is rejected by an import policy, or the route is unresolved. • **Update source**—Last tiebreaker is the lowest IP address value.
Local AS	Autonomous system (AS) number of the local routing device.
Age	How long the route has been known.
AIGP	Accumulated interior gateway protocol (AIGP) BGP attribute.
Metric	Cost value of the indicated route. For routes within an AS, the cost is determined by IGP and the individual protocol metrics. For external routes, destinations, or routing domains, the cost is determined by a preference value.
MED-plus-IGP	Metric value for BGP path selection to which the IGP cost to the next-hop destination has been added.
TTL-Action	For MPLS LSPs, state of the TTL propagation attribute. Can be enabled or disabled for all RSVP-signaled and LDP-signaled LSPs or for specific VRF routing instances. For sample output, see **show route table**.

Table 101: show route extensive Output Fields (continued)

Field Name	Field Description
Task	Name of the protocol that has added the route.
Announcement bits	List of protocols that are consumers of the route. Using the following output as an example, **Announcement bits (3): 0-KRT 5-Resolve tree 2 8-BGP RT Background** there are (3) announcement bits to reflect the three clients (protocols) that have state for this route: Kernel (0-KRT), 5 (resolution tree process 2), and 8 (BGP). The notation ***n*-Resolve inet** indicates that the route is used for route resolution for next hops found in the routing table. ***n*** is an index used by Juniper Networks customer support only.
AS path	AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated: • **I**—IGP. • **E**—EGP. • **Recorded**—The AS path is recorded by the sample process (sampled). • **?**—Incomplete; typically, the AS path was aggregated. When AS path numbers are included in the route, the format is as follows: • **[ ]**—Brackets enclose the local AS number associated with the AS path if more than one AS number is configured on the routing device, or if AS path prepending is configured. • **{ }**—Braces enclose AS sets, which are groups of AS numbers in which the order does not matter. A set commonly results from route aggregation. The numbers in each AS set are displayed in ascending order. • **( )**—Parentheses enclose a confederation. • **([ ])**—Parentheses and brackets enclose a confederation set. NOTE: In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance.
validation-state	(BGP-learned routes) Validation status of the route: • **Invalid**—Indicates that the prefix is found, but either the corresponding AS received from the EBGP peer is not the AS that appears in the database, or the prefix length in the BGP update message is longer than the maximum length permitted in the database. • **Unknown**—Indicates that the prefix is not among the prefixes or prefix ranges in the database. • **Unverified**—Indicates that origin validation is not enabled for the BGP peers. • **Valid**—Indicates that the prefix and autonomous system pair are found in the database.
FECs bound to route	Point-to-multipoint root address, multicast source address, and multicast group address when multipoint LDP (M-LDP) inband signaling is configured.
AS path: I <Originator>	(For route reflected output only) Originator ID attribute set by the route reflector.

Table 101: show route extensive Output Fields (continued)

Field Name	Field Description
route status	Indicates the status of a BGP route: • **Accepted**—The specified BGP route is imported by the default BGP policy. • **Import**—The route is imported into a Layer 3 VPN routing instance. • **Import-Protect**—A remote instance egress that is protected. • **Multipath**—A BGP multipath active route. • **MultipathContrib**—The route is not active but contributes to the BGP multipath. • **Protect**—An egress route that is protected. • **Stale**—A route that is marked stale due to graceful restart.
Primary Upstream	When multipoint LDP with multicast-only fast reroute (MoFRR) is configured, the primary upstream path. MoFRR transmits a multicast join message from a receiver toward a source on a primary path, while also transmitting a secondary multicast join message from the receiver toward the source on a backup path.
RPF Nexthops	When multipoint LDP with MoFRR is configured, the reverse-path forwarding (RPF) next-hop information. Data packets are received from both the primary path and the secondary paths. The redundant packets are discarded at topology merge points due to the RPF checks.
Label	Multiple MPLS labels are used to control MoFRR stream selection. Each label represents a separate route, but each references the same interface list check. Only the primary label is forwarded while all others are dropped. Multiple interfaces can receive packets using the same label.
weight	Value used to distinguish MoFRR primary and backup routes. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible.
VC Label	MPLS label assigned to the Layer 2 circuit virtual connection.
MTU	Maximum transmission unit (MTU) of the Layer 2 circuit.
VLAN ID	VLAN identifier of the Layer 2 circuit.
Cluster list	(For route reflected output only) Cluster ID sent by the route reflector.
Originator ID	(For route reflected output only) Address of router that originally sent the route to the route reflector.
Prefixes bound to route	Forwarding Equivalent Class (FEC) bound to this route. Applicable only to routes installed by LDP.
Communities	Community path attribute for the route. See the Output Field table in the *show route detail* command for all possible values for this field.
Layer2-info: encaps	Layer 2 encapsulation (for example, VPLS).
control flags	Control flags: **none** or Site Down.
mtu	Maximum transmission unit (MTU) information.
Label-Base, range	First label in a block of labels and label block size. A remote PE routing device uses this first label when sending traffic toward the advertising PE routing device.

Table 101: show route extensive Output Fields (continued)

Field Name	Field Description
status vector	Layer 2 VPN and VPLS network layer reachability information (NLRI).
Localpref	Local preference value included in the route.
Router ID	BGP router ID as advertised by the neighbor in the open message.
Primary Routing Table	In a routing table group, the name of the primary routing table in which the route resides.
Secondary Tables	In a routing table group, the name of one or more secondary tables in which the route resides.
Originating RIB	Name of the routing table whose active route was used to determine the forwarding next-hop entry in the resolution database. For example, in the case of inet.0 resolving through inet.0 and inet.3, this field indicates which routing table, inet.0 or inet.3, provided the best path for a particular prefix.
Node path count	Number of nodes in the path.
Forwarding nexthops	Number of forwarding next hops. The forwarding next hop is the network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.

Sample Output

show route extensive

```
user@host> show route extensive

inet.0: 22 destinations, 23 routes (21 active, 0 holddown, 1 hidden)
203.0.113.10/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 203.0.113.10/16 -> {192.168.71.254}
        *Static Preference: 5
                Next-hop reference count: 29
                Next hop: 192.168.71.254 via fxp0.0, selected
                State: <Active NoReadvrt Int Ext>
                Local AS:    64496
                Age: 1:34:06
                Task: RT
                Announcement bits (2): 0-KRT 3-Resolve tree 2
                AS path: I

203.0.113.30/30 (2 entries, 1 announced)
        *Direct Preference: 0
                Next hop type: Interface
                Next-hop reference count: 2
                Next hop: via so-0/3/0.0, selected
                State: <Active Int>
                Local AS:    64496
                Age: 1:32:40
                Task: IF
                Announcement bits (1): 3-Resolve tree 2
                AS path: I
         OSPF   Preference: 10
                Next-hop reference count: 1
```

```
                Next hop: via so-0/3/0.0, selected
                State: <Int>
                Inactive reason: Route Preference
                Local AS:    64496
                Age: 1:32:40    Metric: 1
                Area: 0.0.0.0
                Task: OSPF
                AS path: I

203.0.113.103/32 (1 entry, 1 announced)
        *Local  Preference: 0
                Next hop type: Local
                Next-hop reference count: 7
                Interface: so-0/3/0.0
                State: <Active NoReadvrt Int>
                Local AS:    644969
                Age: 1:32:43
                Task: IF
                Announcement bits (1): 3-Resolve tree 2
                AS path: I

...

203.0.113.203/30 (1 entry, 1 announced)
TSI:
KRT in-kernel 203.0.113.203/30 -> {203.0.113.216}
        *OSPF   Preference: 10
                Next-hop reference count: 9
                Next hop: via so-0/3/0.0
                Next hop: 203.0.113.216 via ge-3/1/0.0, selected
                State: <Active Int>
                Local AS:    64496
                Age: 1:32:19    Metric: 2
                Area: 0.0.0.0
                Task: OSPF
                Announcement bits (2): 0-KRT 3-Resolve tree 2
                AS path: I

...

198.51.100.2/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 198.51.100.2/32 -> {}
        *PIM    Preference: 0
                Next-hop reference count: 18
                State: <Active NoReadvrt Int>
                Local AS:    64496
                Age: 1:34:08
                Task: PIM Recv
                Announcement bits (2): 0-KRT 3-Resolve tree 2
                AS path: I

...

198.51.100.22/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 198.51.100.22/32 -> {}
        *IGMP   Preference: 0
                Next-hop reference count: 18
                State: <Active NoReadvrt Int>
```

```
                Local AS:    64496
                Age: 1:34:06
                Task: IGMP
                Announcement bits (2): 0-KRT 3-Resolve tree 2
                AS path: I

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

203.0.113.103/32 (1 entry, 1 announced)
        State: <FlashAll>
        *RSVP   Preference: 7
                Next-hop reference count: 6
                Next hop: 203.0.113.216 via ge-3/1/0.0 weight 0x1, selected
                Label-switched-path green-r1-r3
                Label operation: Push 100096
                State: <Active Int>
                Local AS:    64496
                Age: 1:28:12    Metric: 2
                Task: RSVP
                Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
                AS path: I

203.0.113.238/32 (1 entry, 1 announced)
        State: <FlashAll>
        *RSVP   Preference: 7
                Next-hop reference count: 6
                Next hop: via so-0/3/0.0 weight 0x1, selected
                Label-switched-path green-r1-r2
                State: <Active Int>
                Local AS:    64496
                Age: 1:28:12    Metric: 1
                Task: RSVP
                Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
                AS path: I

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)

...

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

47.0005.80ff.f800.0000.0108.0001.0102.5507.1052/152 (1 entry, 0 announced)
        *Direct Preference: 0
                Next hop type: Interface
                Next-hop reference count: 1
                Next hop: via lo0.0, selected
                State: <Active Int>
                Local AS:    64496
                Age: 1:34:07
                Task: IF
                AS path: I

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

0   (1 entry, 1 announced)
TSI:
KRT in-kernel 0      /36 -> {}
        *MPLS   Preference: 0
                Next hop type: Receive
                Next-hop reference count: 6
```

```
                State: <Active Int>
                Local AS:    64496
                Age: 1:34:08    Metric: 1
                Task: MPLS
                Announcement bits (1): 0-KRT
                AS path: I

...

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
  299840 (1 entry, 1 announced)
  TSI:
  KRT in-kernel 299840 /52 -> {indirect(1048575)}
          *RSVP   Preference: 7/2
                  Next hop type: Flood
                  Address: 0x9174a30
                  Next-hop reference count: 4
                  Next hop type: Router, Next hop index: 798
                  Address: 0x9174c28
                  Next-hop reference count: 2
                  Next hop: 198.51.100.2 via lt-1/2/0.9 weight 0x1
                  Label-switched-path R2-to-R4-2p2mp
                  Label operation: Pop
                  Next hop type: Router, Next hop index: 1048574
                  Address: 0x92544f0
                  Next-hop reference count: 2
                  Next hop: 198.51.100.2 via lt-1/2/0.7 weight 0x1
                  Label-switched-path R2-to-R200-p2mp
                  Label operation: Pop
                  Next hop: 198.51.100.2 via lt-1/2/0.5 weight 0x8001
                  Label operation: Pop
                  State: <Active Int>
                  Age: 1:29       Metric: 1
                  Task: RSVP
                  Announcement bits (1): 0-KRT
                  AS path: I...

800010 (1 entry, 1 announced)

TSI:
KRT in-kernel 800010 /36 -> {vt-3/2/0.32769}
        *VPLS   Preference: 7
                Next-hop reference count: 2
                Next hop: via vt-3/2/0.32769, selected
                Label operation: Pop
                State: <Active Int>
                Age: 1:31:53
                Task: Common L2 VC
                Announcement bits (1): 0-KRT
                AS path: I

vt-3/2/0.32769 (1 entry, 1 announced)
TSI:
KRT in-kernel vt-3/2/0.32769.0      /16 -> {indirect(1048574)}
        *VPLS   Preference: 7
                Next-hop reference count: 2
                Next hop: 203.0.113.216 via ge-3/1/0.0 weight 0x1, selected
                Label-switched-path green-r1-r3
                Label operation: Push 800012, Push 100096(top)
                Protocol next hop: 203.0.113.103
```

```
                Push 800012
                Indirect next hop: 87272e4 1048574
                State: <Active Int>
                Age: 1:31:53    Metric2: 2
                Task: Common L2 VC
                Announcement bits (2): 0-KRT 1-Common L2 VC
                AS path: I
                Communities: target:11111:1 Layer2-info: encaps:VPLS,
                control flags:, mtu: 0
                Indirect next hops: 1
                        Protocol next hop: 203.0.113.103 Metric: 2
                        Push 800012
                        Indirect next hop: 87272e4 1048574
                        Indirect path forwarding next hops: 1
                               Next hop: 203.0.113.216 via ge-3/1/0.0 weight 0x1

                        203.0.113.103/32 Originating RIB: inet.3
                          Metric: 2                       Node path count: 1
                          Forwarding nexthops: 1
                                Nexthop: 203.0.113.216 via ge-3/1/0.0

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

2001:db8::10:255:71:52/128 (1 entry, 0 announced)
        *Direct Preference: 0
                Next hop type: Interface
                Next-hop reference count: 1
                Next hop: via lo0.0, selected
                State: <Active Int>
                Local AS:    64496
                Age: 1:34:07
                Task: IF
                AS path: I

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
        *Direct Preference: 0
                Next hop type: Interface
                Next-hop reference count: 1
                Next hop: via lo0.0, selected
                State: <Active NoReadvrt Int>
                Local AS:    64496
                Age: 1:34:07
                Task: IF
                AS path: I

ff02::2/128 (1 entry, 1 announced)
TSI:
KRT in-kernel ff02::2/128 -> {}
        *PIM    Preference: 0
                Next-hop reference count: 18
                State: <Active NoReadvrt Int>
                Local AS:    64496
                Age: 1:34:08
                Task: PIM Recv6
                Announcement bits (1): 0-KRT
                AS path: I

ff02::d/128 (1 entry, 1 announced)
TSI:
KRT in-kernel ff02::d/128 -> {}
```

```
        *PIM    Preference: 0
                Next-hop reference count: 18
                State: <Active NoReadvrt Int>
                Local AS:    64496
                Age: 1:34:08
                Task: PIM Recv6
                Announcement bits (1): 0-KRT
                AS path: I

ff02::16/128 (1 entry, 1 announced)
TSI:
KRT in-kernel ff02::16/128 -> {}
        *MLD    Preference: 0
                Next-hop reference count: 18
                State: <Active NoReadvrt Int>
                Local AS:    64496
                Age: 1:34:06
                Task: MLD
                Announcement bits (1): 0-KRT
                AS path: I

private.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
        *Direct Preference: 0
                Next hop type: Interface
                Next-hop reference count: 1
                Next hop: via lo0.16385, selected
                State: <Active NoReadvrt Int>
                Age: 1:34:07
                Task: IF
                AS path: I

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)

203.0.113.103:1:3:1/96 (1 entry, 1 announced)
        *BGP    Preference: 170/-101
                Route Distinguisher: 203.0.113.103:1
                Next-hop reference count: 7
                Source: 203.0.113.103
                Protocol next hop: 203.0.113.103
                Indirect next hop: 2 no-forward
                State: <Secondary Active Int Ext>
                Local AS:    64496 Peer AS:    64496
                Age: 1:28:12    Metric2: 1
                Task: BGP_69.203.0.113.103+179
                Announcement bits (1): 0-green-l2vpn
                AS path: I
                Communities: target:11111:1 Layer2-info: encaps:VPLS,
                control flags:, mtu: 0
                Label-base: 800008, range: 8
                Localpref: 100
                Router ID: 203.0.113.103
                Primary Routing Table bgp.l2vpn.0

203.0.113.152:1:1:1/96 (1 entry, 1 announced)
TSI:
Page 0 idx 0 Type 1 val 8699540
        *L2VPN  Preference: 170/-1
                Next-hop reference count: 5
```

```
                Protocol next hop: 203.0.113.152
                Indirect next hop: 0 -
                State: <Active Int Ext>
                Age: 1:34:03    Metric2: 1
                Task: green-l2vpn
                Announcement bits (1): 1-BGP.0.0.0.0+179
                AS path: I
                Communities: Layer2-info: encaps:VPLS, control flags:Site-Down,
                mtu: 0
                Label-base: 800016, range: 8, status-vector: 0x9F

203.0.113.152:1:5:1/96 (1 entry, 1 announced)
TSI:
Page 0 idx 0 Type 1 val 8699528
        *L2VPN  Preference: 170/-101
                Next-hop reference count: 5
                Protocol next hop: 203.0.113.152
                Indirect next hop: 0 -
                State: <Active Int Ext>
                Age: 1:34:03    Metric2: 1
                Task: green-l2vpn
                Announcement bits (1): 1-BGP.0.0.0.0+179
                AS path: I
                Communities: Layer2-info: encaps:VPLS, control flags:, mtu: 0
                Label-base: 800008, range: 8, status-vector: 0x9F

...

l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

TSI:

203.0.113.163:CtrlWord:4:3:Local/96 (1 entry, 1 announced)
        *L2CKT  Preference: 7
                Next hop: via so-1/1/2.0 weight 1, selected
                Label-switched-path my-lsp
                Label operation: Push 100000[0]
                Protocol next hop: 203.0.113.163 Indirect next hop: 86af000 296
                State: <Active Int>
                Local AS:    64499
                Age: 10:21
                Task: l2 circuit
                Announcement bits (1): 0-LDP
                AS path: I
                VC Label 100000, MTU 1500, VLAN ID 512


203.0.113.55/24 (1 entry, 1 announced)
TSI:
KRT queued (pending) add
  198.51.100.0/24 -> {Push 300112}
        *BGP    Preference: 170/-101
                Next hop type: Router
                Address: 0x925c208
                Next-hop reference count: 2
                Source: 203.0.113.9
                Next hop: 203.0.113.9 via ge-1/2/0.15, selected
                Label operation: Push 300112
                Label TTL action: prop-ttl
                State: <Active Ext>
```

```
                Local AS:  64509 Peer AS: 65539
                Age: 1w0d 23:06:56
                AIGP: 25
                Task: BGP_65539.203.0.113.9+56732
                Announcement bits (1): 0-KRT
                AS path: 65539 64508 I
                Accepted
                Route Label: 300112
                Localpref: 100
                Router ID: 213.0.113.99
```

show route extensive (Access Route)

user@host> **show route 203.0.113.102 extensive**

```
inet.0: 39256 destinations, 39258 routes (39255 active, 0 holddown, 1 hidden)
203.0.113.102/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 203.0.113.102/32 -> {192.0.2.2}
OSPF area : 0.0.0.0, LSA ID : 203.0.113.102, LSA type : Extern
        *Access Preference: 13
                Next-hop reference count: 78472
                Next hop: 192.0.2.2 via fe-0/0/0.0, selected
                State: <Active Int>
       Age: 12
                Task: RPD Unix Domain Server./var/run/rpd_serv.local
                Announcement bits (2): 0-KRT 1-OSPFv2
                AS path: I
```

user@host> **show route 2001:db8:4641:1::/48 extensive**

```
inet6.0: 75 destinations, 81 routes (75 active, 0 holddown, 0 hidden)
  2001:db8:4641:1::/48 (1 entry, 1 announced)
  TSI:
  KRT in-kernel 2001:db8:4641:1::/48 -> {#0 0.13.1.0.0.1}
          *Access Preference: 13
                  Next hop type: Router, Next hop index: 74548
                  Address: 0x1638c1d8
                  Next-hop reference count: 6
                  Next hop: #0 0.13.1.0.0.1 via demux0.1073753267, selected
                  Session Id: 0x0
                  State: <Active Int>
                  Age: 4:17
                  Validation State: unverified
                  Task: RPD Unix Domain Server./var/run/rpd_serv.local
                  Announcement bits (2): 0-KRT 4-Resolve tree 2
                  AS path: I
2001:db8:4641:1::/128 (1 entry, 1 announced)
  TSI:
  KRT in-kernel 2001:db8:4641:1::/128 -> {#0 0.13.1.0.0.1}
          *Access-internal Preference: 12
                  Next hop type: Router, Next hop index: 74548
                  Address: 0x1638c1d8
                  Next-hop reference count: 6
                  Next hop: #0 0.13.1.0.0.1 via demux0.1073753267, selected
                  Session Id: 0x0
                  State: <Active Int>
                  Age: 4:17
```

```
                Validation State: unverified
                Task: RPD Unix Domain Server./var/run/rpd_serv.local
                Announcement bits (2): 0-KRT 4-Resolve tree 2
                AS path: I
```

show route extensive (BGP PIC Edge)

```
user@host> show route 198.51.100.6 extensive
```

```
ed.inet.0: 6 destinations, 9 routes (6 active, 0 holddown, 0 hidden)
  198.51.100.6/32 (3 entries, 2 announced)
         State: <CalcForwarding>
  TSI:
  KRT in-kernel 198.51.100.6/32 -> {indirect(1048574), indirect(1048577)}
  Page 0 idx 0 Type 1 val 9219e30
      Nexthop: Self
      AS path: [2] 3 I
      Communities: target:2:1
  Path 198.51.100.6 from 198.51.100.4 Vector len 4.  Val: 0
..
          #Multipath Preference: 255
                  Next hop type: Indirect
                  Address: 0x93f4010
                  Next-hop reference count: 2
..
                  Protocol next hop: 198.51.1001.4
                  Push 299824
                  Indirect next hop: 944c000 1048574 INH Session ID: 0x3
                  Indirect next hop: weight 0x1
                  Protocol next hop: 198.51.100.5
                  Push 299824
                  Indirect next hop: 944c1d8 1048577 INH Session ID: 0x4
                  Indirect next hop: weight 0x4000
                  State: <ForwardingOnly Int Ext)>
                  Inactive reason: Forwarding use only
                  Age: 25         Metric2: 15
                  Validation State: unverified
                  Task: RT
                  Announcement bits (1): 0-KRT
                  AS path: 3 I
                  Communities: target:2:1
```

show route extensive (FRR and LFA)

```
user@host> show route 203.0.113.20 extensive
```

```
inet.0: 46 destinations, 49 routes (45 active, 0 holddown, 1 hidden)
203.0.113.20/24 (2 entries, 1 announced)
        State: FlashAll
TSI:
KRT in-kernel 203.0.113.20/24 -> {Push 299776, Push 299792}
        *RSVP   Preference: 7/1
                Next hop type: Router, Next hop index: 1048574
                Address: 0xbbbc010
                Next-hop reference count: 5
                Next hop: 203.0.113.112 via ge-2/1/8.0 weight 0x1, selected
                Label-switched-path europa-d-to-europa-e
                Label operation: Push 299776
                Label TTL action: prop-ttl
```

```
                Session Id: 0x201
                Next hop: 203.0.113.122 via ge-2/1/4.0 weight 0x4001
                Label-switched-path europa-d-to-europa-e
                Label operation: Push 299792
                Label TTL action: prop-ttl
                Session Id: 0x202
                State: Active Int
                Local AS:   64500
                Age: 5:31  Metric: 2
                Task: RSVP
                Announcement bits (1): 0-KRT
                AS path: I
        OSPF    Preference: 10
                Next hop type: Router, Next hop index: 615
                Address: 0xb9d78c4
                Next-hop reference count: 7
                Next hop: 203.0.113.112 via ge-2/1/8.0, selected
                Session Id: 0x201
                State: Int
                Inactive reason: Route Preference
                Local AS:   64500
                Age: 5:35  Metric: 3
                Area: 0.0.0.0
                Task: OSPF
                AS path: I
```

show route extensive (IS-IS)

```
user@host> show route extensive
```

```
IS-IS Preference: 15
                Level: 1
                Next hop type: Router, Next hop index: 1048577
                Address: 0xXXXXXXXXXX
                Next-hop reference count: YY
                Next hop: 203.0.113.22 via ae1.0 balance 43%, selected
                Session Id: 0x141
                Next hop: 203.0.113.22 via ae0.0 balance 57%
```

show route extensive (Route Reflector)

```
user@host> show route extensive
```

```
203.0.113.0/8 (1 entry, 1 announced)

TSI:
KRT in-kernel 203.0.113.0/8 -> {indirect(40)}
        *BGP    Preference: 170/-101
                Source: 192.168.4.214
                Protocol next hop: 198.51.100.192 Indirect next hop: 84ac908 40
                State: <Active Int Ext>
                Local AS: 65548 Peer AS: 65548
                Age: 3:09       Metric: 0       Metric2: 0
                Task: BGP_65548.192.168.4.214+1033
                Announcement bits (2): 0-KRT 4-Resolve inet.0
                AS path: 65544 64507 I <Originator>
                Cluster list:  198.51.100.1
                Originator ID: 203.0.113.88
                Communities: 7777:7777
```

```
                Localpref: 100
                Router ID: 203.0.113.4
                Indirect next hops: 1
                        Protocol next hop: 203.0.113.192 Metric: 0
                        Indirect next hop: 84ac908 40
                        Indirect path forwarding next hops: 0
                                Next hop type: Discard
```

show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

```
user@host> show route label 299872 detail
```

```
mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
299872 (1 entry, 1 announced)
        *LDP    Preference: 9
                Next hop type: Flood
                Next-hop reference count: 3
                Address: 0x9097d90
                Next hop: via vt-0/1/0.1
                Next-hop index: 661
                Label operation: Pop
                Address: 0x9172130
                Next hop: via so-0/0/3.0
                Next-hop index: 654
                Label operation: Swap 299872
                State: **Active Int>
                Local AS:  64511
                Age: 8:20       Metric: 1
                Task: LDP
                Announcement bits (1): 0-KRT
                AS path: I
              FECs bound to route: P2MP root-addr 203.0.113.166, grp 203.0.113.1,
 src 192.168.142.2
```

show route label detail (Multipoint LDP with Multicast-Only Fast Reroute)

```
user@host> show route label 301568 detail
```

```
mpls.0: 18 destinations, 18 routes (18 active, 0 holddown, 0 hidden)
301568 (1 entry, 1 announced)
        *LDP    Preference: 9
                Next hop type: Flood
                Address: 0x2735208
                Next-hop reference count: 3
                Next hop type: Router, Next hop index: 1397
                Address: 0x2735d2c
                Next-hop reference count: 3
                Next hop: 203.0.113.82 via ge-1/2/22.0
                Label operation: Pop
                Load balance label:  None;
                Next hop type: Router, Next hop index: 1395
                Address: 0x2736290
                Next-hop reference count: 3
                Next hop: 203.0.113.2 via ge-1/2/18.0
                Label operation: Pop
                Load balance label:  None;
                State: <Active Int AckRequest MulticastRPF>
                Local AS:    64500
```

```
               Age: 54:05      Metric: 1
               Validation State: unverified
               Task: LDP
               Announcement bits (1): 0-KRT
               AS path: I
              FECs bound to route: P2MP root-addr 198.51.100.1, grp: 203.0.113.1,
 src: 192.168.219.11
               Primary Upstream : 198.51.100.3:0--198.51.100.2:0
                  RPF Nexthops  :
                       ge-1/2/15.0, 10.2.94.1, Label: 301568, weight: 0x1
                       ge-1/2/14.0, 10.2.3.1, Label: 301568, weight: 0x1
               Backup Upstream : 198.51.100.3:0--198.51.100.6:0
                  RPF Nexthops :
                      ge-1/2/20.0, 198.51.100.96, Label: 301584, weight: 0xfffe

                      ge-1/2/19.0, 198.51.100.36, Label: 301584, weight: 0xfffe
```

show route extensive (Flexible VXLAN Tunnel Profile)

user@host> **show route 192.168.0.2 extensive**

```
...
CUSTOMER_0001.inet.0: 5618 destinations, 6018 routes (5618 active, 0 holddown, 0
 hidden)

192.168.0.2/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 192.168.0.2/32 -> {fti0.6 Flags NSR-incapable}
Opaque data client: FLEX-TNL
Address: 0xd00eee8
Opaque-data reference count: 2
Opaque data: Flexible IPv6 VXLAN tunnel profile
        *Static Preference: 5/100
               Next hop type: Router, Next hop index: 74781
               Address: 0x5d9b03cc
               Next-hop reference count: 363
               Next hop: via fti0.6, selected
               Session Id: 0x24c8
               State: <Active Int NSR-incapable OpaqueData Programmed>
               Age: 1:34:00
               Validation State: unverified
                       Tag: 10000001   Tag2: 1
               Announcement bits (2): 1-KRT 3-Resolve tree 30
               AS path: I
               Flexible IPv6 VXLAN tunnel profile
                   Action: Encapsulate
                   Interface: fti0.6 (Index: 10921)
                   VNI: 10000001
                   Source Prefix: 2001:db8:255::2/128
                   Source UDP Port Range: 54614 - 60074
                   Destination Address: 2001:db8:80:1:1:1:0:1
                   Destination UDP Port: 4790
                   VXLAN Flags: 0x08
...
```

show route instance

Syntax

```
show route instance
<brief | detail | summary>
<instance-name>
<operational>
```

Release Information Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description (QFabric systems only) Display routing instance information.

Options

none—(Same as **brief**) Display standard information about all routing instances.

brief | detail | summary—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to **brief**. (These options are not available with the **operational** keyword.)

instance-name—(Optional) Display information for a specified routing instance.

operational—(Optional) Display operational routing instances.

Required Privilege Level view

List of Sample Output

show route instance on page 1885
show route instance detail on page 1885
show route instance operational on page 1886
show route instance summary on page 1887

Output Fields Table 102 on page 1884 lists the output fields for the **show route instance** command. Output fields are listed in the approximate order in which they appear.

Table 102: show route instance Output Fields

Field Name	Field Description	Level of Output
Instance or ***instance-name***	Name of the routing instance.	All levels
Operational Routing Instances	(**operational** keyword only) Names of all operational routing instances.	—
Type	Type of routing instance: **forwarding** or **virtual-router**.	All levels
State	State of the routing instance: **active** or **inactive**.	**detail**
Interfaces	Name of interfaces belonging to this routing instance.	**detail**

Table 102: show route instance Output Fields (continued)

Field Name	Field Description	Level of Output
Tables	Tables (and number of routes) associated with this routing instance.	**detail**
Router ID	Identifier for the router.	**detail**
Primary RIB	Primary table for this routing instance.	**brief** none **summary**
Active/holddown/hidden	Number of active, hold-down, and hidden routes.	All levels

Sample Output

show route instance

```
user@switch> show route instance
Instance             Type
        Primary RIB                                  Active/holddown/hidden
master               forwarding
        inet.0                                       4/0/1

__juniper_private1__ forwarding
        __juniper_private1__.inet.0                  1/0/3

__juniper_private2__ forwarding
        __juniper_private2__.inet.0                  0/0/1

__juniper_private3__ forwarding
        __juniper_private3__.inet.0                  1/0/2

__juniper_private4__ forwarding
        __juniper_private4__.inet.0                  4/0/2

__master.anon__      forwarding

r1                 virtual-router

r2                 virtual-router
```

show route instance detail

```
user@switch> show route instance detail
master:
  Router ID: 10.3.3.7
  Type: forwarding        State: Active
  Tables:
    inet.0                : 5 routes (4 active, 0 holddown, 1 hidden)

__juniper_private1__:
  Router ID: 0.0.0.0
  Type: forwarding        State: Active
  Interfaces:
    lo0.16385
```

```
    bme0.0
  Tables:
    __juniper_private1__.inet.0: 6 routes (1 active, 0 holddown, 3 hidden)

__juniper_private2__:
  Router ID: 0.0.0.0
  Type: forwarding        State: Active
  Interfaces:
    lo0.16384
  Tables:
    __juniper_private2__.inet.0: 1 routes (0 active, 0 holddown, 1 hidden)

__juniper_private3__:
  Router ID: 0.0.0.0
  Type: forwarding        State: Active
  Interfaces:
    bme0.1
  Tables:
    __juniper_private3__.inet.0: 4 routes (1 active, 0 holddown, 2 hidden)

__juniper_private4__:
  Router ID: 0.0.0.0
  Type: forwarding        State: Active
  Interfaces:
    bme0.2
  Tables:
    __juniper_private4__.inet.0: 8 routes (4 active, 0 holddown, 2 hidden)

__master.anon__:
  Router ID: 0.0.0.0
  Type: forwarding        State: Active

r1:
  Router ID: 0.0.0.0
  Type: virtual-router    State: Active
  Interfaces:
    xe-0/0/0.0

r2:
  Router ID: 0.0.0.0
  Type: virtual-router    State: Active
  Interfaces:
    xe-0/0/3.0
```

show route instance operational

```
user@switch> show route instance operational
Operational Routing Instances:

__juniper_private1__
__juniper_private2__
__juniper_private3__
__juniper_private4__
r1---qfabric
r2---qfabric
master
```

show route instance summary

```
user@switch> show route instance summary
Instance             Type
         Primary RIB                                    Active/holddown/hidden
master               forwarding
         inet.0                                         4/0/1

__juniper_private1__ forwarding
         __juniper_private1__.inet.0                    1/0/3

__juniper_private2__ forwarding
         __juniper_private2__.inet.0                    0/0/1

__juniper_private3__ forwarding
         __juniper_private3__.inet.0                    1/0/2

__juniper_private4__ forwarding
         __juniper_private4__.inet.0                    4/0/2

__master.anon__      forwarding

r1                  virtual-router
r2                  virtual-router
```

show route protocol

List of Syntax

Syntax on page 1888
Syntax (EX Series Switches) on page 1888

Syntax

```
show route protocol protocol
<brief | detail | extensive | terse>
<logical-system (all | logical-system-name)>
```

Syntax (EX Series Switches)

```
show route protocol protocol
<brief | detail | extensive | terse>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
ospf2 and **ospf3** options introduced in Junos OS Release 9.2.
ospf2 and **ospf3** options introduced in Junos OS Release 9.2 for EX Series switches.
flow option introduced in Junos OS Release 10.0.
flow option introduced in Junos OS Release 10.0 for EX Series switches.

Description

Display the route entries in the routing table that were learned from a particular protocol.

Options

brief | detail | extensive | terse—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to **brief**.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

protocol—Protocol from which the route was learned:

- **access**—Access route for use by DHCP application
- **access-internal**—Access-internal route for use by DHCP application
- **aggregate**—Locally generated aggregate route
- **arp**—Route learned through the Address Resolution Protocol
- **atmvpn**—Asynchronous Transfer Mode virtual private network
- **bgp**—Border Gateway Protocol
- **ccc**—Circuit cross-connect
- **direct**—Directly connected route
- **dvmrp**—Distance Vector Multicast Routing Protocol
- **esis**—End System-to-Intermediate System
- **flow**—Locally defined flow-specification route
- **frr**—Precomputed protection route or backup route used when a link goes down

- **isis**—Intermediate System-to-Intermediate System
- **ldp**—Label Distribution Protocol
- **l2circuit**—Layer 2 circuit
- **l2vpn**—Layer 2 virtual private network
- **local**—Local address
- **mpls**—Multiprotocol Label Switching
- **msdp**—Multicast Source Discovery Protocol
- **ospf**—Open Shortest Path First versions 2 and 3
- **ospf2**—Open Shortest Path First versions 2 only
- **ospf3**—Open Shortest Path First version 3 only
- **pim**—Protocol Independent Multicast
- **rip**—Routing Information Protocol
- **ripng**—Routing Information Protocol next generation
- **rsvp**—Resource Reservation Protocol
- **rtarget**—Local route target virtual private network
- **spring-te**—Traffic-engineered Source Packet Routing in Networking (SPRING) or segment routing
- **static**—Statically defined route
- **tunnel**—Dynamic tunnel
- **vpn**—Virtual private network

NOTE: EX Series switches run a subset of these protocols. See the switch CLI for details.

Required Privilege Level view

List of Sample Output

show route protocol bgp terse on page 1894
show route protocol direct on page 1894
show route protocol frr on page 1895
show route protocol l2circuit detail on page 1895
show route protocol l2vpn extensive on page 1896
show route protocol ldp on page 1897
show route protocol ldp extensive on page 1897
show route protocol ospf (Layer 3 VPN) on page 1899
show route protocol ospf detail on page 1899
show route protocol rip on page 1899
show route protocol rip detail on page 1900
show route protocol ripng table inet6 on page 1900
show route protocol spring-te on page 1900
show route protocol static detail on page 1901

Output Fields For information about output fields, see the output field tables for the *show route* command, the *show route detail* command, the show route extensive command, or the *show route terse* command.

Sample Output

show route protocol access

```
user@host> show route protocol access
inet.0: 30380 destinations, 30382 routes (30379 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

13.160.0.3/32      *[Access/13] 00:00:09
                    > to 13.160.0.2 via fe-0/0/0.0
13.160.0.4/32      *[Access/13] 00:00:09
                    > to 13.160.0.2 via fe-0/0/0.0
13.160.0.5/32      *[Access/13] 00:00:09
                    > to 13.160.0.2 via fe-0/0/0.0
```

show route protocol access-internal extensive

```
user@host> show route protocol access-internal 13.160.0.19 extensive
inet.0: 100020 destinations, 100022 routes (100019 active, 0 holddown, 1 hidden)
13.160.0.19/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 13.160.0.19/32 -> {13.160.0.2}
        *Access-internal Preference: 12
                Next-hop reference count: 200000
                Next hop: 13.160.0.2 via fe-0/0/0.0, selected
                State: <Active Int>
      Age: 36
                Task: RPD Unix Domain Server./var/run/rpd_serv.local
                Announcement bits (1): 0-KRT
                AS path: I
```

show route protocol arp

```
user@host> show route protocol arp
```

```
inet.0: 43 destinations, 43 routes (42 active, 0 holddown, 1 hidden)

inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)

cust1.inet.0: 1033 destinations, 2043 routes (1033 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

20.20.1.3/32        [ARP/4294967293] 00:04:35, from 20.20.1.1
                      Unusable
20.20.1.4/32        [ARP/4294967293] 00:04:35, from 20.20.1.1
                      Unusable
20.20.1.5/32        [ARP/4294967293] 00:04:32, from 20.20.1.1
                      Unusable
20.20.1.6/32        [ARP/4294967293] 00:04:34, from 20.20.1.1
                      Unusable
20.20.1.7/32        [ARP/4294967293] 00:04:35, from 20.20.1.1
                      Unusable
20.20.1.8/32        [ARP/4294967293] 00:04:35, from 20.20.1.1
                      Unusable
20.20.1.9/32        [ARP/4294967293] 00:04:35, from 20.20.1.1
                      Unusable
20.20.1.10/32       [ARP/4294967293] 00:04:35, from 20.20.1.1
                      Unusable
20.20.1.11/32       [ARP/4294967293] 00:04:33, from 20.20.1.1
                      Unusable
20.20.1.12/32       [ARP/4294967293] 00:04:33, from 20.20.1.1
                      Unusable
20.20.1.13/32       [ARP/4294967293] 00:04:33, from 20.20.1.1
                      Unusable
...
```

show route protocol bgp

```
user@host> show route protocol bgp 192.168.64.0/21
```

```
inet.0: 335832 destinations, 335833 routes (335383 active, 0 holddown, 450 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.64.0/21       *[BGP/170] 6d 10:41:16, localpref 100, from 192.168.69.71
                      AS path: 10458 14203 2914 4788 4788 I
                    > to 192.168.167.254 via fxp0.0
```

show route protocol bgp detail

```
user@host> show route protocol bgp 66.117.63.0/24 detail
```

```
inet.0: 335805 destinations, 335806 routes (335356 active, 0 holddown, 450 hidden)
66.117.63.0/24  (1 entry, 1 announced)
        *BGP    Preference: 170/-101
                Next hop type: Indirect
                Next-hop reference count: 1006436
                Source: 192.168.69.71
                Next hop type: Router, Next hop index: 324
                Next hop: 192.168.167.254 via fxp0.0, selected
                Protocol next hop: 192.168.69.71
                Indirect next hop: 8e166c0 342
                State: <Active Ext>
                Local AS:    69 Peer AS: 10458
                Age: 6d 10:42:42        Metric2: 0
```

```
                Task: BGP_10458.192.168.69.71+179
                Announcement bits (3): 0-KRT 2-BGP RT Background 3-Resolve tree
1
                AS path: 10458 14203 2914 4788 4788 I
                Communities: 2914:410 2914:2403 2914:3400
                Accepted
                Localpref: 100
                Router ID: 207.17.136.192
```

show route protocol bgp detail (Labeled Unicast)

```
user@host> show route protocol bgp 1.1.1.8/32 detail
inet.0: 45 destinations, 46 routes (45 active, 0 holddown, 0 hidden)
1.1.1.8/32 (2 entries, 2 announced)
State:
*BGP Preference: 1/-101
Next hop type: Indirect, Next hop index: 0
Address: 0xc007f30
Next-hop reference count: 2
Source: 1.1.1.1
Next hop type: Router, Next hop index: 614
Next hop: 20.1.1.2 via ge-0/0/1.0, selected
Label-switched-path lsp1
Label operation: Push 1000126, Push 1000125, Push 1000124, Push 1000123, Push
299872(top)
Label TTL action: prop-ttl, prop-ttl, prop-ttl, prop-ttl, prop-ttl(top)
Load balance label: Label 1000126: None; Label 1000125: None; Label 1000124: None;
 Label 1000123: None; Label 299872: None;
Label element ptr: 0xc007860
Label parent element ptr: 0xc0089a0
Label element references: 1
Label element child references: 0
Label element lsp id: 0
Session Id: 0x140
Protocol next hop: 1.1.1.4
Label operation: Push 1000126, Push 1000125, Push 1000124, Push 1000123(top)
Label TTL action: prop-ttl, prop-ttl, prop-ttl, prop-ttl
Load balance label: Label 1000126: None; Label 1000125: None; Label 1000124: None;
 Label 1000123: None;
Indirect next hop: 0xae8d300 1048576 INH Session ID: 0x142
State:
Local AS: 5 Peer AS: 5
Age: 22:43 Metric2: 2
Validation State: unverified
Task: BGP_5.1.1.1.1
Announcement bits (2): 0-KRT 7-Resolve tree 2
AS path: I
Accepted
Route Labels: 1000123(top) 1000124 1000125 1000126
Localpref: 100
Router ID: 1.1.1.1
```

show route protocol bgp detail (Aggregate Extended Community Bandwidth)

```
user@host> show route 10.0.2.0 protocol bgp detail
inet.0: 20 destinations, 26 routes (20 active, 0 holddown, 0 hidden)
10.0.2.0/30 (2 entries, 1 announced)
```

```
       *BGP    Preference: 170/-101
               Next hop type: Router, Next hop index: 0
               Address: 0xb618990
               Next-hop reference count: 3
               Source: 10.0.1.1
               Next hop: 10.0.0.2 via ge-0/0/0.0 balance 40%
               Session Id: 0x0
               Next hop: 10.0.1.1 via ge-0/0/1.0 balance 60%, selected
               Session Id: 0x0
               State: <Active Ext>
               Local AS: 65000 Peer AS: 65001
               Age: 20:33
               Validation State: unverified
               Task: BGP_65001.10.0.1.1
               Announcement bits (3): 0-KRT 2-BGP_Listen.0.0.0.0+179
3-BGP_RT_Background
               AS path: 65001 I
               Communities: bandwidth:65000:60000000
         Accepted Multipath
               Localpref: 100
               Router ID: 128.49.121.137
        BGP    Preference: 170/-101
               Next hop type: Router, Next hop index: 595
               Address: 0xb7a1330
               Next-hop reference count: 9
               Source: 10.0.0.2
               Next hop: 10.0.0.2 via ge-0/0/0.0, selected
               Session Id: 0x141
               State: <NotBest Ext>
               Inactive reason: Not Best in its group - Active preferred
               Local AS: 65000 Peer AS: 65001
               Age: 20:33
               Validation State: unverified
               Task: BGP_65001.10.0.0.2
               AS path: 65001 I
               Communities: bandwidth:65000:40000000
               Accepted MultipathContrib
               Localpref: 100
               Router ID: 128.49.121.132
```

show route protocol bgp extensive

```
user@host> show route protocol bgp 192.168.64.0/21 extensive

inet.0: 335827 destinations, 335828 routes (335378 active, 0 holddown, 450 hidden)
192.168.64.0/21 (1 entry, 1 announced)
TSI:
KRT in-kernel 1.9.0.0/16 -> {indirect(342)}
Page 0 idx 1 Type 1 val db31a80
    Nexthop: Self
    AS path: [69] 10458 14203 2914 4788 4788 I
    Communities: 2914:410 2914:2403 2914:3400
Path 1.9.0.0 from 192.168.69.71 Vector len 4.  Val: 1
        *BGP    Preference: 170/-101
                Next hop type: Indirect
                Next-hop reference count: 1006502
                Source: 192.168.69.71
                Next hop type: Router, Next hop index: 324
                Next hop: 192.168.167.254 via fxp0.0, selected
```

```
                Protocol next hop: 192.168.69.71
                Indirect next hop: 8e166c0 342
                State: <Active Ext>
                Local AS:    69 Peer AS: 10458
                Age: 6d 10:44:45        Metric2: 0
                Task: BGP_10458.192.168.69.71+179
                Announcement bits (3): 0-KRT 2-BGP RT Background 3-Resolve tree
1
                AS path: 10458 14203 2914 4788 4788 I
                Communities: 2914:410 2914:2403 2914:3400
                Accepted
                Localpref: 100
                Router ID: 207.17.136.192
                Indirect next hops: 1
                        Protocol next hop: 192.168.69.71
                        Indirect next hop: 8e166c0 342
                        Indirect path forwarding next hops: 1
                                Next hop type: Router
                                Next hop: 192.168.167.254 via fxp0.0
                        192.168.0.0/16 Originating RIB: inet.0
                          Node path count: 1
                          Forwarding nexthops: 1
                                Nexthop: 192.168.167.254 via fxp0.0
```

show route protocol bgp terse

```
user@host> show route protocol bgp 192.168.64.0/21 terse

inet.0: 24 destinations, 32 routes (23 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

A Destination        P Prf   Metric 1   Metric 2  Next hop        AS path
  192.168.64.0/21    B 170        100            >172.16.100.1    10023 21 I
```

show route protocol direct

```
user@host> show route protocol direct

inet.0: 335843 destinations, 335844 routes (335394 active, 0 holddown, 450 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.8.0/24         *[Direct/0] 17w0d 10:31:49
                       > via fe-1/3/1.0
10.255.165.1/32     *[Direct/0] 25w4d 04:13:18
                       > via lo0.0
172.16.30.0/24       *[Direct/0] 17w0d 23:06:26
                       > via fe-1/3/2.0
192.168.164.0/22    *[Direct/0] 25w4d 04:13:20
                       > via fxp0.0

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

47.0005.80ff.f800.0000.0108.0001.0102.5516.5001/152
                    *[Direct/0] 25w4d 04:13:21
                       > via lo0.0
```

```
inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

2001:db8::10:255:165:1/128
                   *[Direct/0] 25w4d 04:13:21
                    > via lo0.0
fe80::2a0:a5ff:fe12:ad7/128
                   *[Direct/0] 25w4d 04:13:21
                    > via lo0.0
```

show route protocol frr

```
user@host> show route protocol frr
```

```
inet.0: 43 destinations, 43 routes (42 active, 0 holddown, 1 hidden)

inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)

cust1.inet.0: 1033 destinations, 2043 routes (1033 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

20.20.1.3/32       *[FRR/200] 00:05:38, from 20.20.1.1
                    > to 20.20.1.3 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.4/32       *[FRR/200] 00:05:38, from 20.20.1.1
                    > to 20.20.1.4 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.5/32       *[FRR/200] 00:05:35, from 20.20.1.1
                    > to 20.20.1.5 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.6/32       *[FRR/200] 00:05:37, from 20.20.1.1
                    > to 20.20.1.6 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.7/32       *[FRR/200] 00:05:38, from 20.20.1.1
                    > to 20.20.1.7 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.8/32       *[FRR/200] 00:05:38, from 20.20.1.1
                    > to 20.20.1.8 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.9/32       *[FRR/200] 00:05:38, from 20.20.1.1
                    > to 20.20.1.9 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.10/32      *[FRR/200] 00:05:38, from 20.20.1.1
...
```

show route protocol l2circuit detail

```
user@host> show route protocol l2circuit detail
```

```

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
100000 (1 entry, 1 announced)
        *L2CKT  Preference: 7
                Next hop: via ge-2/0/0.0, selected
                Label operation: Pop       Offset: 4
                State: <Active Int>
                Local AS:    99
                Age: 9:52
                Task: Common L2 VC
```

```
                Announcement bits (1): 0-KRT
                AS path: I

ge-2/0/0.0 (1 entry, 1 announced)
        *L2CKT  Preference: 7
                Next hop: via so-1/1/2.0 weight 1, selected
                Label-switched-path my-lsp
                Label operation: Push 100000, Push 100000(top)[0] Offset: -4
                Protocol next hop: 10.245.255.63
                Push 100000 Offset: -4
                 Indirect next hop: 86af0c0 298
                State: <Active Int>
                Local AS:    99
                Age: 9:52
                Task: Common L2 VC
                Announcement bits (2): 0-KRT 1-Common L2 VC
                AS path: I

l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

10.245.255.63:CtrlWord:4:3:Local/96 (1 entry, 1 announced)
        *L2CKT  Preference: 7
                Next hop: via so-1/1/2.0 weight 1, selected
                Label-switched-path my-lsp
                Label operation: Push 100000[0]
                Protocol next hop: 10.245.255.63 Indirect next hop: 86af000 296
                State: <Active Int>
                Local AS:    99
                Age: 10:21
                Task: l2 circuit
                Announcement bits (1): 0-LDP
                AS path: I
                VC Label 100000, MTU 1500, VLAN ID 512
```

show route protocol l2vpn extensive

```
user@host> show route protocol l2vpn extensive


inet.0: 14 destinations, 15 routes (13 active, 0 holddown, 1 hidden)

inet.3: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

mpls.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
800001 (1 entry, 1 announced)
TSI:
KRT in-kernel 800001 /36 -> {so-0/0/0.0}
        *L2VPN  Preference: 7
                Next hop: via so-0/0/0.0 weight 49087 balance 97%, selected
                Label operation: Pop       Offset: 4
                State: <Active Int>
                Local AS:    69
                Age: 7:48
                Task: Common L2 VC
                Announcement bits (1): 0-KRT
                AS path: I

so-0/0/0.0 (1 entry, 1 announced)
```

```
TSI:
KRT in-kernel so-0/0/0.0.0      /16 -> {indirect(288)}
        *L2VPN  Preference: 7
                Next hop: via so-0/0/1.0, selected
                Label operation: Push 800000 Offset: -4
                Protocol next hop: 10.255.14.220
                Push 800000 Offset: -4
                 Indirect next hop: 85142a0 288
                State: <Active Int>
                Local AS:    69
                Age: 7:48
                Task: Common L2 VC
                Announcement bits (2): 0-KRT 1-Common L2 VC
                AS path: I
                Communities: target:69:1 Layer2-info: encaps:PPP,
                control flags:2, mtu: 0
```

show route protocol ldp

user@host> **show route protocol ldp**

```
inet.0: 12 destinations, 13 routes (12 active, 0 holddown, 0 hidden)

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.16.1/32    *[LDP/9] 1d 23:03:35, metric 1
                    > via t1-4/0/0.0, Push 100000
192.168.17.1/32    *[LDP/9] 1d 23:03:35, metric 1
                    > via t1-4/0/0.0

private1__.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

mpls.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

100064             *[LDP/9] 1d 23:03:35, metric 1
                    > via t1-4/0/0.0, Pop
100064(S=0)        *[LDP/9] 1d 23:03:35, metric 1
                    > via t1-4/0/0.0, Pop
100080             *[LDP/9] 1d 23:03:35, metric 1
                    > via t1-4/0/0.0, Swap 100000
```

show route protocol ldp extensive

user@host> **show route protocol ldp extensive**

```
192.168.16.1/32 (1 entry, 1 announced)
        State: <FlashAll>
        *LDP    Preference: 9
                Next-hop reference count: 3
                Next hop: via t1-4/0/0.0, selected
                Label operation: Push 100000
                State: <Active Int>
                Local AS: 64500
                Age: 1d 23:03:58        Metric: 1
                Task: LDP
                Announcement bits (2): 0-Resolve tree 1 2-Resolve tree 2
                AS path: I
```

```
192.168.17.1/32 (1 entry, 1 announced)
        State: <FlashAll>
        *LDP    Preference: 9
                Next-hop reference count: 3
                Next hop: via t1-4/0/0.0, selected
                State: <Active Int>
                Local AS: 64500
                Age: 1d 23:03:58        Metric: 1
                Task: LDP
                Announcement bits (2): 0-Resolve tree 1 2-Resolve tree 2
                AS path: I

private1__.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

mpls.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)

100064 (1 entry, 1 announced)
TSI:
KRT in-kernel 100064 /36 -> {t1-4/0/0.0}
        *LDP    Preference: 9
                Next-hop reference count: 2
                Next hop: via t1-4/0/0.0, selected
                State: <Active Int>
                Local AS: 64500
                Age: 1d 23:03:58        Metric: 1
                Task: LDP
                Announcement bits (1): 0-KRT
                AS path: I
                Prefixes bound to route: 192.168.17.1/32

100064(S=0) (1 entry, 1 announced)
TSI:
KRT in-kernel 100064 /40 -> {t1-4/0/0.0}
        *LDP    Preference: 9
                Next-hop reference count: 2
                Next hop: via t1-4/0/0.0, selected
                Label operation: Pop
                State: <Active Int>
                Local AS: 64500
                Age: 1d 23:03:58        Metric: 1
                Task: LDP
                Announcement bits (1): 0-KRT
                AS path: I

100080 (1 entry, 1 announced)
TSI:
KRT in-kernel 100080 /36 -> {t1-4/0/0.0}
        *LDP    Preference: 9
                Next-hop reference count: 2
                Next hop: via t1-4/0/0.0, selected
                Label operation: Swap 100000
                State: <Active Int>
                Local AS: 64500
                Age: 1d 23:03:58        Metric: 1
                Task: LDP
                Announcement bits (1): 0-KRT
                AS path: I
                Prefixes bound to route: 192.168.16.1/32
```

show route protocol ospf (Layer 3 VPN)

```
user@host> show route protocol ospf
inet.0: 40 destinations, 40 routes (39 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.4/30       *[OSPF/10] 00:05:18, metric 4
                    > via t3-3/2/0.0
10.39.1.8/30        [OSPF/10] 00:05:18, metric 2
                    > via t3-3/2/0.0
10.255.14.171/32   *[OSPF/10] 00:05:18, metric 4
                    > via t3-3/2/0.0
10.255.14.179/32   *[OSPF/10] 00:05:18, metric 2
                    > via t3-3/2/0.0
172.16.233.5/32       *[OSPF/10] 20:25:55, metric 1

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.16/30       [OSPF/10] 00:05:43, metric 1
                    > via so-0/2/2.0
10.255.14.173/32   *[OSPF/10] 00:05:43, metric 1
                    > via so-0/2/2.0
172.16.233.5/32       *[OSPF/10] 20:26:20, metric 1
```

show route protocol ospf detail

```
user@host> show route protocol ospf detail
VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.16/30 (2 entries, 0 announced)
         OSPF   Preference:  10
                Nexthop: via so-0/2/2.0, selected
                State: <Int>
                Inactive reason: Route Preference
                Age: 6:25       Metric: 1
                Area: 0.0.0.0
                Task: VPN-AB-OSPF
                AS path: I
                Communities: Route-Type:0.0.0.0:1:0

...
```

show route protocol rip

```
user@host> show route protocol rip
inet.0: 26 destinations, 27 routes (25 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
10.255.14.177/32   *[RIP/100] 20:24:34, metric 2
                    > to 10.39.1.22 via t3-0/2/2.0
172.16.233.9/32       *[RIP/100] 00:03:59, metric 1
```

show route protocol rip detail

```
user@host> show route protocol rip detail
inet.0: 26 destinations, 27 routes (25 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
10.255.14.177/32 (1 entry, 1 announced)
        *RIP    Preference: 100
                Nexthop: 10.39.1.22 via t3-0/2/2.0, selected
                State: <Active Int>
                Age: 20:25:02   Metric: 2
                Task: VPN-AB-RIPv2
                Announcement bits (2): 0-KRT 2-BGP.0.0.0.0+179
                AS path: I
                Route learned from 10.39.1.22 expires in 96 seconds
```

show route protocol ripng table inet6

```
user@host> show route protocol ripng table inet6
inet6.0: 4215 destinations, 4215 routes (4214 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

1111::1/128        *[RIPng/100] 02:13:33, metric 2
                    > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::2/128        *[RIPng/100] 02:13:33, metric 2
                    > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::3/128        *[RIPng/100] 02:13:33, metric 2
                    > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::4/128        *[RIPng/100] 02:13:33, metric 2
                    > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::5/128        *[RIPng/100] 02:13:33, metric 2
                    > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::6/128        *[RIPng/100] 02:13:33, metric 2
                    > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
```

show route protocol spring-te

```
user@host> show route protocol spring-te
inet.3: 26 destinations, 28 routes (25 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

202.3.0.3/32       *[SPRING-TE/8] 00:03:32, metric 1, metric2 10
                      to 10.0.100.2 via et-0/0/9:0.0, Push 50031, Push 50021(top)

                   >  to 10.1.100.2 via et-0/0/9:1.0, Push 50031, Push 50021(top)

202.4.0.4/32       *[SPRING-TE/8] 00:03:32, metric 1, metric2 10
                   >  to 20.0.100.2 via et-0/0/5:0.0, Push 50041, Push 50011(top)

                       to 30.1.100.2 via et-0/0/3:0.0, Push 50041, Push 50011,
Push 50021(top)

inetcolor.0: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
```

```
202.3.0.3-2111/64
        *[SPRING-TE/8] 00:02:34, metric 1, metric2 10
                      to 10.0.100.2 via et-0/0/9:0.0, Push 50031, Push 50021(top)

                    >  to 10.1.100.2 via et-0/0/9:1.0, Push 50031, Push 50021(top)

202.3.0.3-1234/64
                     *[SPRING-TE/8] 00:02:34, metric 1, metric2 10
                      to 10.0.100.2 via et-0/0/9:0.0, Push 50031, Push 50021(top)

                    >  to 10.1.100.2 via et-0/0/9:1.0, Push 50031, Push 50021(top)
```

show route protocol static detail

```
user@host> show route protocol static detail
```

```
inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
10.5.0.0/16 (1 entry, 1 announced)
        *Static Preference: 5
                Next hop type: Router, Next hop index: 324
                Address: 0x9274010
                Next-hop reference count: 27
                Next hop: 192.168.187.126 via fxp0.0, selected
                Session Id: 0x0
                State: <Active NoReadvrt Int Ext>
                Age: 7w3d 21:24:25
                Validation State: unverified
                Task: RT
                Announcement bits (1): 0-KRT
                AS path: I

10.10.0.0/16 (1 entry, 1 announced)
        *Static Preference: 5
                Next hop type: Router, Next hop index: 324
                Address: 0x9274010
                Next-hop reference count: 27
                Next hop: 192.168.187.126 via fxp0.0, selected
                Session Id: 0x0
                State: <Active NoReadvrt Int Ext>
                Age: 7w3d 21:24:25
                Validation State: unverified
                Task: RT
                Announcement bits (1): 0-KRT
                AS path: I

10.13.10.0/23 (1 entry, 1 announced)
        *Static Preference: 5
                Next hop type: Router, Next hop index: 324
                Address: 0x9274010
                Next-hop reference count: 27
                Next hop: 192.168.187.126 via fxp0.0, selected
                Session Id: 0x0
                State: <Active NoReadvrt Int Ext>
                Age: 7w3d 21:24:25
                Validation State: unverified
                Task: RT
                Announcement bits (1): 0-KRT
                AS path: I
```

show security tpm status

Syntax show security tpm status

Release Information Command introduced in Junos OS Release 15.1X49-D80.
TPM Family and TPM Firmware version details are introduced in Junos OS Release 15.1X49-D120.

Description Display the current status of the Trusted Platform Module (TPM). You can use this **show security tpm status** command to check the status of TPM ownership, master binding key, master encryption password, family version, and firmware version.

Options This command has no options.

Required Privilege Level security

Related Documentation
- Using Trusted Platform Module to Bind Secrets on SRX Series Devices on page 157
- request security tpm master-encryption-password set on page 1691

List of Sample Output show security tpm status on page 1903

Sample Output

show security tpm status

```
user@host> show security tpm status
TPM Status:
  Enabled: yes
  Owned: yes
  Master Binding Key: not-created
  Master Encryption Key: not-configured
  TPM Family: 1.2
  TPM Firmware version: 4.40
```

Table 103 on page 1903 lists the output fields for the **show security tpm status** command.

Table 103: show security tpm status Output Fields

Field Name	Field Description
Enabled	Specifies whether TPM is enabled or disabled.
Owned	Specifies the TPM ownership. TPM can be owned even if the Master Encryption Key and Master Encryption Key are not created/configured.

Table 103: show security tpm status Output Fields (continued)

Field Name	Field Description
Master Binding Key	Displays the TPM's Master Binding Key status whether it is created or not created. TPM generates cryptographic keys and encrypts them so that those can only be decrypted by the TPM. This process is know as binding. Each TPM has a master binding key, which is also know as storage root key.
Master Encryption Key	Displays Master Encryption Password status whether it is set or not set. The encrypted data and the hash of the configuration is protected by the TPM module using the master encryption password.
TPM Family	Displays Trusted Computing Group's (TCG) TPM family version.
TPM Firmware version	Displays the firmware version loaded in TPM.

show security ssh key-pair-identity

Syntax

```
show security ssh key-pair-identity
  ( brief <identity-name> | public identity-name )
```

Release Information Command introduced in Junos OS Release 15.1X49-D70.

Description Display the SSH key pair identity information.

Options

- **brief *identity-name***—Display the brief information for a specified identity. The *identity-name* variable is optional, if an identity is not specified, the command will list brief information of all identities.
- **public *identity-name*** —Display the public key for a specified identity.

NOTE: The public and brief options are mutually exclusive

Required Privilege Level view

Related Documentation

- request security ssh key-pair-identity generate on page 1690
- clear security ssh key-pair-identity on page 1668

List of Sample Output

show security ssh key-pair-identity brief on page 1905
show security ssh key-pair-identity brief sample on page 1905

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

show security ssh key-pair-identity brief

```
user@host> show security ssh key-pair-identity brief
SSH Key Pair Identity Information:
  Name             Create Time      Encrypted
  sample           Dec 28, 17:40    yes
  identity-name    Dec 28, 17:26    yes
```

show security ssh key-pair-identity brief sample

```
user@host> show security ssh key-pair-identity brief sample
```

```
SSH Key Pair Identity Information:
  Name             Create Time      Encrypted
  sample           Dec 28, 17:34    yes
```

show security pki local-certificate

Syntax

```
show security pki local-certificate
<brief | detail>
<certificate-id certificate-id-name>
<system-generated>
```

Release Information Command introduced in Junos OS Release 11.1 for EX Series switches.

Description Display information about the local digital certificates and the corresponding public keys installed in the switch.

Options

none—(Same as brief) Display information about all local digital certificates and corresponding public keys.

brief | detail—(Optional) Display information about local digital certificates and corresponding public keys for the specified level of output.

certificate-id *certificate-id-name*—(Optional) Display information about only the specified the local digital certificate and corresponding public keys.

system-generated—(Optional) Display information about the automatically generated self-signed certificate.

Required Privilege Level view

Related Documentation

- Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 256

List of Sample Output

show security pki local-certificate on page 1909
show security pki local-certificate detail on page 1909

Output Fields Table 104 on page 1907 lists the output fields for the **show security pki local-certificate** command. Output fields are listed in the approximate order in which they appear.

Table 104: show security pki local-certificate Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels
Certificate version	Revision number of the digital certificate.	**detail**
Serial number	Unique serial number of the digital certificate.	**detail**
Issued by	Authority that issued the digital certificate.	none **brief**

Table 104: show security pki local-certificate Output Fields (continued)

Field Name	Field Description	Level of Output
Issued to	Device that was issued the digital certificate.	none **brief**
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the authority. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the authority. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Alternate subject	Domain name or IP address of the device related to the digital certificate.	**detail**
Validity	Time period when the digital certificate is valid. Values are: • **Not before**—Start time when the digital certificate becomes valid. • **Not after**—End time when the digital certificate becomes invalid.	All levels
Public key algorithm	Encryption algorithm used with the private key, such as **rsaEncryption (1024 bits)**.	All levels
Public key verification status	Public key verification status: **Failed** or **Passed**. The **detail** output also provides the verification hash.	All levels
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as **sha1WithRSAEncryption**.	**detail**
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	**detail**
Distribution CRL	Distinguished name information and URL for the certificate revocation list (CRL) server.	**detail**
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Key encipherment**.	**detail**

Sample Output

show security pki local-certificate

```
user@switch> show security pki local-certificate
```

```
Certificate identifier: local-entrust2
  Issued to: router2.juniper.net, Issued by: juniper
  Validity:
    Not before: 2005 Nov 21st, 23:28:22 GMT
    Not after: 2008 Nov 21st, 23:58:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
```

show security pki local-certificate detail

```
user@switch> show security pki local-certificate detail
```

```
Certificate identifier: local-entrust3
  Certificate version: 3
  Serial number: 4355 94f9
  Issuer:
    Organization: juniper, Country: us
  Subject:
    Organization: juniper, Country: us, Common name: switch1.juniper.net
  Alternate subject: switch1.juniper.net
  Validity:
    Not before: 2005 Nov 21st, 23:33:58 GMT
    Not after: 2008 Nov 22nd, 00:03:58 GMT
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
    fb:79:df:d4:a9:03:0f:d3:69:7e:c1:e4:27:35:9c:d9:b1:a2:47:78
    d2:6d:f3:e5:f4:68:4f:b3:04:45:88:57:99:82:39:a6:51:9e:5f:42
    23:3f:d7:6e:3d:a5:54:a9:b1:2d:6e:90:dd:12:8a:bf:ef:2b:20:50
    ba:f0:da:d9:0c:ad:5e:d6:c6:98:3a:ae:3f:90:dd:94:78:c1:ea:2e
    7c:f0:2d:d4:79:d4:cd:f0:52:df:5e:72:f2:e7:ae:66:f7:61:f4:bc
    72:57:3e:6c:6d:d3:24:58:8b:f4:ef:da:2a:6a:fa:eb:98:f8:34:84
    79:54:da:4f:d3:6f:52:1f
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    61:3a:d0:b4:7a:16:9b:39:ba:81:3f:9d:ab:34:e5:c8:be:3b:a1:6d (sha1)
    60:a0:ff:58:05:4a:65:73:9d:74:3a:e1:83:6f:1b:c8 (md5)
  Distribution CRL:
    C=us, O=juniper, CN=CRL1
    http://CA-1/CRL/juniper_us_crlfile.crl
  Use for key: Digital signature
```

show services unified-access-control authentication-table

Syntax

```
show services unified-access-control authentication-table
```

Release Information

Command introduced in Junos OS Release 9.4. Options updated in Junos OS Release 12.1.

Description

Display a summary of the authentication table entries configured from the IC Series UAC Appliance. Authentication tables store mappings between traffic sessions and Unified Access Control (UAC) roles. The IC Series appliance uses the roles specified in the mappings to help determine which UAC policies to apply to a session.

Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a UAC deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series appliance.

You can also use this command to display the content of the authentication table in a user role firewall implementation. The table, pushed from a supporting UAC device, provides the user roles associated with incoming traffic.

Options

- **detail**—Display a detailed view of all authentication table entries.
- **extended**—Display a view of all authentication table entries with the user roles listed.
- **identifier** ***id***—Display all authentication table entries with the specified identifier number.
- **ip** ***source-ip-address***—Display any authentication table entry for the specified IP address.
- **role** ***role-name***—Display all authentication table entries for the specified role name.
- **user** ***username***—Display all authentication table entries for the specified user.

Required Privilege Level

view

Related Documentation

- *Firewall User Authentication Overview*

List of Sample Output

Sample Output

show services unified-access-control authentication-table

user@host>**show services unified-access-control authentication-table**

```
Id    Source IP       Username     Age      Role identifier
1     198.51.100.22          user1        0        0000000001.000005.0
Total: 1
```

show services unified-access-control authentication-table detail

user@host>**show services unified-access-control authentication-table detail**

```
Identifier: 1
  Source IP: 198.51.100.22
  Username: john
  Age: 0
  Role identifier       Role name
    0000000001.000005.0 Users
    1113249951.100616.0 PersonalFirewall
    1183670148.427197.0 UAC
Total: 1
```

show services unified-access-control authentication-table extended

user@host>**show services unified-access-control authentication-table extended**

```
Id    Source IP       Username     Age   Role name
3     10.214.161.195          johna      60    Users, PersonalFirewall
6     10.214.161.183          mayb      60    role-1
Total: 2
```

show services unified-access-control authentication-table identifier id

user@host>**show services unified-access-control authentication-table identifier 1**

```
Identifier: 1
  Source IP: 10.214.161.195
  Username: johna
  Age: 0
  Role identifier       Role name
    0000000001.000005.0 Users
    1113249951.100616.0 PersonalFirewall
    1183670148.427197.0 UAC
Total: 1
```

show services unified-access-control authentication-table ip

user@host>**show services unified-access-control authentication-table ip 10.214.161.183**

```
Id    Source IP       Username     Age      Role identifier
8     10.214.161.183          mayb          0        1420298444.225667.0
Total: 1
```

show services unified-access-control authentication-table role

```
user@host>show services unified-access-control authentication-table role role-1
Id    Source IP       Username     Age      Role identifier
6     10.214.161.183          maybe         60       1420298444.225667.0
Total: 1
```

show services unified-access-control authentication-table user username

```
user@host>show services unified-access-control authentication-table user prasanta
Id    Source IP       Username     Age      Role identifier
7     10.214.161.195         paul1     0        0000000001.000005.0
Total: 1
```

show services unified-access-control policies

Syntax

```
show services unified-access-control policies
```

Release Information Command introduced in Junos OS Release 9.4.

Description Display a summary of resource access policies configured from the IC Series UAC Appliance.

Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series appliance.

Options

- **detail**—Display a detailed view of all policies.
- **identifier** *id*—Display information about a specific policy by identification number.

Required Privilege Level view

Related Documentation

- *Firewall User Authentication Overview*

List of Sample Output

Sample Output

show services unified-access-control policies

```
user@host> services unified-access-control policies
Id    Resource               Action Apply        Role identifier
1     10.100.15.0/24:*       allow  selected     1113249951.100616.0
2     10.100.17.0/24:*       deny   all
```

Sample Output

show services unified-access-control policies detail

```
user@host> services unified-access-control policies detail
Identifier: 1
  Resource: 10.100.15.0/24:*
  Resource: 10.100.16.23-10.100.16.60:*
  Action: allow
  Apply: selected
  Role identifier       Role name
    1113249951.100616.0 Personal Firewall
```

```
    1112927873.881659.0 Antivirus
    1183670148.427197.0 UAC
Identifier: 2
  Resource: 10.100.17.0/24:*
  Resource: 10.100.16.23-10.100.16.60:*
  Resource: 10.100.18.0/24:*
  Action: deny
  Apply: all
```

Sample Output

show services unified-access-control policies identifier 1

```
user@host> show services unified-access-control policies identifier 1
```

```
Identifier: 1
  Resource: 10.100.15.0/24:*
  Resource: 10.100.16.23-10.100.16.60:*
  Action: allow
  Apply: selected
  Role identifier       Role name
    1113249951.100616.0 Personal Firewall
    1112927873.881659.0 Antivirus
    1183670148.427197.0 UAC
```

show services unified-access-control status

Syntax show services unified-access-control status

Release Information Command introduced in Junos OS Release 9.4.

Description Display the status of the connection between the SRX Series device and the IC Series UAC Appliance as well as statistics to help debug connections to the IC Series appliance.

Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series appliance.

Required Privilege Level view

Related Documentation
- *Firewall User Authentication Overview*

List of Sample Output show services unified-access-control status on page 1915

Sample Output

show services unified-access-control status

```
user@host> show services unified-access-control status
Host           Address         Port   Interface     State
dev106vm26     10.64.11.106    11123  ge-0/0/0.0    connected
dev107vm26     10.64.11.106    11123  ge-0/0/0.0    closed
```

show snmp statistics

Syntax

```
show snmp statistics
<subagents>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Option **subagents** introduced in Junos OS Release 14.2.

Description

Display statistics about Simple Network Management Protocol (SNMP) packets sent and received by the router or switch.

Options

subagents—(Optional) Display the statistics of the protocol data unit (PDU), the number of SNMP requests and responses per subagent, and the SNMP statistics received from each subagent per logical system.

Required Privilege Level

view

Related Documentation

- *clear snmp statistics*

List of Sample Output

show snmp statistics on page 1921
show snmp statistics subagents on page 1921

Output Fields

Table 105 on page 1917 describes the output fields for the **show snmp statistics** command. Output fields are listed in the approximate order in which they appear.

Table 105: show snmp statistics Output Fields

Field Name	Field Description
Input	Information about received packets: • **Packets(snmpInPkts)**—Total number of messages delivered to the SNMP entity from the transport service. • **Bad versions—(snmpInBadVersions**) Total number of messages delivered to the SNMP entity that were for an unsupported SNMP version. • **Bad community names—(snmpInBadCommunityNames)** Total number of messages delivered to the SNMP entity that used an SNMP community name not known to the entity. • **Bad community uses—(snmpInBadCommunityUses)** Total number of messages delivered to the SNMP entity that represented an SNMP operation that was not allowed by the SNMP community named in the message. • **ASN parse errors—(snmpInASNParseErrs)** Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages. • **Too bigs—(snmpInTooBigs)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **tooBig**. • **No such names—(snmpInNoSuchNames)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **noSuchName**. • **Bad values—(snmpInBadValues)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **badValue**. • **Read onlys—(snmpInReadOnlys)** Total number of valid SNMP PDUs delivered to the SNMP entity with an error status field of **readOnly**. Only incorrect implementations of SNMP generate this error.

Table 105: show snmp statistics Output Fields (continued)

Field Name	Field Description
Input (continued)	• **General errors—(snmpInGenErrs)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **genErr**. • **Total requests varbinds—(snmpInTotalReqVars)** Total number of MIB objects retrieved successfully by the SNMP entity as a result of receiving valid SNMP **GetRequest** and **GetNext** PDUs. • **Total set varbinds—(snmpInSetVars)** Total number of MIB objects modified successfully by the SNMP entity as a result of receiving valid SNMP **SetRequest** PDUs. • **Get requests—(snmpInGetRequests)** Total number of SNMP **GetRequest** PDUs that have been accepted and processed by the SNMP entity. • **Get nexts—(snmpInGetNexts)** Total number of SNMP **GetNext** PDUs that have been accepted and processed by the SNMP entity. • **Set requests—(snmpInSetRequests)** Total number of SNMP **SetRequest** PDUs that have been accepted and processed by the SNMP entity. • **Get responses—(snmpInGetResponses)** Total number of SNMP **GetResponse** PDUs that have been accepted and processed by the SNMP entity. • **Traps—(snmpInTraps)** Total number of SNMP traps generated by the SNMP entity. • **Silent drops—(snmpSilentDrops)** Total number of **GetRequest**, **GetNextRequest**, **GetBulkRequest**, **SetRequests**, and **InformRequest** PDUs delivered to the SNMP entity that were silently dropped because the size of a reply containing an alternate response PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the requests. • **Proxy drops—(snmpProxyDrops)** Total number of **GetRequest**, **GetNextRequest**, **GetBulkRequest**, **SetRequests**, and **InformRequest** PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in such a way (other than a timeout) that no response PDU could be returned. • **Commit pending drops**—Number of SNMP packets for **Set** requests dropped because of a previous pending SNMP **Set** request on the committed configuration. • **Throttle drops**—Number of SNMP packets for any requests dropped reaching the throttle limit.

Table 105: show snmp statistics Output Fields (continued)

Field Name	Field Description
V3 Input	Information about SNMP version 3 packets: • **Unknown security models—(snmpUnknownSecurityModels)** Total number of packets received by the SNMP engine that were dropped because they referenced a security model that was not known to or supported by the SNMP engine. • **Invalid messages—(snmpInvalidMsgs)** Number of packets received by the SNMP engine that were dropped because there were invalid or inconsistent components in the SNMP message. • **Unknown pdu handlers—(snmpUnknownPDUHandlers)** Number of packets received by the SNMP engine that were dropped because the PDU contained in the packet could not be passed to an application responsible for handling the PDU type. • **Unavailable contexts—(snmpUnavailableContexts)** Number of requests received for a context that is known to the SNMP engine, but is currently unavailable. • **Unknown contexts—(snmpUnknownContexts)** Total number of requests received for a context that is unknown to the SNMP engine. • **Unsupported security levels—(usmStatsUnsupportedSecLevels)** Total number of packets received by the SNMP engine that were dropped because they requested a security level unknown to the SNMP engine (or otherwise unavailable). • **Not in time windows—(usmStatsNotInTimeWindows)** Total number of packets received by the SNMP engine that were dropped because they appeared outside the authoritative SNMP engine's window. • **Unknown user names—(usmStatsUnknownUserNames)** Total number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine. • **Unknown engine ids—(usmStatsUnknownEngineIDs)** Total number of packets received by the SNMP engine that were dropped because they referenced an SNMP engine ID that was not known to the SNMP engine. • **Wrong digests—(usmStatsWrongDigests)** Total number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value. • **Decryption errors—(usmStatsDecryptionErrors)** Total number of packets received by the SNMP engine that were dropped because they could not be decrypted.

Table 105: show snmp statistics Output Fields (continued)

Field Name	Field Description
Output	Information about transmitted packets: • **Packets—(snmpOutPkts)** Total number of messages passed from the SNMP entity to the transport service. • **Too bigs—(snmpOutTooBigs)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **tooBig**. • **No such names—(snmpOutNoSuchNames)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **noSuchName**. • **Bad values—(snmpOutBadValues)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **badValue**. • **General errors—(snmpOutGenErrs)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **genErr**. • **Get requests—(snmpOutGetRequests)** Total number of SNMP **GetRequest** PDUs generated by the SNMP entity. • **Get nexts—(snmpOutGetNexts)** Total number of SNMP **GetNext** PDUs generated by the SNMP entity. • **Set requests—(snmpOutSetRequests)** Total number of SNMP **SetRequest** PDUs generated by the SNMP entity. • **Get responses—(snmpOutGetResponses)** Total number of SNMP **GetResponse** PDUs generated by the SNMP entity. • **Traps—(snmpOutTraps)** Total number of SNMP traps generated by the SNMP entity.

Table 106 on page 1920 describes the output fields for the **show snmp statistics subagents** command. Output fields are listed in the approximate order in which they appear.

Table 106: show snmp statistics subagents Output Fields

Field Name	Field Description
Subagent	Location of the SNMP subagent.
Request PDUs	Number of PDUs requested by the SNMP manager.
Response PDUs	Number of response PDUs sent by the SNMP subagent.
Request Variables	Number of variable bindings on the PDUs requested by the SNMP manager.
Response Variables	Number of variable bindings on the PDUs sent by the SNMP subagent.
Average Response Time	Average time taken by the SNMP subagent to send statistics response.
Maximum Response Time	Maximum time taken by the SNMP subagent to send the statistics response.

Sample Output

show snmp statistics

```
user@host> show snmp statistics
```

```
SNMP statistics:
  Input:
    Packets: 246213, Bad versions: 12, Bad community names: 12,
    Bad community uses: 0, ASN parse errors: 96,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 227084, Total set varbinds: 67,
    Get requests: 44942, Get nexts: 190371, Set requests: 10712,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0,
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 1
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 44, Wrong digests: 23, Decryption errors: 0
  Output:
    Packets: 246093, Too bigs: 0, No such names: 31561,
    Bad values: 0, General errors: 2,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 246025, Traps: 0
```

show snmp statistics subagents

```
user@host> show snmp statistics subagents

  Subagent: /var/run/cosd-20
    Request PDUs: 0, Response PDUs: 0,
    Request Variables: 0, Response Variables: 0,
    Average Response Time(ms): 0.00,
    Maximum Response Time(ms): 0.00

  Subagent: /var/run/pfed-30
    Request PDUs: 0, Response PDUs: 0,
    Request Variables: 0, Response Variables: 0,
    Average Response Time(ms): 0.00,
    Maximum Response Time(ms): 0.00

  Subagent: /var/run/rmopd-15
    Request PDUs: 0, Response PDUs: 0,
    Request Variables: 0, Response Variables: 0,
    Average Response Time(ms): 0.00,
    Maximum Response Time(ms): 0.00

  Subagent: /var/run/chassisd-30
    Request PDUs: 33116, Response PDUs: 33116,
    Request Variables: 33116, Response Variables: 33116,
    Average Response Time(ms): 1.83,
    Maximum Response Time(ms): 203.48

  Subagent: /var/run/pkid-13
    Request PDUs: 0, Response PDUs: 0,
```

```
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/apsd-13
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/dfcd-32
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/mib2d-33
  Request PDUs: 74211, Response PDUs: 74211,
  Request Variables: 74211, Response Variables: 74211,
  Average Response Time(ms): 2.30,
  Maximum Response Time(ms): 51.04

Subagent: /var/run/license-check-16
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/craftd-14
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/bfdd-19
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/smihelperd-24
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/cfmd-18
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/rpd_snmp
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/l2tpd-18
  Request PDUs: 0, Response PDUs: 0,
```

```
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00
```

show ssl-certificates

Syntax show ssl certificates

Release Information Command introduced in Junos OS Release 17.2R1 for EX Series switches.

Description Display information about the Secure Sockets Layer (SSL) certificates installed on the switch. When you configure PEAP as the authentication protocol for MAC RADIUS authentication, you must load the server-side Secure Sockets Layer (SSL) certificate on the switch. PEAP requires an SSL certificate to create a secure TLS tunnel to protect user authentication, and uses server-side public key certificates to authenticate the server. It then creates an encrypted TLS tunnel between the client and the authentication server. The key for this encryption are transported using the server's public key. The ensuing exchange of authentication information inside the tunnel to authenticate the client is then encrypted and user credentials are safe from eavesdropping.

Options **none**—Display information about all SSL certificates.

detail—Display information about SSL certificates for the specified level of output.

Required Privilege Level view

Related Documentation
- *Configuring PEAP for MAC RADIUS Authentication*

List of Sample Output
show ssl-certificates on page 1925
show ssl-certificates detail on page 1925

Output Fields Table 104 on page 1907 lists the output fields for the **show ssl-certificates** command. Output fields are listed in the approximate order in which they appear.

Table 107: show ssl-certificates Output Fields

Field Name	Field Description	Level of Output
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: • **C**—Country of origin. • **ST**—State or province name. • **L**—Locality. • **O**—Organization of origin. • **OU**—Organizational unit. • **CN**—Common name of the authority.	All levels
Valid from	Start time when the digital certificate becomes valid.	**detail**

Table 107: show ssl-certificates Output Fields (continued)

Field Name	Field Description	Level of Output
Valid from	End time when the digital certificate becomes invalid.	**detail**
Serial number	Unique serial number of the digital certificate.	**detail**
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **C**—Country of origin. • **ST**—State or province name. • **L**—Locality. • **O**—Organization of origin. • **OU**—Organizational unit. • **CN**—Common name of the authority.	**detail**

Sample Output

show ssl-certificates

```
user@root> show ssl-certificates

 Issuer:
/C=IN/ST=KA/L=Blr/O=JNPR/OU=CP/CN=User-Radius/emailAddress=user@juniper.net
```

show ssl-certificates detail

```
user@root> show ssl-certificates detail

    Issuer:
/C=IN/ST=KA/L=Blr/O=JNPR/OU=CP/CN=User-Radius/emailAddress=user@juniper.net
    Valid From:    May 30 17:41:04 2016 GMT
    Valid Till:    May 29 17:41:04 2026 GMT
    Serial Number: 0
    Subject:
/C=IN/ST=KA/L=Blr/O=JNPR/OU=CP/CN=User-Radius/emailAddress=user@juniper.net
```

show subscribers

Syntax

```
show subscribers
<detail | extensive | terse>
<aci-interface-set-name aci-interface-set-name>
<address address>
<agent-circuit-identifier agent-circuit-identifier>
<agent-remote-identifier agent-remote-identifier>
<aggregation-interface-set-name interface-set-name>
<client-type client-type>
<count>
<id session-id <accounting-statistics>>
<interface interface <accounting-statistics>>
<logical-system logical-system>
<mac-address mac-address>
<physical-interface physical-interface-name>
<profile-name profile-name>
<routing-instance routing-instance>
<stacked-vlan-id stacked-vlan-id>
<subscriber-state subscriber-state>
<user-name user-name>
<vci vci-identifier>
<vpi vpi-identifier>
<vlan-id vlan-id>
```

Release Information

Command introduced in Junos OS Release 9.3.
Command introduced in Junos OS Release 9.3 for EX Series switches.
client-type, **mac-address**, **subscriber-state**, and **extensive** options introduced in Junos OS Release 10.2.
count option usage with other options introduced in Junos OS Release 10.2.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Options **aci-interface-set-name** and **agent-circuit-identifier** introduced in Junos OS Release 12.2.
The **physical-interface** and **user-name** options introduced in Junos OS Release 12.3.
Options **vci** and **vpi** introduced in Junos OS Release 12.3R3 and supported in later 12.3R*x* releases.
Options **vci** and **vpi** supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Enhanced subscriber management supported in Junos OS Release 15.1R3 on MX Series routers.
accounting-statistics option added in Junos OS Release 15.1R3 and 17.4R1 on MX Series routers.
aggregation-interface-set-name option added in Junos OS Release 18.4R1 on MX Series routers.

Description

Display information for active subscribers.

Options

detail | extensive | terse—(Optional) Display the specified level of output.

aci-interface-set-name—(Optional) Display all dynamic subscriber sessions that use the specified agent circuit identifier (ACI) interface set. Use the ACI interface set name generated by the router, such as aci-1003-ge-1/0/0.4001, and not the actual ACI value found in the DHCP or PPPoE control packets.

address—(Optional) Display subscribers whose IP address matches the specified address. You must specify the IPv4 or IPv6 address prefix without a netmask (for example, 192.0.2.0). If you specify the IP address as a prefix with a netmask (for example, 192.0.2.0/32), the router displays a message that the IP address is invalid, and rejects the command.

agent-circuit-identifier—(Optional) Display all dynamic subscriber sessions whose ACI value matches the specified string. You can specify either the complete ACI string or a substring. To specify a substring, you must enter characters that form the beginning of the string, followed by an asterisk (*) as a wildcard to substitute for the remainder of the string. The wildcard can be used only at the end of the specified substring; for example:

```
user@host1> show subscribers agent-circuit-identifier substring*
```

Junos OS Release	Substring Support
Junos OS Release 13.3R1	You can specify a substring without a wildcard.
Starting in Junos OS Release 14.1R1	You must specify the complete ACI string; you cannot specify a wildcard.
Starting in Junos OS Release 15.1R7, 16.1R7, 16.2R3, 17.1R3, 17.2R3, 17.3R3, 17.4R2, 18.1R2, 18.2R1	You can specify a substring, but you must include the wildcard character at the end of the substring.

agent-remote-identifier—(Optional) Display all dynamic subscriber sessions whose ARI value matches the specified string. You must specify the complete ACI string; you cannot specify a wildcard.

aggregation-interface-set-name *interface-set-name*—(Optional) Display summary information for the specified aggregation node interface set, including interface, VLAN ID, username and LS:RI.

client-type—(Optional) Display subscribers whose client type matches one of the following client types:

- **dhcp**—DHCP clients only.
- **dotlx**—Dotlx clients only.
- **essm**—ESSM clients only.
- **fixed-wireless-access**—Fixed wireless access clients only.
- **fwauth**—FwAuth (authenticated across a firewall) clients only.
- **l2tp**—L2TP clients only.

- **mlppp**—MLPPP clients only.
- **ppp**—PPP clients only.
- **pppoe**—PPPoE clients only.
- **static**—Static clients only.
- **vlan**—VLAN clients only.
- **vlan-oob**—VLAN out-of-band (ANCP-triggered) clients only.
- **vpls-pw**—VPLS pseudowire clients only.
- **xauth**—Xauth clients only.

count—(Optional) Display the count of total subscribers and active subscribers for any specified option. You can use the **count** option alone or with the **address**, **client-type**, **interface**, **logical-system**, **mac-address**, **profile-name**, **routing-instance**, **stacked-vlan-id**, **subscriber-state**, or **vlan-id** options.

id ***session-id***—(Optional) Display a specific subscriber session whose session ID matches the specified subscriber ID. You can display subscriber IDs by using the **show subscribers extensive** or the **show subscribers interface extensive** commands.

id ***session-id*** **accounting-statistics**—(Optional) Display accurate subscriber accounting statistics for a subscriber session with the specified ID. Requires the **actual-transmit-statistics** statement to be configured in the dynamic profile for the dynamic logical interface. If the statement is not configured, a value of 0 is displayed for accounting statistics.

interface—(Optional) Display subscribers whose interface matches the specified interface.

interface **accounting-statistics**—(Optional) Display subscriber accounting statistics for the specified interface. Requires the **actual-transmit-statistics** statement to be configured in the dynamic profile for the dynamic logical interface.

logical-system—(Optional) Display subscribers whose logical system matches the specified logical system.

mac-address—(Optional) Display subscribers whose MAC address matches the specified MAC address.

physical-interface-name—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose physical interface matches the specified physical interface.

profile-name—(Optional) Display subscribers whose dynamic profile matches the specified profile name.

routing-instance—(Optional) Display subscribers whose routing instance matches the specified routing instance.

stacked-vlan-id—(Optional) Display subscribers whose stacked VLAN ID matches the specified stacked VLAN ID.

subscriber-state—(Optional) Display subscribers whose subscriber state matches the specified subscriber state (ACTIVE, CONFIGURED, INIT, TERMINATED, or TERMINATING).

user-name—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose username matches the specified subscriber name.

vci-identifier—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual circuit identifier (VCI) matches the specified VCI identifier. The range of values is 0 through 255.

vpi-identifier—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual path identifier (VPI) matches the specified VPI identifier. The range of values is 0 through 65,535.

vlan-id—(Optional) Display subscribers whose VLAN ID matches the specified VLAN ID, regardless of whether the subscriber uses a single-tagged or double-tagged VLAN. For subscribers using a double-tagged VLAN, this option displays subscribers where the inner VLAN tag matches the specified VLAN ID. To display only subscribers where the specified value matches only double-tagged VLANs, use the **stacked-vlan-id** ***stacked-vlan-id*** option to match the outer VLAN tag.

NOTE: Because of display limitations, logical system and routing instance output values are truncated when necessary.

Required Privilege Level

view

Related Documentation

- *show subscribers summary*
- *Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration*
- *Verifying and Managing Configurations for Dynamic VLANs Based on Access-Line Identifiers*
- *Verifying and Managing Junos OS Enhanced Subscriber Management*

List of Sample Output

show subscribers address detail (Enhanced Subscriber Management) on page 1960

Output Fields Table 108 on page 1931 lists the output fields for the **show subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 108: show subscribers Output Fields

Field Name	Field Description
Interface	Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface. The * character indicates a continuation of addresses for the same session.
IP Address/VLAN ID	Subscriber IP address or VLAN ID associated with the subscriber in the form *tpid.vlan-id* No IP address or VLAN ID is assigned to an L2TP tunnel-switched session. For these subscriber sessions the value is **Tunnel-switched**.
User Name	Name of subscriber.
LS:RI	Logical system and routing instance associated with the subscriber.
Type	Subscriber client type (DHCP, FWA, GRE, L2TP, PPP, PPPoE, STATIC-INTERFACE, VLAN).
IP Address	Subscriber IPv4 address.
IP Netmask	Subscriber IP netmask. (MX Series) This field displays 255.255.255.255 by default. For tunneled or terminated PPP subscribers only, this field displays the actual value of Framed-IP-Netmask when the SDB_FRAMED_PROTOCOL attribute in the session database is equal to AUTHD_FRAMED_PROTOCOL_PPP. This occurs in the use case where the LNS generates access-internal routes when it receives Framed-IP-Netmask from RADIUS during authorization. When it receives Framed-Pool from RADIUS, the pool mask is ignored and the default /32 mask is used.
Primary DNS Address	IP address of primary DNS server. This field is displayed with the **extensive** option only when the address is provided by RADIUS.
Secondary DNS Address	IP address of secondary DNS server. This field is displayed with the **extensive** option only when the address is provided by RADIUS.
IPv6 Primary DNS Address	IPv6 address of primary DNS server. This field is displayed with the **extensive** option only when the address is provided by RADIUS.
IPv6 Secondary DNS Address	IPv6 address of secondary DNS server. This field is displayed with the **extensive** option only when the address is provided by RADIUS.
Domain name server inet	IP addresses for the DNS server, displayed in order of configuration. This field is displayed with the **extensive** option only when the addresses are derived from the access profile or the global access configuration.

Table 108: show subscribers Output Fields (continued)

Field Name	Field Description
Domain name server inet6	IPv6 addresses for the DNS server, displayed in order of configuration. This field is displayed with the **extensive** option only when the addresses are derived from the access profile or the global access configuration.
Primary WINS Address	IP address of primary WINS server.
Secondary WINS Address	IP address of secondary WINS server.
IPv6 Address	Subscriber IPv6 address, or multiple addresses.
IPv6 Prefix	Subscriber IPv6 prefix. If you are using DHCPv6 prefix delegation, this is the delegated prefix.
IPv6 User Prefix	IPv6 prefix obtained through NDRA.
IPv6 Address Pool	Subscriber IPv6 address pool. The IPv6 address pool is used to allocate IPv6 prefixes to the DHCPv6 clients.
IPv6 Network Prefix Length	Length of the network portion of the IPv6 address.
IPv6 Prefix Length	Length of the subscriber IPv6 prefix.
Logical System	Logical system associated with the subscriber.
Routing Instance	Routing instance associated with the subscriber.
Interface	(Enhanced subscriber management for MX Series routers) Name of the enhanced subscriber management logical interface, in the form **demux0.*nnnn*** (for example, **demux0.3221225472**), to which access-internal and framed subscriber routes are mapped.
Interface Type	Whether the subscriber interface is **Static** or **Dynamic**.

Table 108: show subscribers Output Fields (continued)

Field Name	Field Description
Interface Set	Internally generated name of the dynamic ACI or ALI interface set used by the subscriber session. The prefix of the name indicates the string received in DHCP or PPPoE control packets on which the interface set is based. For ALI interface sets, the prefix indicates that the value is configured as a trusted option to identify the subscriber line. The name of the interface set uses one of the following prefixes: • **aci**—ACI; for example, aci-1033-demux0.3221225524. This is the only prefix allowed for ACI interface sets. • **ari**—ARI; for example, ari-1033-demux0.3221225524. • **aci+ari**—Both the ACI and ARI; for example, aci+ari-1033-demux0.3221225524. • **noids**—Neither the ACI nor the ARI were received; for example, noids-1033-demux0.3221225524. NOTE: ACI interface sets are configured with the **agent-circuit-identifier** autoconfiguration stanza. ALI interface sets are configured with the **line-identity** autoconfiguration stanza. Besides dynamic ACI and ALI interface sets, this field can be an interface set based on a substring of the ARI string. This occurs when the dynamic profile includes the predefined variable $junos-pon-id-interface-set-name, and the profile is applied for a passive optical network (PON). The ARI string is inserted by the optical line terminal (OLT). The final substring in the string, unique for the PON, identifies individual subscriber circuits, and is used as the name of the interface set.
Interface Set Type	Interface type of the ACI interface set: **Dynamic**. This is the only ACI interface set type currently supported.
Interface Set Session ID	Identifier of the dynamic ACI interface set entry in the session database.
Underlying Interface	Name of the underlying interface for the subscriber session.
Dynamic Profile Name	Dynamic profile used for the subscriber.
Dynamic Profile Version	Version number of the dynamic profile used for the subscriber.
MAC Address	MAC address associated with the subscriber.
State	Current state of the subscriber session (**Init**, **Configured**, **Active**, **Terminating**, **Tunneled**).
L2TP State	Current state of the L2TP session, **Tunneled** or **Tunnel-switched**. When the value is **Tunnel-switched**, two entries are displayed for the subscriber; the first entry is at the LNS interface on the LTS and the second entry is at the LAC interface on the LTS.
Tunnel switch Profile Name	Name of the L2TP tunnel switch profile that initiates tunnel switching.
Local IP Address	IP address of the local gateway (LAC).
Remote IP Address	IP address of the remote peer (LNS).
VLAN Id	VLAN ID associated with the subscriber in the form *tpid.vlan-id*.

Table 108: show subscribers Output Fields (continued)

Field Name	Field Description
Stacked VLAN Id	Stacked VLAN ID associated with the subscriber in the form *tpid.vlan-id*.
RADIUS Accounting ID	RADIUS accounting ID associated with the subscriber.
Agent Circuit ID	For the **dhcp** client type, option 82 agent circuit ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format. For the **vlan-oob** client type, the agent circuit ID or access-loop circuit identifier that identifies the subscriber line based on the subscriber-facing DSLAM interface on which the subscriber request originates.
Agent Remote ID	For the **dhcp** client type, option 82 agent remote ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format. For the **vlan-oob** client type, the agent remote ID or access-loop remote identifier that identifies the subscriber line based on the NAS-facing DSLAM interface on which the subscriber request originates.
Aggregation Interface-set Name	Value of the $junos-aggregation-interface-set-name predefined variable; one of the following: • When the **hierarchical-access-network-detection** option is configured for the access lines and the value of the Access-Aggregation-Circuit-ID-ASCII attribute (TLV 0x0003) received either in the ANCP Port Up message or PPPoE PADR IA tags begins with a **#** character, then the variable takes the value of the remainder of the string after the **#** character. • When the **hierarchical-access-network-detection** option is not configured, or if the sting does not begin with the **#** character, then the variable takes the value specified with the **predefined-variable-defaults** statement.
Accounting Statistics	Actual transmitted subscriber accounting statistics by session ID or interface. Service accounting statistics are not included. These statistics do not include overhead bytes or dropped packets; they are the accurate statistics used by RADIUS. The statistics are counted when the **actual-transmit-statistics** statement is included in the dynamic profile.
DHCP Relay IP Address	IP address used by the DHCP relay agent.
ATM VPI	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual path identifier (VPI) on the subscriber's physical interface.
ATM VCI	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual circuit identifier (VCI) for each VPI configured on the subscriber interface.
Login Time	Date and time at which the subscriber logged in.
DHCPV6 Options	**len** = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCPv6 options.
Server DHCP Options	**len** = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCP options.
Server DHCPV6 Options	**len** = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCPv6 options.

Table 108: show subscribers Output Fields (continued)

Field Name	Field Description
DHCPV6 Header	**len** = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCPv6 options.
Effective shaping-rate	Actual downstream traffic shaping rate for the subscriber, in kilobits per second.
IPv4 Input Service Set	Input service set in access dynamic profile.
IPv4 Output Service Set	Output service set in access dynamic profile.
PCEF Profile	PCEF profile in access dynamic profile.
PCEF Rule/Rulebase	PCC rule or rulebase used in dynamic profile.
Dynamic configuration	Values for variables that are passed into the dynamic profile from RADIUS.
Service activation time	Time at which the first family in this service became active.
IPv4 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to IPv4 packets that fail the RPF check.
IPv6 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to IPv6 packets that fail the RPF check.
DHCP Options	**len** = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCP options, as defined in RFC 2132.
Session ID	ID number for a subscriber session.
Underlying Session ID	For DHCPv6 subscribers on a PPPoE network, displays the session ID of the underlying PPPoE interface.
Service Sessions	Number of service sessions (that is, a service activated using RADIUS CoA) associated with the subscribers.
Service Session ID	ID number for a subscriber service session.
Service Session Name	Service session profile name.
Session Timeout (seconds)	Number of seconds of access provided to the subscriber before the session is automatically terminated.
Idle Timeout (seconds)	Number of seconds subscriber can be idle before the session is automatically terminated.
IPv6 Delegated Address Pool	Name of the pool used for DHCPv6 prefix delegation.
IPv6 Delegated Network Prefix Length	Length of the prefix configured for the IPv6 delegated address pool.

Table 108: show subscribers Output Fields (continued)

Field Name	Field Description
IPv6 Interface Address	Address assigned by the Framed-Ipv6-Prefix AAA attribute. This field is displayed only when the predefined variable $junos-ipv6-address is used in the dynamic profile.
IPv6 Framed Interface Id	Interface ID assigned by the Framed-Interface-Id AAA attribute.
ADF IPv4 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv4 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
IPv4 Input Filter Name	Name assigned to the IPv4 input filter (client or service session).
IPv4 Output Filter Name	Name assigned to the IPv4 output filter (client or service session).
IPv6 Input Filter Name	Name assigned to the IPv6 input filter (client or service session).
IPv6 Output Filter Name	Name assigned to the IPv6 output filter (client or service session).
IFL Input Filter Name	Name assigned to the logical interface input filter (client or service session).
IFL Output Filter Name	Name assigned to the logical interface output filter (client or service session).
DSL type	PPPoE subscriber's access line type reported by the PPPoE intermediate agent in a PADI or PADO packet in the Vendor-Specific-Tags TLV in subattribute DSL-Type (0x0091). The DSL type is one of the following types: **ADSL**, **ADSL2**, **ADSL2+**, **OTHER**, **SDSL**, **VDSL**, or **VDSL2**.
Frame/Cell Mode	Mode type of the PPPoE subscriber's access line determined by the PPPoE daemon based on the received subattribute DSL-Type (0x0091): • **Cell**—When the DSL line type is one of the following: ADSL, ADSL2, or ADSL2+. • **Frame**—When the DSL line type is one of the following: OTHER, SDSL, VDSL, or VDSL2. The value is stored in the subscriber session database.
Overhead accounting bytes	Number of bytes added to or subtracted from the actual downstream cell or frame overhead to account for the technology overhead of the DSL line type. The value is determined by the PPPoE daemon based on the received subattribute DSL-Type (0x0091). The value is stored in the subscriber session database.

Table 108: show subscribers Output Fields (continued)

Field Name	Field Description
Actual upstream data rate	Unadjusted upstream data rate for the PPPoE subscriber's access line reported by the PPPoE intermediate agent in a PADI or PADO packet in the Vendor-Specific-Tags TLV in subattribute Actual-Net-Data-Rate-Upstream (0x0081).
Actual downstream data rate	Unadjusted downstream data rate for the PPPoE subscriber's access line reported by the PPPoE intermediate agent in a PADI or PADO packet in the Vendor-Specific-Tags TLV in subattribute Actual-Net-Data-Rate-Downstream (0x0082).
Adjusted downstream data rate	Adjusted downstream data rate for the PPPoE subscriber's access line, calculated by the PPPoE daemon and stored in the subscriber session database.
Adjusted upstream data rate	Adjusted upstream data rate for the PPPoE subscriber's access line, calculated by the PPPoE daemon and stored in the subscriber session database.
Local TEID-U	Tunnel endpoint identifier on the BNG for the GTP-U user plane tunnel to the eNodeB. The identifier is allocated by the BNG. A fully qualified local TEID-C consists of this identifier and the **GTPU Tunnel Local IP address** value.
Local TEID-C	Tunnel endpoint identifier on the BNG for the GTP-C control plane tunnel to the MME. The identifier is allocated by the BNG. A fully qualified local TEID-C consists of this identifier and the **GTPC Local IP address** value.
Remote TEID-U	Tunnel endpoint identifier on the eNodeB for the GTP-U user plane tunnel to the BNG. The identifier is allocated by the eNodeB. A fully qualified remote TEID-U consists of this identifier and the **GTPU Tunnel Remote IP address** value.
Remote TEID-C	Tunnel endpoint identifier on the MME for the GTP-C control plane tunnel to the BNG. The identifier is allocated by the MME. A fully qualified remote TEID-C consists of this identifier and the **GTPC Remote IP address** value.
GTPU Tunnel Remote IP address	IP address of the S1-U interface on the eNodeB for the GTP-U tunnel endpoint. A fully qualified remote TEID-U consists of this address and the **Remote TEID-U** value.
GTPU Tunnel Local IP address	IP address of the S1-U interface on the BNG for the GTP-U tunnel endpoint. A fully qualified local TEID-U consists of this address and the **Local TEID-U** value
GTPC Remote IP address	IP address of the S11 interface on the MME for the GTP-C tunnel endpoint. A fully qualified remote TEID-C consists of this address and the **Remote TEID-C** value.
GTPC Local IP address	IP address of the S11 interface on the BNG for the GTP-C tunnel endpoint. A fully qualified local TEID-C consists of this address and the **Local TEID-C** value.

Table 108: show subscribers Output Fields (continued)

Field Name	Field Description
Access Point Name	Access point name (APN) for the user equipment. The APN corresponds to the connection and service parameters that the subscriber's mobile device can use for connecting to the carrier's gateway to the Internet.

Sample Output

show subscribers (IPv4)

```
user@host> show subscribers
Interface               IP Address/VLAN ID   User Name         LS:RI
ge-1/3/0.1073741824     10                                     default:default
demux0.1073741824       203.0.113.10         WHOLESALER-CLIENT default:default
demux0.1073741825       203.0.113.3          RETAILER1-CLIENT  test1:retailer1
demux0.1073741826       203.0.113.3          RETAILER2-CLIENT  test1:retailer2
```

show subscribers (IPv6)

```
user@host> show subscribers
Interface          IP Address/VLAN ID   User Name           LS:RI
ge-1/0/0.0         2001:db8:c0:0:0:0/74    WHOLESALER-CLIENT   default:default
     *             2001:db8:1/128          subscriber-25       default:default
```

show subscribers (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers
Interface           IP Address/VLAN ID         User Name
LS:RI
demux0.1073741834   0x8100.1002 0x8100.1
default:default
demux0.1073741835   0x8100.1001 0x8100.1
default:default
pp0.1073741836      203.0.113.13             dualstackuser1@example1.com
default:ASP-1
*                   2001:db8:1::/48
*                   2001:db8:1:1::/64
pp0.1073741837      203.0.113.33             dualstackuser2@example1.com
default:ASP-1
*                   2001:db8:1:2:5::/64
```

show subscribers (Single Session DHCP Dual Stack)

```
user@host> show subscribers

Interface           IP Address/VLAN ID        User Name               LS:RI
demux0.1073741364   192.168.10.10             dual-stack-retail35     default:default
                    2001:db8::100:0:0:0/74                            default:default
                    2001:db8:3ffe:0:4::/64
```

show subscribers (Single Session DHCP Dual Stack detail)

```
user@host> show subscribers id 27 detail

Type: DHCP
User Name: dual-stack-retail33
IP Address: 10.10.0.53
IPv6 Address: 2001:db8:3000:0:0:8003::2
IPv6 Prefix: 2001:db8:3ffe:0:4::/64
Logical System: default
Routing Instance: default
Interface: ae0.3221225472
Interface type: Static
Underlying Interface: ae0.3221225472
Dynamic Profile Name: dhcp-retail-18
MAC Address: 00:00:5E:00:53:02
State: Active
DHCP Relay IP Address: 10.10.0.1
Radius Accounting ID: 27
Session ID: 27
PFE Flow ID: 2
Stacked VLAN Id: 2000
VLAN Id: 1
Login Time: 2014-05-15 10:12:10 PDT
DHCP Options: len 60
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 00 64 01 01 02
00 06 00 04 00 03 00 19 00 03 00 0c 00 00 00 00 00 00 00 00
00 00 00 00 00 19 00 0c 00 00 00 00 00 00 00 00 00 00 00 00
```

show subscribers (LNS on MX Series Routers)

```
user@host> show subscribers

Interface          IP Address/VLAN ID   User Name         LS:RI
si-4/0/0.1         192.0.2.0          user@example.com   default:default
```

show subscribers (L2TP Switched Tunnels)

```
user@host> show subscribers

Interface           IP Address/VLAN ID    User Name              LS:RI
si-2/1/0.1073741842 Tunnel-switched      user@example.com       default:default

si-2/1/0.1073741843 Tunnel-switched      user@example.com       default:default
```

show subscribers aggregation-interface-set-name

```
user@host> show subscribers aggregation-interface-set-name FRA*

Interface              IP Address/VLAN ID             User Name               LS:RI
ge-1/0/0.3221225472    50                              ancp                   default:isp1-subscriber
```

show subscribers client-type dhcp detail

```
user@host> show subscribers client-type dhcp detail
```

```
Type: DHCP
IP Address: 203.0.113.29
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux
MAC Address: 00:00:5e:00:53:98
State: Active
Radius Accounting ID: user :2304
Login Time: 2009-08-25 14:43:52 PDT

Type: DHCP
IP Address: 203.0.113.27
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744383
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:00:5e:00:53:f3
State: Active
Radius Accounting ID: 1234 :2560
Login Time: 2009-08-25 14:43:56 PDT
```

show subscribers client-type dhcp detail (DHCPv6)

```
user@host> show subscribers client-type dhcp detail
Type: DHCP
User Name: DEFAULTUSER
IPv6 Address: 2001:db8::2
IPv6 Prefix: 2001:db8:1::/64
Logical System: default
Routing Instance: default
Interface: demux0.3221225602
Interface type: Static
Underlying Interface: demux0.3221225602
Dynamic Profile Name: client-profile
MAC Address: 00:00:5E:00:53:01
State: Active
Radius Accounting ID: 142
Session ID: 142
PFE Flow ID: 148
Stacked VLAN Id: 1
VLAN Id: 1
Login Time: 2018-03-29 12:27:38 EDT
DHCP Options: len 56
00 08 00 02 00 00 00 01 00 0e 00 01 00 01 22 4f d0 33 00 11
01 00 00 01 00 03 00 0c 00 00 00 0a 00 04 9d 40 00 07 62 00
00 19 00 0c 00 00 00 0b 00 04 9d 40 00 07 62 00
Server DHCPV6 Options: len 94
00 0a 00 06 11 22 33 44 55 66 00 11 00 09 00 00 0c 4c 00 02
00 01 aa 00 11 00 20 00 00 0a 4c 00 02 00 02 32 33 00 03 00
03 34 35 36 00 05 00 06 31 32 33 34 35 36 00 06 00 01 31 00
11 00 09 00 00 0b 4c 00 02 00 01 bb 00 11 00 12 00 00 0d e9
00 01 00 03 aa bb cc 00 02 00 03 dd ee cc
DHCPV6 Header: len 4
01 fc e4 96
```

show subscribers client-type dhcp extensive

```
user@host> show subscribers client-type dhcp extensive
Type: DHCP
User Name: user
IP Address: 192.0.2.4
IP Netmask: 255.0.0.0
IPv6 Address: 2001:db8:3::103
IPv6 Prefix: 2001:db8::/68
Domain name server inet6: 2001:db8:1 abcd::2
Logical System: default
Routing Instance: default
Interface: ge-0/0/0.0
Interface type: Static
Underlying Interface: ge-0/0/0.0
MAC Address: 00:00:5e:00:53:01
State: Configured
Radius Accounting ID: 10
Session ID: 10
PFE Flow ID: 2
VLAN Id: 100
Agent Circuit ID: ge-0/0/0:100
Agent Remote ID: ge-0/0/0:100
Login Time: 2017-05-23 12:52:22 IST
DHCPV6 Options: len 69
00 01 00 0e 00 01 00 01 59 23 e3 31 00 10 94 00 00 01 00 08
00 02 00 00 00 19 00 29 00 00 00 00 00 04 9d 40 00 07 62 00
00 1a 00 19 00 09 3a 80 00 27 8d 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
Server DHCP Options: len 13
3a 04 00 00 00 ff 00 3b 04 00 00 0f 00
Server DHCPV6 Options: len 8
00 0a 00 04 ab cd ef ab
DHCPV6 Header: len 4
01 00 00 04
IP Address Pool: al_pool30
IPv6 Address Pool: ia_na_pool
IPv6 Delegated Address Pool: prefix_delegate_pool
```

show subscribers client-type fixed-wireless-access

```
user@host> show subscribers client-type fixed-wireless-access

Interface             IP Address/VLAN ID            User Name
LS:RI
ps1.3221225472        192.0.2.10                    505024101215074
default:default
ps1.3221225473        192.0.2.11                    505024101215075
default:default
```

show subscribers client-type fixed-wireless-access detail (Detail)

```
user@host> show subscribers client-type fixed-wireless-access detail
Type: FWA
User Name: 505024101215074
IP Address: 192.0.2.10
IP Netmask: 255.255.0.0
```

```
Interface: ps1.3221225472
Interface type: Dynamic
Dynamic Profile Name: fwa-profile
State: Active
Radius Accounting ID: 1
Session ID: 1
PFE Flow ID: 11
Login Time: 2019-04-10 14:10:12 PDT
Local TEID-U: 1
Local TEID-C: 1
Remote TEID-U: 2000000
Remote TEID-C: 1000000
GTPU Tunnel Remote IP Address: 203.0.113.1.3
GTPU Tunnel Local IP Address: 203.0.113.2.5
GTPC Remote IP Address: 203.0.113.1.2
GTPC Local IP Address: 203.0.113.1.1
Access Point Name: user21
```

show subscribers client-type vlan-oob detail

```
user@host> show subscribers client-type vlan-oob detail
```

```
Type: VLAN-OOB
User Name: L2WS.line-aci-1.line-ari-1
Logical System: default
Routing Instance: ISP1
Interface: demux0.1073744127
Interface type: Dynamic
Underlying Interface: ge-1/0/0
Dynamic Profile Name: Prof_L2WS
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 1234
Session ID: 77
VLAN Id: 126
Core-Facing Interface: ge-2/1/1
VLAN Map Id: 6
Inner VLAN Map Id: 2001
Agent Circuit ID: line-aci-1
Agent Remote ID: line-ari-1
Login Time: 2013-10-29 14:43:52 EDT
```

show subscribers count

```
user@host> show subscribers count
```

```
Total Subscribers: 188, Active Subscribers: 188
```

show subscribers address detail (IPv6)

```
user@host> show subscribers address 203.0.113.137 detail
```

```
Type: PPPoE
User Name: pppoeTerV6User1Svc
IP Address: 203.0.113.137
IP Netmask: 255.0.0.0
IPv6 User Prefix: 2001:db8:0:c88::/32
Logical System: default
Routing Instance: default
```

```
Interface: pp0.1073745151
Interface type: Dynamic
Underlying Interface: demux0.8201
Dynamic Profile Name: pppoe-client-profile
MAC Address: 00:00:5e:00:53:53
Session Timeout (seconds): 31622400
Idle Timeout (seconds): 86400
State: Active
Radius Accounting ID: example demux0.8201:6544
Session ID: 6544
Agent Circuit ID: ifl3720
Agent Remote ID: ifl3720
Login Time: 2012-05-21 13:37:27 PDT
Service Sessions: 1
```

show subscribers detail (IPv4)

```
user@host> show subscribers detail
```

```
Type: DHCP
IP Address: 203.0.113.29
IP Netmask: 255.255.0.0
Primary DNS Address: 192.0.2.0
Secondary DNS Address: 192.0.2.1
Primary WINS Address: 192.0.2.3
Secondary WINS Address: 192.0.2.4
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:00:5e:00:53:98
State: Active
Radius Accounting ID: example :2304
Idle Timeout (seconds): 600
Login Time: 2009-08-25 14:43:52 PDT
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
33 2d 37 2d 30 37 05 01 06 0f 21 2c
Service Sessions: 2
```

show subscribers detail (IPv6)

```
user@host> show subscribers detail
```

```
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2001:db8:ffff:1::/32
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:00:5e:00:53:03
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
```

```
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

show subscribers detail (pseudowire Interface for GRE Tunnel)

```
user@host> show subscribers detail
Interface           IP Address/VLAN ID        User Name           LS:RI
ps0.3221225484      192.0.2.2
ps0.3221225485      192.0.2.3
demux0.3221225486    1                                          default:default

demux0.3221225487    1                                          default:default

demux0.3221225488   198.51.0.1                                  default:default

demux0.3221225489   198.51.0.2                                  default:default
```

show subscribers detail (IPv6 Static Demux Interface)

```
user@host> show subscribers detail
Type: STATIC-INTERFACE
User Name: user@example.com
IPv6 Prefix: 2001:db8:3:4:5:6:7:aa/32
Logical System: default
Routing Instance: default
Interface: demux0.1
Interface type: Static
Dynamic Profile Name: junos-default-profile
State: Active
Radius Accounting ID: 185
Login Time: 2010-05-18 14:33:56 EDT
```

show subscribers detail (L2TP LNS Subscribers on MX Series Routers)

```
user@host> show subscribers detail
Type: L2TP
User Name: user@example.com
IP Address: 203.0.113.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
```

show subscribers detail (L2TP Switched Tunnels)

```
user@host> show subscribers detail
```

```
Type: L2TP
User Name: user@example.com
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741842
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 203.0.113.51
Remote IP Address: 192.0.2.0
Radius Accounting ID: 21
Session ID: 21
Login Time: 2013-01-18 03:01:11 PST

Type: L2TP
User Name: user@example.com
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741843
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 203.0.113.31
Remote IP Address: 192.0.2.1
Session ID: 22
Login Time: 2013-01-18 03:01:14 PST
```

show subscribers detail (Tunneled Subscriber)

```
user@host> show subscribers detail
```

```
Type: PPPoE
User Name: user1@example.com
Logical System: default
Routing Instance: default
Interface: pp0.1
State: Active, Tunneled
Radius Accounting ID: 512
```

show subscribers detail (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers detail
```

```
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST
```

```
Type: PPPoE
User Name: dualstackuser1@example1.com
IP Address: 203.0.113.13
IPv6 Prefix: 2001:db8:1::/32
IPv6 User Prefix: 2001:db8:1:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST

Type: DHCP
IPv6 Prefix: 2001:db8:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: test :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

show subscribers detail (ACI Interface Set Session)

```
user@host> show subscribers detail
```

```
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0
Interface Set: aci-1001-ge-1/0/0.2800
Interface Set Session ID: 0
Underlying Interface: ge-1/0/0.2800
Dynamic Profile Name: aci-vlan-set-profile-2
Dynamic Profile Version: 1
State: Active
Session ID: 1
Agent Circuit ID: aci-ppp-dhcp-20
Login Time: 2012-05-26 01:54:08 PDT
```

show subscribers detail (PPPoE Subscriber Session with ACI Interface Set)

```
user@host> show subscribers detail
```

```
Type: PPPoE
User Name: ppphint2
IP Address: 203.0.113.15
```

```
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Interface Set: aci-1001-demux0.1073741824
Interface Set Type: Dynamic
Interface Set Session ID: 2
Underlying Interface: demux0.1073741824
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: 3
Session ID: 3
Agent Circuit ID: aci-ppp-dhcp-dvlan-50
Login Time: 2012-03-07 13:46:53 PST
```

show subscribers extensive

```
user@host> show subscribers extensive
```

```
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2001:db8:ffff:1::/32
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:00:5e:00:53:03
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Address Pool: pd_pool
IPv6 Network Prefix Length: 48
```

show subscribers extensive (Aggregation Node Interface Set and DSL Forum Attributes)

```
user@host> show subscribers extensive
```

```
Type: VLAN-OOB
User Name: ancp
Logical System: default
Routing Instance: isp1-subscriber
Interface: ge-1/0/0.3221225472
Interface type: Dynamic
Interface Set: FRA-DPU-C-100
Underlying Interface: ge-1/0/0
Core IFL Name: ge-1/0/4.0
Dynamic Profile Name: Prof_L2BSA
State: Active
Radius Accounting ID: 1
Session ID: 1
PFE Flow ID: 13
VLAN Id: 50
```

```
VLAN Map Id: 20
Inner VLAN Map Id: 1
Inner VLAN Tag Protocol Id: 0x88a8
Agent Circuit ID: circuit 201
Agent Remote ID: remote-id
Aggregation Interface-set Name: FRA-DPU-C-100
Login Time: 2018-05-29 08:43:42 EDT
Accounting interval: 72000
Dynamic configuration:
  junos-cos-scheduler-map: 100m
  junos-inner-vlan-tag-protocol-id: 0x88a8
  junos-vlan-map-id: 20

Type: PPPoE
IP Address: 192.85.128.1
IP Netmask: 255.255.255.255
Logical System: default
Routing Instance: default
Interface: pp0.3221225474
Interface type: Dynamic
Interface Set: ge-1/0/0
Underlying Interface: demux0.3221225473
Dynamic Profile Name: pppoe-client-profile-with-cos
MAC Address: 00:10:94:00:00:03
State: Active
Radius Accounting ID: 3
Session ID: 3
PFE Flow ID: 16
Stacked VLAN Id: 50
VLAN Id: 7
Agent Circuit ID: circuit 201
Agent Remote ID: remote-id
Aggregation Interface-set Name: FRA-DPU-C-100
Login Time: 2018-05-29 08:43:45 EDT
IP Address Pool: pool-1
Accounting interval: 72000
DSL type: G.fast
Frame/cell mode: Frame
Overhead accounting bytes: 10
Actual upstream data rate: 100000 kbps
Actual downstream data rate: 200000 kbps
Calculated downstream data rate: 180000 kbps
Calculated upstream data rate: 90000 kbps
Adjusted upstream data rate: 80000 kbps
Adjusted downstream data rate: 160000 kbps
DSL Line Attributes
  Agent Circuit ID: circuit 201
  Agent Remote ID: remote-id
  Actual upstream data rate: 100000
  Actual downstream data rate: 200000
  DSL type: G.fast
  Access Aggregation Circuit ID: #FRA-DPU-C-100
  Attribute type: 0xAA, Attribute length: 4
    198 51 100 78
```

show subscribers extensive (Passive Optical Network Circuit Interface Set)

```
user@host> show subscribers client-type dhcp extensive
```

```
Type: DHCP
IP Address: 192.0.2.136
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073741842
Interface type: Dynamic
Interface Set: otl01.xyz101-202
Underlying Interface: demux0.1073741841
Dynamic Profile Name: dhcp-profile
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: user :19
Session ID: 19
VLAN Id: 1100
Agent Remote ID: ABCD01234|100M|AAAA01234|otl01.xyz101-202

Login Time: 2017-03-29 10:30:46 PDT
DHCP Options: len 97
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 02 33 04 00 00
17 70 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 32 2f
32 2d 31 2d 31 37 05 01 06 0f 21 2c 52 2b 02 29 41 42 43 44
30 31 32 33 34 7c 31 30 30 4d 7c 41 41 41 41 30 31 32 33 34
7c 6f 74 6c 30 31 2e 78 79 7a 31 30 31 2d 32 30 32
IP Address Pool: POOL-V4
```

show subscribers extensive (DNS Addresses from Access Profile or Global Configuration)

```
user@host> show subscribers extensive
```

```
Type: DHCP
User Name: test-user@example-com
IP Address: 192.0.2.119
IP Netmask: 255.255.255.255
Domain name server inet: 198.51.100.1 198.51.100.2
IPv6 Address: 2001:db8::1:11
Domain name server inet6: 2001:db8:5001::12 2001:db8:3001::12
Logical System: default
Routing Instance: default
Interface: ge-2/0/3.0
Interface type: Static
Underlying Interface: ge-2/0/3.0
MAC Address: 00:00:5E:00:53:00
State: Active
Radius Accounting ID: 5
Session ID: 5
Login Time: 2017-01-31 11:16:21 IST
DHCP Options: len 53
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 03 33 04 00 00
00 3c 0c 16 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 35 2f
31 32 2d 30 2d 30 37 05 01 06 0f 21 2c
IP Address Pool: v4-pool
```

show subscribers extensive (DNS Addresses from RADIUS)

```
user@host> show subscribers extensive
```

```
Type: DHCP
User Name: test-user@example-com
```

```
IP Address: 192.0.2.119
IP Netmask: 255.255.255.255
Primary DNS Address: 198.51.100.1
Secondary DNS Address: 198.51.100.2
IPv6 Address: 2001:db8::1:11
IPv6 Primary DNS Address: 2001:db8:5001::12
IPv6 Secondary DNS Address: 2001:db8:3001::12
Logical System: default
Routing Instance: default
Interface: ge-2/0/3.0
Interface type: Static
Underlying Interface: ge-2/0/3.0
MAC Address: 00:00:5E:00:53:00
State: Active
Radius Accounting ID: 5
Session ID: 5
Login Time: 2017-01-31 11:16:21 IST
DHCP Options: len 53
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 03 33 04 00 00
00 3c 0c 16 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 35 2f
31 32 2d 30 2d 30 37 05 01 06 0f 21 2c
IP Address Pool: v4-pool
```

show subscribers extensive (IPv4 DNS Addresses from RADIUS, IPv6 from Access Profile or Global Configuration)

```
user@host> show subscribers extensive
```

```
Type: DHCP
User Name: test-user@example-com
IP Address: 192.0.2.119
IP Netmask: 255.255.255.255
Primary DNS Address: 198.51.100.1
Secondary DNS Address: 198.51.100.2
IPv6 Address: 2001:db8::1:11
Domain name server inet6: 2001:db8:5001::12 2001:db8:3001::12
Logical System: default
Routing Instance: default
Interface: ge-2/0/3.0
Interface type: Static
Underlying Interface: ge-2/0/3.0
MAC Address: 00:00:5E:00:53:00
State: Active
Radius Accounting ID: 5
Session ID: 5
Login Time: 2017-01-31 11:16:21 IST
DHCP Options: len 53
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 03 33 04 00 00
00 3c 0c 16 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 35 2f
31 32 2d 30 2d 30 37 05 01 06 0f 21 2c
IP Address Pool: v4-pool
```

show subscribers extensive (RPF Check Fail Filter)

```
user@host> show subscribers extensive
```

```
...
Type: VLAN
  Logical System: default
  Routing Instance: default
```

```
  Interface: ae0.1073741824
  Interface type: Dynamic
  Dynamic Profile Name: vlan-prof
  State: Active
  Session ID: 9
  VLAN Id: 100
  Login Time: 2011-08-26 08:17:00 PDT
  IPv4 rpf-check Fail Filter Name: rpf-allow-dhcp
  IPv6 rpf-check Fail Filter Name: rpf-allow-dhcpv6
...
```

show subscribers extensive (L2TP LNS Subscribers on MX Series Routers)

```
user@host> show subscribers extensive
```

```
Type: L2TP
User Name: user@example.com
IP Address: 203.0.113.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
IPv4 Input Filter Name: classify-si-5/2/0.1073749824-in
IPv4 Output Filter Name: classify-si-5/2/0.1073749824-out
```

show subscribers extensive (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers extensive
```

```
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@example1.com
IP Address: 203.0.113.13
IPv6 Prefix: 2001:db8:1::/32
IPv6 User Prefix: 2001:db8:1:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:5e:00:53:02
```

```
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST
IPv6 Delegated Network Prefix Length: 48
IPv6 Interface Address: 2001:db8:2016:1:1::1/64
IPv6 Framed Interface Id: 1:1:2:2
IPv4 Input Filter Name: FILTER-IN-pp0.1073741825-in
IPv4 Output Filter Name: FILTER-OUT-pp0.1073741825-out
IPv6 Input Filter Name: FILTER-IN6-pp0.1073741825-in
IPv6 Output Filter Name: FILTER-OUT6-pp0.1073741825-out

Type: DHCP
IPv6 Prefix: 2001:db8:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: test :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Delegated Network Prefix Length: 48
```

show subscribers extensive (ADF Rules)

```
user@host> show subscribers extensive
```

```
...
   Service Session ID: 12
   Service Session Name: SERVICE-PROFILE
   State: Active
   Family: inet
     ADF IPv4 Input Filter Name: __junos_adf_12-demux0.3221225474-inet-in
                       Rule 0: 010101000b0101020b020200201811
                               from {
                                   source-address 203.0.113.232;
                                   destination-address 198.51.100.0/24;
                                   protocol 17;
                               }
                               then {
                                   accept;
                               }
```

show subscribers extensive (Effective Shaping-Rate)

```
user@host> show subscribers extensive
```

```
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741837
```

```
Interface type: Dynamic
Interface Set: ifset-1
Underlying Interface: ae1
Dynamic Profile Name: svlan-dhcp-test
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.201
VLAN Id: 0x8100.201
Login Time: 2011-11-30 00:18:04 PST
Effective shaping-rate: 31000000k
...
```

show subscribers extensive (PPPoE Subscriber Access Line Rates

```
user@host> show subscribers extensive
```

```
Type: PPPoE
 IP Address: 198.51.100.1
 IP Netmask: 255.255.255.255
 Logical System: default
 Routing Instance: default
 Interface: pp0.3221225475
 Interface type: Dynamic
 Underlying Interface: demux0.3221225474
 Dynamic Profile Name: pppoe-client-profile-with-cos
 MAC Address: 00:00:5e:00:53:02
 State: Active
 Radius Accounting ID: 4
 Session ID: 4
 PFE Flow ID: 14
 Stacked VLAN Id: 40
 VLAN Id: 1
 Agent Circuit ID: circuit0
 Agent Remote ID: remote0
 Login Time: 2017-04-06 15:52:32 PDT

 User Name: DAVE-L2BSA-SERVICE
 Logical System: default
 Routing Instance: isp-1-subscriber
 Interface: ge-1/2/4.3221225472
 Interface type: Dynamic
 Interface Set: ge-1/2/4
 Underlying Interface: ge-1/2/4
 Core IFL Name: ge-1/3/4.0
 Dynamic Profile Name: L2BSA-88a8-400LL1300VO
 State: Active
Radius Accounting ID: 1
 Session ID: 1
 PFE Flow ID: 14
 VLAN Id: 13
 VLAN Map Id: 102
 Inner VLAN Map Id: 1
 Agent Circuit ID: circuit-aci-3
 Agent Remote ID: remote49-3
 Login Time: 2017-04-05 16:59:29 EDT
 Service Sessions: 4
 IFL Input Filter Name: L2BSA-CP-400LL1300VO-ge-1/2/4.3221225472-in
 IFL Output Filter Name: L2BSA-CP-400LL1300VO-ge-1/2/4.3221225472-out
 Accounting interval: 900
 DSL type: VDSL
```

```
Frame/Cell Mode: Frame
Overhead accounting bytes: -10
Actual upstream data rate: 1024 kbps
Actual downstream data rate: 4096 kbps
Adjusted downstream data rate: 3686 kbps
Adjusted upstream data rate: 922 kbps
Dynamic configuration:
  junos-vlan-map-id: 102
  Service Session ID: 5
  Service Session Name: SRL-L1
  State: Active
  Family: inet, inet6
  IFL Input Filter Name: L2BSA-FWF-in-10048-ge-1/2/4.3221225472-in
  IFL Output Filter Name: L2BSA-FWF-out-25088-ge-1/2/4.3221225472-out
  Service Activation time: 2017-04-05 16:59:30 EDT
  Dynamic configuration:
    l2bsa-fwf-in: L2BSA-FWF-in-10048
    l2bsa-fwf-out: L2BSA-FWF-out-25088
    rldown: 25088
    rlup: 10048
```

show subscribers extensive (Subscriber Session Using PCEF Profile)

```
user@host> show subscribers extensive
```

```
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225517
Interface type: Dynamic
Underlying Interface: ge-1/0/3
Dynamic Profile Name: svlan-dhcp
State: Active
Session ID: 59
PFE Flow ID: 71
Stacked VLAN Id: 0x8100.1
VLAN Id: 0x8100.2
Login Time: 2017-03-28 08:23:08 PDT

Type: DHCP
User Name: pcefuser
IP Address: 192.0.2.26
IP Netmask: 255.0.0.0
Logical System: default
Routing Instance: default
Interface: demux0.3221225518
Interface type: Dynamic
Underlying Interface: demux0.3221225517
Dynamic Profile Name: dhcp-client-prof
MAC Address: 00:00:5e:00:53:01
State: Active
Radius Accounting ID: 60
Session ID: 60
PFE Flow ID: 73
Stacked VLAN Id: 1
VLAN Id: 2
Login Time: 2017-03-28 08:23:08 PDT
Service Sessions: 1
DHCP Options: len 9
35 01 01 37 04 01 03 3a 3b
```

```
IP Address Pool: pool-ipv4
IPv4 Input Service Set: tdf-service-set
IPv4 Output Service Set: tdf-service-set
PCEF Profile: pcef-prof-1
PCEF Rule/Rulebase: default
Dynamic configuration:
  junos-input-service-filter: svc-filt-1
  junos-input-service-set: tdf-service-set
  junos-output-service-filter: svc-filt-1
  junos-output-service-set: tdf-service-set
  junos-pcef-profile: pcef-prof-1
  junos-pcef-rule: default

   Service Session ID: 61
   Service Session Name: pcef-serv-prof
   State: Active
   Family: inet
   IPv4 Input Service Set: tdf-service-set
   IPv4 Output Service Set: tdf-service-set
   PCEF Profile: pcef-prof-1
   PCEF Rule/Rulebase: limit-fb
   Service Activation time: 2017-03-28 08:31:19 PDT
   Dynamic configuration:
     pcef-prof: pcef-prof-1
     pcef-rule1: limit-fb
     svc-filt: svc-filt-1
     svc-set: tdf-service-set
```

show subscribers aci-interface-set-name detail (Subscriber Sessions Using Specified ACI Interface Set)

```
user@host> show subscribers aci-interface-set-name aci-1003-ge-1/0/0.4001 detail
```

```
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 203.0.113.17
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address:
State: Active
Radius Accounting ID: 14
```

```
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT
```

show subscribers agent-circuit-identifier detail (Subscriber Sessions Using Specified ACI Substring)

```
user@host> show subscribers agent-circuit-identifier aci-ppp-vlan detail
```

```
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 203.0.113.17
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:5e:00:53:52
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT
```

show subscribers id accounting-statistics

```
user@host> show subscribers id 601 accounting-statistics
```

```
Session ID: 601
Accounting Statistics:
Input bytes : 199994
Output bytes : 121034
Input packets: 5263
Output packets: 5263
IPv6:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
```

show subscribers interface accounting-statistics

```
user@host> show subscribers interface pp0.3221226949 accounting-statistics
```

```
Session ID: 501
Accounting Statistics:
Input bytes : 199994
Output bytes : 121034
Input packets: 5263
Output packets: 5263
IPv6:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Session ID: 502
Accounting Statistics:
Input bytes : 87654
Output bytes : 72108
Input packets: 3322
Output packets: 3322
IPv6:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Session ID: 503
Accounting Statistics:
Input bytes : 156528
Output bytes : 123865
Input packets: 7448
Output packets: 7448
IPv6:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
```

show subscribers interface extensive

user@host> **show subscribers interface demux0.1073741826 extensive**

```
Type: VLAN
User Name: user@test.example.com
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Dynamic
Dynamic Profile Name: profile-vdemux-relay-23qos
MAC Address: 00:00:5e:00:53:04
State: Active
Radius Accounting ID: 12
Session ID: 12
Stacked VLAN Id: 0x8100.1500
VLAN Id: 0x8100.2902
Login Time: 2011-10-20 16:21:59 EST

Type: DHCP
User Name: user@test.example.com
IP Address: 192.0.2.0
IP Netmask: 255.255.255.0
Logical System: default
```

```
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Static
MAC Address: 00:00:5e:00:53:04
State: Active
Radius Accounting ID: 21
Session ID: 21
Login Time: 2011-10-20 16:24:33 EST
Service Sessions: 2

Service Session ID: 25
Service Session Name: SUB-QOS
State: Active

Service Session ID: 26
Service Session Name: service-cb-content
State: Active
IPv4 Input Filter Name: content-cb-in-demux0.1073741826-in
IPv4 Output Filter Name: content-cb-out-demux0.1073741826-out
```

show subscribers logical-system terse

```
user@host> show subscribers logical-system test1 terse
```

```
Interface           IP Address/VLAN ID   User Name         LS:RI
demux0.1073741825     203.0.113.3         RETAILER1-CLIENT  test1:retailer1
demux0.1073741826     203.0.113.4         RETAILER2-CLIENT  test1:retailer2
```

show subscribers physical-interface count

```
user@host> show subscribers physical-interface ge-1/0/0 count
```

```
Total subscribers: 3998, Active Subscribers: 3998
```

show subscribers routing-instance inst1 count

```
user@host> show subscribers routing-instance inst1 count
```

```
Total Subscribers: 188, Active Subscribers: 183
```

show subscribers stacked-vlan-id detail

```
user@host> show subscribers stacked-vlan-id 101 detail
```

```
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id detail (Combined Output)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 detail
```

```
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id interface detail (Combined Output for a Specific Interface)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 interface ge-1/2/0.* detail
```

```
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers user-name detail

```
user@host> show subscribers user-name larry1 detail
```

```
Type: DHCP
User Name: larry1
IP Address: 203.0.113.37
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.1
Interface type: Static
Dynamic Profile Name: foo
MAC Address: 00:00:5e:00:53:01
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-11-07 08:25:59 PST
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 01 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 32 2f
37 2d 30 2d 30 37 05 01 06 0f 21 2c
```

show subscribers vlan-id

```
user@host> show subscribers vlan-id 100
```

```
Interface           IP Address                              User Name
ge-1/0/0.1073741824
ge-1/2/0.1073741825
```

show subscribers vlan-id detail

```
user@host> show subscribers vlan-id 100 detail
```

```
Type: VLAN
Interface: ge-1/0/0.1073741824
```

```
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT

Type: VLAN
Interface: ge-1/2/0.1073741825
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT
```

show subscribers vpi vci extensive (PPPoE-over-ATM Subscriber Session)

```
user@host> show subscribers vpi 40 vci 50 extensive
```

```
Type: PPPoE
User Name: testuser
IP Address: 203.0.113.2
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: pp0.0
Interface type: Static
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: 2
Session ID: 2
ATM VPI: 40
ATM VCI: 50
Login Time: 2012-12-03 07:49:26 PST
IP Address Pool: pool_1
IPv6 Framed Interface Id: 200:65ff:fe23:102
```

show subscribers address detail (Enhanced Subscriber Management)

```
user@host> show subscribers address 203.0.113.111 detail
```

```
Type: DHCP
User Name: simple_filters_service
IP Address: 203.0.113.111
IP Netmask: 255.0.0.0
Logical System: default
Routing Instance: default
Interface: demux0.3221225482
Interface type: Dynamic
Underlying Interface: demux0.3221225472
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:00:5e:00:53:0f
State: Active
Radius Accounting ID: 11
Session ID: 11
PFE Flow ID: 15
Stacked VLAN Id: 210
VLAN Id: 209
Login Time: 2014-03-24 12:53:48 PDT
Service Sessions: 1
```

```
DHCP Options: len 3
35 01 01
```

show system autorecovery state

Syntax show system autorecovery state

Release Information Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Description Perform checks and show status of all autorecovered items.

Required Privilege Level view

Related Documentation
- request system autorecovery state on page 1692

List of Sample Output show system autorecovery state on page 1962

Output Fields Table 109 on page 1962 lists the output fields for the **show system autorecovery state** command. Output fields are listed in the approximate order in which they appear.

Table 109: show system autorecovery state Output Fields

Field Name	Field Description
File	The name of the file on which autorecovery checks are performed.
Slice	The disk partition on which autorecovery checks are performed.
Recovery Information	Indicates whether autorecovery information for the file or slice has been saved.
Integrity Check	Displays the status of the file's integrity check (passed or failed).
Action / Status	Displays the status of the item, or the action required to be taken for that item.

Sample Output

show system autorecovery state

```
user@host> show system autorecovery state

Configuration:
File            Recovery Information    Integrity Check    Action / Status
rescue.conf.gz  Saved                   Passed             None
Licenses:
File            Recovery Information    Integrity Check    Action / Status
JUNOS282736.lic Saved                   Passed             None
JUNOS282737.lic Not Saved               Not checked        Requires save
BSD Labels:
Slice           Recovery Information    Integrity Check    Action / Status
```

```
s1              Saved           Passed          None
s2              Saved           Passed          None
s3              Saved           Passed          None
s4              Saved           Passed          None
```

show system license (View)

Syntax

```
show system license
<installed | keys | status | usage>
```

Release Information Command introduced in Junos OS Release 9.5. Logical system status option added in Junos OS Release 11.2.

Description Display licenses and information about how licenses are used.

Options

none—Display all license information.

installed—(Optional) Display installed licenses only.

keys—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.

status—(Optional) Display license status for a specified logical system or for all logical systems.

usage—(Optional) Display the state of licensed features.

Required Privilege Level view

Related Documentation

- *Adding New Licenses (CLI Procedure)*

List of Sample Output

show system license on page 1965
show system license installed on page 1965
show system license keys on page 1966
show system license usage on page 1966
show system license status logical-system all on page 1966

Output Fields Table 110 on page 1964 lists the output fields for the **show system license** command. Output fields are listed in the approximate order in which they appear.

Table 110: show system license Output Fields

Field Name	Field Description
Feature name	Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present.
Licenses used	Number of licenses used by the device. You use this information to verify that the number of licenses used matches the number configured. If a licensed feature is configured, the feature is considered used.

Table 110: show system license Output Fields (continued)

Field Name	Field Description
Licenses installed	Information about the installed license key: • **License identifier**—Identifier associated with a license key. • **License version**—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key. • **Valid for device**—Device that can use a license key. • **Features**—Feature associated with a license.
Licenses needed	Number of licenses required for features being used but not yet properly licensed.
Expiry	Time remaining in the grace period before a license is required for a feature being used.
Logical system license status	Displays whether a license is enabled for a logical system.

Sample Output

show system license

```
user@host> show system license

License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  av_key_kaspersky_engine               1            1           0    2012-03-30
 01:00:00 IST
  wf_key_surfcontrol_cpa                0            1           0    2012-03-30
 01:00:00 IST
  dynamic-vpn                           0            1           0    permanent
  ax411-wlan-ap                         0            2           0    permanent

Licenses installed:
  License identifier: JUNOS301998
  License version: 2
  Valid for device: AG4909AA0080
  Features:
    av_key_kaspersky_engine - Kaspersky AV
      date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST

  License identifier: JUNOS302000
  License version: 2
  Valid for device: AG4909AA0080
  Features:
    wf_key_surfcontrol_cpa - Web Filtering
      date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

show system license installed

```
user@host> show system license installed

License identifier: JUNOS301998
```

```
  License version: 2
  Valid for device: AG4909AA0080
  Features:
    av_key_kaspersky_engine - Kaspersky AV
      date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST

  License identifier: JUNOS302000
  License version: 2
  Valid for device: AG4909AA0080
  Features:
    wf_key_surfcontrol_cpa - Web Filtering
      date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

show system license keys

```
user@host> show system license keys

XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
         xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
         xxxxxx xxxxxx xxx
```

show system license usage

```
user@host> show system license usage

                                 Licenses     Licenses    Licenses  Expiry
Feature name                        used     installed      needed
  av_key_kaspersky_engine              1           1           0    2012-03-30
 01:00:00 IST
  wf_key_surfcontrol_cpa               0           1           0    2012-03-30
 01:00:00 IST
  dynamic-vpn                          0           1           0    permanent
  ax411-wlan-ap                        0           2           0    permanent
```

show system license status logical-system all

```
user@host> show system license status logical-system all
Logical system license status:

logical system name                 license status
root-logical-system                 enabled
LSYS0                               enabled
LSYS1                               enabled
LSYS2                               enabled
```

show system login lockout

Syntax show system login lockout

Release Information Command introduced in Junos OS Release 11.2.

Description Display the usernames locked after unsuccessful login attempts.

Required Privilege Level view and system

Related Documentation
- lockout-period on page 1208
- clear system login lockout on page 1669

List of Sample Output show system login lockout on page 1967

Output Fields Table 111 on page 1967 lists the output fields for the **show system login lockout** command. Output fields are listed in the approximate order in which they appear.

Table 111: show system login lockout

Field Name	Field Description	Level of Output
User	Username	All levels
Lockout start	Date and time the username was locked	All levels
Lockout end	Date and time the username was unlocked	All levels

Sample Output

show system login lockout

```
user@host> show system login lockout

User                 Lockout start           Lockout end
root                 2011-05-11 09:11:15 UTC 2011-05-11 09:13:15 UTC
```

show system download

Syntax show system download <*download-id*>

Release Information Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Description Display a brief summary of all the download instances along with their current state and extent of progress. If a **download-id** is provided, the command displays a detailed report of the particular download instance.

Options
- **download-id**—(Optional) The ID number of the download instance.

Required Privilege Level view

Related Documentation
- request system download start on page 1699

List of Sample Output show system download on page 1968
show system download 1 on page 1969

Output Fields Table 112 on page 1968 lists the output fields for the **show system download** command. Output fields are listed in the approximate order in which they appear.

Table 112: show system download Output Fields

Field Name	Field Description
ID	Displays the download identification number.
Status	Displays the state of a particular download.
Start Time	Displays the start time of a particular download.
Progress	Displays the percentage of a download that has been completed.
URL	Displays the URL from which the file was downloaded.

Sample Output

show system download

```
user@host> show system download
Download Status Information:
ID  Status      Start Time       Progress  URL
```

```
1   Active      May 4 06:28:36   5%         ftp://ftp-server//tftpboot/1m_file
2   Active      May 4 06:29:07   3%         ftp://ftp-server//tftpboot/5m_file
3   Error       May 4 06:29:22   Unknown    ftp://ftp-server//tftpboot/badfile
4   Completed   May 4 06:29:40   100%       ftp://ftp-server//tftpboot/smallfile
```

show system download 1

```
user@host> show system download 1

Download ID     : 1
Status          : Active
Progress        : 6%
URL             : ftp://ftp-server//tftpboot/1m_file
Local Path      : /var/tmp/1m_file
Maximum Rate    : 1k
Creation Time   : May 4 06:28:36
Scheduled Time  : May 4 06:28:36
Start Time      : May 4 06:28:37
Error Count     : 0
```

show system services dhcp binding

Syntax

```
show system services dhcp binding
<detail>
<address>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

(EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server client binding information.

Options

none—Display brief information about all active client bindings.

detail—(Optional) Display detailed information about all active client bindings.

address—(Optional) Display detailed client binding information for the specified IP address only.

Required Privilege Level

view and system

Related Documentation

- clear system services dhcp binding on page 1670

List of Sample Output

show system services dhcp binding on page 1971
show system services dhcp binding address on page 1971
show system services dhcp binding address detail on page 1971

Output Fields

Table 113 on page 1970 describes the output fields for the **show system services dhcp binding** command. Output fields are listed in the approximate order in which they appear.

Table 113: show system services dhcp binding Output Fields

Field Name	Field Description	Level of Output
Allocated address	List of IP addresses the DHCP server has assigned to clients.	All levels
MAC address	Corresponding media access control (MAC) hardware address of the client.	All levels
Client identifier	(***address*** option only) Client's unique identifier (represented by an ASCII string or hexadecimal digits). This identifier is used by the DHCP server to index its database of address bindings.	All levels
Binding Type	Type of binding assigned to the client. DHCP servers can assign a dynamic binding from a pool of IP addresses or a static binding to one or more specific IP addresses.	All levels
Lease Expires at	Time the lease expires or **never** for leases that do not expire.	All levels

Table 113: show system services dhcp binding Output Fields (continued)

Field Name	Field Description	Level of Output
Lease Obtained at	(***address*** option only) Time the client obtained the lease from the DHCP server.	**detail**
State	Status of the binding. Bindings can be active or expired.	**detail**
Pool	Address pool that contains the IP address assigned to the client.	**detail**
Request received on	Interface on which the DHCP message exchange occurs. The IP address pool is configured based on the interface's IP address. If a relay agent is used, its IP address is also displayed.	**detail**
DHCP options	User-defined options created for the DHCP server. If no options have been defined, this field is blank.	**detail**

Sample Output

show system services dhcp binding

```
user@host> show system services dhcp binding

Allocated address   MAC address        Binding Type   Lease expires at
192.168.1.2         00:a0:12:00:12:ab  static         never
192.168.1.3         00:a0:12:00:13:02  dynamic        2004-05-03 13:01:42 PDT
```

show system services dhcp binding address

```
user@host> show system services dhcp binding 192.168.1.3

DHCP binding information:
Allocated address: 192.168.1.3
Mac address: 00:a0:12:00:12:ab
Client identifier
61 63 65 64 2d 30 30 3a 61 30 3a 31 32 3a 30 30aced-00:a0:12:00
3a 31 33 3a 30 32:13:02

Lease information:
    Binding Type dynamic
    Obtained at 2004-05-02 13:01:42 PDT
    Expires at 2004-05-03 13:01:42 PDT
```

show system services dhcp binding address detail

```
user@host> show system services dhcp binding 192.168.1.3 detail

DHCP binding information:
Allocated address        192.168.1.3
MAC address  00:a0:12:00:12:ab
    Pool              192.168.1.0/24
Request received on fe-0/0/0, relayed by 192.168.4.254

Lease information:
```

```
    Type              DHCP
    Obtained at       2004-05-02 13:01:42 PDT
    Expires at        2004-05-03 13:01:42 PDT
State active

DHCP options:
    Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
    Name: domain-name, Value: mydomain.tld
    Code: 19, Type: flag, Value: off
    Code: 40, Type: string, Value: domain.tld
    Code: 32, Type: ip-address, Value: 3.3.3.33
```

show system services dhcp client

Syntax

```
show system services dhcp client
< interface-name >
<statistics>
```

Release Information

Command introduced in Junos OS Release 8.5.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display information about DHCP clients.

Options

- none—Display DHCP information for all interfaces.
- ***interface-name***—(Optional) Display DHCP information for the specified interface.
- **statistics**—(Optional) Display DHCP client statistics.

Required Privilege Level

view and system

Related Documentation

- *dhcp (Interfaces)*
- request system services dhcp on page 1715

List of Sample Output

show system services dhcp client on page 1974
show system services dhcp client ge-0/0/34.0 on page 1975
show system services dhcp client statistics on page 1975

Output Fields

Table 114 on page 1973 lists the output fields for the **show system services dhcp client** command. Output fields are listed in the approximate order in which they appear.

Table 114: show system services dhcp client Output Fields

Field Name	Field Description
Logical Interface Name	Name of the logical interface.
Client Status	State of the client binding.
Vendor Identifier	Vendor ID.
Server Address	IP address of the DHCP server.
Address obtained	IP address obtained from the DHCP server.
Lease Obtained at	Date and time the lease was obtained.
Lease Expires in	(EX Series switches only) Time the current lease expires in (seconds).

Table 114: show system services dhcp client Output Fields (continued)

Field Name	Field Description
Lease Expires at	Date and time the lease expires.
DHCP Options	• **Name: server-identifier**, **Value:** IP address of the name server. • **Name: device**, **Value:** IP address of the name device. • **Name: domain-name**, **Value:** Name of the domain.
Packets dropped	**Total** packets dropped.
Messages received	**Number of the following DHCP messages received:** • **DHCPOFFER**—First packet received on a logical interface when DHCP is enabled. • **DHCPACK**—When received from the server, the client sends an ARP request for that address and adds a (ARP response) timer for 4 seconds and stops the earlier timer added for DHCPACK. • **DHCPNAK**—When a DHCPNAK is received instead of DHCPACK, the logical interface sends a DHCPDISCOVER packet.
Messages sent	**Number of the following DHCP messages sent:** • **DHCPDECLINE**—Packet sent when ARP response is received and there is a conflict. The logical interface sends a new DHCPDISCOVER packet. • **DHCPDISCOVER**—Packet sent on the interface for which the DHCP client is enabled. • **DHCPREQUEST**—Packet sent to the DHCP server after accepting the DHCPOFFER. After sending the DHCPREQUEST, the device adds a retransmission-interval timer. • **DHCPINFORM**—Packet sent to the DHCP server for local configuration parameters. • **DHCPRELEASE**—Packet sent to the DHCP server to relinquish network address and cancel remaining lease. • **DHCPRENEW**—Packet sent to the DHCP server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be unicast directly to the server. • **DHCPREBIND**—Packet sent to any server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be broadcast.

Sample Output

show system services dhcp client

```
user@host> show system services dhcp client
Logical Interface name         ge-0/0/34.0
        Hardware address        00:1f:12:38:5f:e5
        Client status           bound
        Address obtained        10.0.0.2
        Update server           disabled
        Lease obtained at       2013-12-23 08:11:40 UTC
        Lease expires in        93
        Lease expires at        2013-12-23 08:13:20 UTC

DHCP options:
    Name: server-identifier, Value: 10.0.0.1
    Code: 1, Type: ip-address, Value: 255.255.255.0
```

Sample Output

show system services dhcp client ge-0/0/34.0

```
user@host> show system services dhcp client ge-0/0/34.0
Logical Interface name         ge-0/0/34.0
       Hardware address        00:1f:12:38:5f:e5
       Client status           bound
       Address obtained        10.0.0.2
       Update server           disabled
       Lease obtained at       2013-12-23 08:11:40 UTC
       Lease expires in        87
       Lease expires at        2013-12-23 08:13:20 UTC

DHCP options:
    Name: server-identifier, Value: 10.0.0.1
    Code: 1, Type: ip-address, Value: 255.255.255.0
```

Sample Output

show system services dhcp client statistics

```
user@host> show system services dhcp client statistics
Packets dropped:
    Total                     0
Messages received:
    DHCPOFFER                 0
    DHCPACK                   8
    DHCPNAK                   0
Messages sent:
    DHCPDECLINE               0
    DHCPDISCOVER              0
    DHCPREQUEST               1
    DHCPINFORM                0
    DHCPRELEASE               0
    DHCPRENEW                 7
    DHCPREBIND                0
```

show system services dhcp conflict

Syntax

```
show system services dhcp conflict
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

(J Series routers only and EX Series switches) Display Dynamic Host Configuration Protocol (DHCP) client-detected conflicts for IP addresses. When a conflict is detected, the DHCP server removes the address from the address pool.

Options

This command has no options.

Required Privilege Level

view and system

Related Documentation

- clear system services dhcp conflict on page 1671

List of Sample Output

show system services dhcp conflict on page 1976

Output Fields

Table 115 on page 1976 describes the output fields for the **show system services dhcp conflict** command. Output fields are listed in the approximate order in which they appear.

Table 115: show system services dhcp conflict Output Fields

Field Name	Field Description
Detection time	Date and time the client detected the conflict.
Detection method	How the conflict was detected.
Address	IP address where the conflict occurs. The addresses in the conflicts list remain excluded from the pool until you use a **clear system services dhcp conflict** command to manually clear the list.

Sample Output

show system services dhcp conflict

```
user@host> show system services dhcp conflict

Detection time           Detection method  Address
2004-08-03 19:04:00 PDT  ARP               10.0.0.1
2004-08-04 04:23:12 PDT  Ping              10.0.0.2
2004-08-05 21:06:44 PDT  Client            10.0.0.3
```

show system services dhcp global

Syntax

```
show system services dhcp global
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

(J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) global configuration options. Global options apply to all scopes and clients served by the DHCP server. Global options are overridden if specified otherwise in scope or client options. Scope options apply to specific subnets or ranges of addresses. Client options apply to specific clients.

Options

This command has no options.

Required Privilege Level

view and system

List of Sample Output

show system services dhcp global on page 1978

Output Fields

Table 116 on page 1977 describes the output fields for the **show system services dhcp global** command. Output fields are listed in the approximate order in which they appear.

Table 116: show system services dhcp global Output Fields

Field Name	Field Description
BOOTP lease length	Length of lease time assigned to BOOTP clients.
Default lease time	Lease time assigned to clients that do not request a specific lease time.
Minimum lease time	Minimum time a client retains an IP address lease on the server.
Maximum lease time	Maximum time a client can retain an IP address lease on the server.
DHCP options	User-defined options created for the DHCP server. If no options have been defined, this field is blank.

Sample Output

show system services dhcp global

```
user@host> show system services dhcp global

Global settings:
    BOOTP lease length         infinite

DHCP lease times:
    Default lease time         1 hour
    Minimum lease time         2 hours
    Maximum lease time         infinite

DHCP options:
    Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
    Name: domain-name, Value: mydomain.tld
    Code: 19, Type: flag, Value: off
    Code: 40, Type: string, Value: domain.tld
    Code: 32, Type: ip-address, Value: 3.3.3.33
```

show system services dhcp pool

Syntax

```
show system services dhcp pool
<detail>
<subnet-address>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

(J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server IP address pools.

Options

none—Display brief information about all IP address pools.

detail—(Optional) Display detailed information.

subnet-address—(Optional) Display information for the specified subnet address.

Required Privilege Level

view and system

List of Sample Output

show system services dhcp pool on page 1980
show system services dhcp pool subnet-address on page 1980
show system services dhcp pool subnet-address detail on page 1980

Output Fields

Table 117 on page 1979 describes the output fields for the **show system services dhcp pool** command. Output fields are listed in the approximate order in which they appear.

Table 117: show system services dhcp pool Output Fields

Field Name	Field Description	Level of Output
Pool name	Subnet on which the IP address pool is defined.	None specified
Low address	Lowest address in the IP address pool.	None specified
High address	Highest address in the IP address pool.	None specified
Excluded addresses	Addresses excluded from the address pool.	None specified
Subnet	(***subnet-address*** option only) Subnet to which the specified address pool belongs.	None specified
Address range	(***subnet-address*** option only) Range of IP addresses in the address pool.	None specified
Addresses assigned	Number of IP addresses in the pool that are assigned to DHCP clients and the total number of IP addresses in the pool.	**detail**
Active	Number of assigned IP addresses in the pool that are active.	**detail**

Table 117: show system services dhcp pool Output Fields (continued)

Field Name	Field Description	Level of Output
Excluded	Number of assigned IP addresses in the pool that are excluded.	**detail**
Default lease time	Lease time assigned to clients that do not request a specific lease time.	**detail**
Minimum lease time	Minimum time a client can retain an IP address lease on the server.	**detail**
Maximum lease time	Maximum time a client can retain an IP address lease on the server.	**detail**
DHCP options	User-defined options created for the DHCP server. If no options have been defined, this field is blank.	**detail**

Sample Output

show system services dhcp pool

```
user@host> show system services dhcp pool

Pool name    Low address   High address   Excluded addresses
192.0.2.0/24 192.0.2.2     192.0.2.254     192.0.2.1
```

show system services dhcp pool subnet-address

```
user@host> show system services dhcp pool 192.0.2.0/24

Pool information:
    Subnet                    192.0.2.0/24
    Address range             192.0.2.2 - 192.0.2.254
    Addresses assigned        2/253
```

show system services dhcp pool subnet-address detail

```
user@host> show system services dhcp pool 192.0.2.0/24 detail

Pool information:
    Subnet                    192.0.2.0/24
    Address range             192.0.2.2 - 192.0.2.254
    Addresses assigned        2/253
      Active: 1, Excluded: 1

DHCP lease times:
    Default lease time        1 hour
    Minimum lease time        2 hours
    Maximum lease time        infinite

DHCP options:
    Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
    Name: domain-name, Value: mydomain.tld
```

```
  Name: router, Value: { 192.0.2.1 }
  Name: server-identifier, Value: 192.0.2.1
  Code: 19, Type: flag, Value: off
  Code: 40, Type: string, Value: domain.tld
  Code: 32, Type: ip-address, Value: 192.0.2.1
```

show system services dhcp relay-statistics

Syntax **show system services dhcp relay-statistics**

Release Information Command introduced in Junos OS Release 8.5 .

Description Display information about the DHCP relay.

Required Privilege Level view and system

Related Documentation
- *dhcp*

List of Sample Output show system services dhcp relay-statistics on page 1983

Output Fields Table 118 on page 1982 lists the output fields for the **show system services dhcp relay-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 118: show system services dhcp relay-statistics Output Fields

Field Name	Field Description
Received packets	Total DHCP packets received.
Forwarded packets	Total DHCP packet forwarded.
Dropped packets	Total DHCP packets dropped for the following reasons: • **Due to a missing interface in the relay database**—Number of packets discarded because they did not belong to a configured interface. • **Due to a missing matching routing instance**—Number of packets discarded because they did not belong to a configured routing instance. • **Due to an error during packet read**—Number of packets discarded because of a system read error. • **Due to an error during packet send**—Number of packets that the DHCP relay application could not send. • **Due to an invalid server address**—Number of packets discarded because an invalid server address was specified. • **Due to a missing valid local address**—Number of packets discarded because there was no valid local address. • **Due to a missing route to the server or client**—Number of packets discarded because there were no addresses available for assignment.

Sample Output

show system services dhcp relay-statistics

```
user@host> show system services dhcp relay-statistics
Received packets: 4
Forwarded packets: 4
Dropped packets: 4
  Due to missing interface in relay database: 4
  Due to missing matching routing instance: 0
  Due to an error during packet read: 0
  Due to an error during packet send: 0
  Due to invalid server address: 0
  Due to missing valid local address: 0
  Due to missing route to server/client: 0
```

show system services dhcp statistics

Syntax show system services dhcp statistics

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server statistics.

Options This command has no options.

Required Privilege Level view and system

Related Documentation
- clear system services dhcp statistics on page 1672

List of Sample Output show system services dhcp statistics on page 1985

Output Fields Table 119 on page 1984 describes the output fields for the **show system services dhcp statistics** command. Output fields are listed in the approximate order in which they appear.

Table 119: show system services dhcp statistics Output Fields

Field Name	Field Description
Default lease time	Lease time assigned to clients that do not request a specific lease time.
Minimum lease time	Minimum time a client can retain an IP address lease on the server.
Maximum lease time	Maximum time a client can retain an IP address lease on the server.
Packets dropped	Total number of packets dropped and number of packets dropped because of: • Invalid hardware address • Invalid opcode • Invalid server address • No available address • No interface match • No routing instance match • No valid local addresses • Packet too short • Read error • Send error

Table 119: show system services dhcp statistics Output Fields (continued)

Field Name	Field Description
Messages received	Number of the following message types sent from DHCP clients and received by the DHCP server: • BOOTREQUEST • DHCPDECLINE • DHCPDISCOVER • DHCPINFORM • DHCPRELEASE • DHCPREQUEST
Messages sent	Number of the following message types sent from the DHCP server to DHCP clients: • BOOTREPLY • DHCPACK • DHCPOFFER • DHCPNAK

Sample Output

show system services dhcp statistics

```
user@host> show system services dhcp statistics

DHCP lease times:
    Default lease time         1 hour
    Minimum lease time         2 hours
    Maximum lease time         infinite

Packets dropped:
    Total                      0
    Bad hardware address       0
    Bad opcode                 0
    Invalid server address     0
    No available addresses     0
    No interface match         0
    No routing instance match  0
    No valid local address     0
    Packet too short           0
    Read error                 0
    Send error                 0

Messages received:
    BOOTREQUEST                0
    DHCPDECLINE                0
    DHCPDISCOVER               0
    DHCPINFORM                 0
    DHCPRELEASE                0
    DHCPREQUEST                0

Messages sent:
    BOOTREPLY                  0
    DHCPACK                    0
```

```
DHCPOFFER                0
DHCPNAK                  0
```

show system services service-deployment

Syntax show system services service-deployment

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Display information about a Session and Resource Control (SRC) client.

Options This command has no options.

Required Privilege Level system
view

List of Sample Output show system services service-deployment on page 1987

Output Fields Table 120 on page 1987 lists the output fields for the **show system services service-deployment** command. Output fields are listed in the approximate order in which they appear.

Table 120: show system services service-deployment Output Fields

Field Name	Field Description
PDT Keepalive settings	Configured PDT keepalive interval, in seconds.
Keepalives sent	Number of keepalives sent.
Notifications sent	Number of notifications sent.
Last update from peer	Time at which the last update from a peer was received.

Sample Output

show system services service-deployment

```
user@host> show system services service-deployment

Connected to 192.0.2.0 port 10288 since 2004-05-03 11:04:34 PDT Keepalive settings:
 Interval 15 seconds Keepalives sent: 750 Notifications sent: 0 Last update from
 peer: 00:00:06 ago
```

show system snapshot media

Syntax

```
show system snapshot < media (compact-flash | external | harddisk | internal | usb) >
```

Release Information

Command introduced in Junos OS Release 10.2 .

Description

Display information about the partitioning scheme present on the media. Information for only one root is displayed for single-root partitioning, whereas information for both roots is displayed for dual-root partitioning.

Options

- compact-flash— Show snapshot information from the CompactFlash card. (Supported on SRX5400, SRX5600, SRX5800)
- external— Show snapshot information from the external CompactFlash card. (Not supported on SRX5000 Series devices)
- hard-disk— Show snapshot information from the Hard Disk. (Supported on SRX5400, SRX5600, SRX5800)
- internal— Show snapshot information from internal media. (Not supported on SRX5000 Series devices)
- usb— Show snapshot information from device connected to USB port.

Required Privilege Level

View

Related Documentation

- *Creating a Snapshot and Using It to Boot an SRX Series device*

List of Sample Output

show system snapshot media compact-flash on page 1989
show system snapshot media external on page 1989
show system snapshot media internal on page 1989
show system snapshot media usb on page 1989
show system snapshot media hard-disk on page 1989

Output Fields

Table 121 on page 1988 lists the output fields for the **show system snapshot media** command. Output fields are listed in the approximate order in which they appear.

Table 121: show system snapshot media Output Fields

Field Name	Field Description
Creation date	Date and time of the last snapshot.
JUNOS version on snapshot	Junos OS release number of individual software packages.

Sample Output

show system snapshot media compact-flash

show system snapshot media compact-flash

```
Information for snapshot on compact-flash (ad0s1)
Creation date: Aug 21 11:58:14 2017
JUNOS version on snapshot:
  junos  : 12.3X48-D40.5-domestic
```

show system snapshot media external

show system snapshot media external

```
Information for snapshot on      external (/dev/da1s2a) (primary)
Creation date: Apr 9 09:41:16 2018
JUNOS version on snapshot:
  junos  : 12.3X48-D40.5-domestic
Information for snapshot on       external (/dev/da1s1a) (backup)
Creation date: Apr 9 09:41:16 2018
JUNOS version on snapshot:
  junos  : 12.3X48-D40.5-domestic
```

show system snapshot media internal

show system snapshot media internal

```
Information for snapshot on       internal (/dev/da0s1a) (primary)
Creation date: Jan 15 10:43:26 2010
JUNOS version on snapshot:
  junos  : 10.1B3-domestic
Information for snapshot on       internal (/dev/da0s2a) (backup)
Creation date: Jan 15 10:15:32 2010
JUNOS version on snapshot:
  junos  : 10.2-20100112.0-domestic
```

show system snapshot media usb

show system snapshot media usb

```
Information for snapshot on usb (da0s1)
Creation date: Apr 9 08:44:46 2018
JUNOS version on snapshot:
  junos  : 12.3X48-D40.5-domestic
```

show system snapshot media hard-disk

show system snapshot media hard-disk

```
Information for snapshot on hard-disk (ad2s1)
Creation date: Apr 9 16:40:18 2018
JUNOS version on snapshot:
  junos  : 12.3X48-D40.5-domestic
```

show system storage partitions

List of Syntax

Syntax (EX Series) on page 1990
Syntax (SRX Series) on page 1990

Syntax (EX Series)

```
show system storage partitions
<all-members>
<local>
<member member-id>
```

Syntax (SRX Series)

```
show system storage partitions
```

Release Information

Command introduced in Junos OS Release 10.2 for SRX300, SRX320, SRX340, SRX345, and SRX550HM devices.
Command introduced in Junos OS Release 11.1 for EX Series switches.

Description

Display information about the disk partitioning scheme.

Options

none—Display partition information.

all-members—(Virtual Chassis systems only) (Optional) Display partition information for all members of the Virtual Chassis.

local—(Virtual Chassis systems only) (Optional) Display partition information for the local Virtual Chassis member.

member *member-id*—(Virtual Chassis systems only) (Optional) Display partition information for the specified member of the Virtual Chassis configuration.

Required Privilege Level

view

Related Documentation

- *Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch*
- *Example: Installing Junos OS on SRX Series Devices Using the Partition Option*

List of Sample Output

show system storage partitions (EX Series) on page 1991
show system storage partitions (SRX Series, Dual Root Partitioning) on page 1991
show system storage partitions (SRX Series, Single Root Partitioning) on page 1992
show system storage partitions (SRX Series, USB) on page 1992

Output Fields

Table 122 on page 1991 describes the output fields for the **show system storage partitions** command. Output fields are listed in the approximate order in which they appear.

Table 122: show system storage partitions Output Fields

Field Name	Field Description
Boot Media	Media (internal or external) from which the switch was booted.
Active Partition	Name of the active root partition.
Backup Partition	Name of the backup (alternate) root partition.
Currently booted from	Partition from which the switch was last booted.
Partitions information	Information about partitions on the boot media: • Partition—Partition identifier. • Size—Size of partition. • Mountpoint—Directory on which the partition is mounted.

Sample Output

show system storage partitions (EX Series)

```
user@switch> show system storage partitions
fpc0:
--------------------------------------------------------------------------------
Boot Media: internal (da0)
Active Partition: da0s1a
Backup Partition: da0s2a
Currently booted from: active (da0s1a)

Partitions information:
  Partition  Size   Mountpoint
  s1a        184M   /
  s2a        184M   altroot
  s3d        369M   /var/tmp
  s3e        123M   /var
  s4d        62M    /config
  s4e               unused (backup config)
```

show system storage partitions (SRX Series, Dual Root Partitioning)

```
show system storage partitions
Boot Media: internal (da0)
Active Partition: da0s2a
Backup Partition: da0s1a
Currently booted from: active (da0s2a)

Partitions Information:
  Partition  Size   Mountpoint
      s1a    293M   altroot
      s2a    293M   /
      s3e    24M    /config
      s3f    342M   /var
      s4a    30M    recovery
```

show system storage partitions (SRX Series, Single Root Partitioning)

show system storage partitions

```
Boot Media: internal (da0)
Partitions Information:
  Partition  Size   Mountpoint
      s1a    898M   /
      s1e    24M    /config
      s1f    61M    /var
```

show system storage partitions (SRX Series, USB)

show system storage partitions

```
Boot Media: usb (da1)
Active Partition: da1s1a
Backup Partition: da1s2a
Currently booted from: active (da1s1a)

Partitions Information:
  Partition  Size   Mountpoint
      s1a    293M   /
      s2a    293M   altroot
      s3e    24M    /config
      s3f    342M   /var
      s4a    30M    recovery
```

show system users

List of Syntax

Syntax

```
show system users
<no-resolve>
```

Syntax (TX Matrix Router)

```
show system users
<all-chassis | all-lcc | lcc number | scc>
<no-resolve>
```

Syntax (TX Matrix Plus Router)

```
show system users
<detail>
<all-chassis | all-lcc | lcc number | sfc number> <no-resolve>
```

Syntax (MX Series Router)

```
show system users
<all-members>
<local>
<member member-id>
<no-resolve>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in JUNOS OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

List information about the users who are currently logged in to the router or switch.

NOTE: The **show system users** command lists the information about administrative users that are logged in to a router or switch using the CLI, J-Web, or an SSH client. The output does not list information about web users or automated users that are logged in from a remote client application using Junos XML APIs, such as NETCONF.

Options

none—List information about the users who are currently logged in to the router or switch.

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Show users currently logged in to all the routers in the chassis.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show users currently logged in to all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, show users currently logged in to all connected T1600 or T4000 LCCs.

all-members—(MX Series routers only) (Optional) Display users currently logged in to all members of the Virtual Chassis configuration.

lcc *number*—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show users currently logged in to a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, show users currently logged in to a specific router that is connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(MX Series routers only) (Optional) Display users currently logged in to the local Virtual Chassis member.

member *member-id*—(MX Series routers only) (Optional) Display users currently logged in to the specified member of the Virtual Chassis configuration. Replace ***member-id*** with a value of 0 or 1.

no-resolve—(Optional) Do not attempt to resolve IP addresses to hostnames.

scc—(TX Matrix routers only) (Optional) Show users currently logged in to the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routersonly) (Optional) Show users currently logged in to the TX Matrix Plus router. Replace ***number*** with 0.

Additional Information

By default, when you issue the **show system users** command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

Required Privilege Level

view

Related Documentation

- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

List of Sample Output

Output Fields

Table 123 on page 1995 describes the output fields for the **show system users** command. Output fields are listed in the approximate order in which they appear.

Table 123: show system users Output Fields

Field Name	Field Description
time **and up**	Current time, in the local time zone, and how long the router or switch has been operational.
users	Number of users logged in to the router or switch.
load averages	Load averages for the last 1 minute, 5 minutes, and 15 minutes.
USER	Username.
TTY	Terminal through which the user is logged in.
FROM	System from which the user has logged in. A hyphen indicates that the user is logged in through the console.
LOGIN@	Time when the user logged in.
IDLE	How long the user has been idle.
WHAT	Processes that the user is running.

Sample Output

show system users

```
user@host> show system users
 7:30PM  up 4 days,  2:26, 2 users, load averages: 0.07, 0.02, 0.01
USER     TTY FROM              LOGIN@  IDLE WHAT
root     d0  -                Fri05PM 4days -csh (csh)
blue   p0 level5.company.net 7:30PM     - cli
```

show system users lcc no-resolve (TX Matrix, TX Matrix Plus Router)

```
user@host> show system users lcc 2 no-resolve

lcc2-re0:
```

```
--------------------------------------------------------------------------
10:34AM PDT up 1 day,  7:11, 5 users, load averages: 0.03, 0.01, 0.00
USER     TTY      FROM                              LOGIN@  IDLE WHAT
root     d0       -                                3:21AM   7:12 /bin/csh
user1    p0       scc-re0                          10:15AM     - telnet hostA
user1    p1       scc-re0                          10:16AM     - telnet hostA
user1    p2       scc-re0                          10:19AM     - telnet hostA
user1    p3       scc-re0                          10:24AM     - telnet hostA
```

show system users (TX Matrix Plus Router)

```
user@host> show system users
sfc0-re0:
--------------------------------------------------------------------------
 1:41AM  up 26 mins, 3 users, load averages: 0.08, 0.04, 0.03
USER     TTY      FROM                              LOGIN@  IDLE WHAT
user2    p0       10.209.208.123                   1:18AM     21 cli
user2    p1       192.0.2.207                     1:37AM      2 cli
user2    p2       192.0.2.19                      1:40AM      - cli

lcc0-re0:
--------------------------------------------------------------------------
 1:41AM  up 26 mins, 0 users, load averages: 0.00, 0.00, 0.03

lcc1-re0:
--------------------------------------------------------------------------
 1:41AM  up 26 mins, 0 users, load averages: 0.00, 0.02, 0.03

lcc2-re0:
--------------------------------------------------------------------------
 1:41AM  up 26 mins, 0 users, load averages: 0.16, 0.06, 0.02

lcc3-re0:
--------------------------------------------------------------------------
 1:41AM  up 26 mins, 0 users, load averages: 0.12, 0.04, 0.04

user3@aj> show system users
sfc0-re0:
--------------------------------------------------------------------------
 1:42AM  up 28 mins, 4 users, load averages: 0.02, 0.03, 0.02
USER     TTY      FROM                              LOGIN@  IDLE WHAT
user     p0       device1.example.com              1:18AM     22 cli
user     p1       device2.example.com              1:37AM      - cli
user     p2       device3.example.com              1:40AM      - cli
user     p3       device4.example.com              1:42AM      - -csh (csh)

lcc0-re0:
--------------------------------------------------------------------------
 1:42AM  up 28 mins, 0 users, load averages: 0.02, 0.01, 0.03

lcc1-re0:
--------------------------------------------------------------------------
 1:42AM  up 28 mins, 0 users, load averages: 0.07, 0.04, 0.03

lcc2-re0:
--------------------------------------------------------------------------
 1:42AM  up 27 mins, 0 users, load averages: 0.07, 0.06, 0.02

lcc3-re0:
```

```
------------------------------------------------------------------------
1:42AM  up 28 mins, 0 users, load averages: 0.05, 0.04, 0.04
```

show system users (QFX Series)

```
user@switch> show system users
USER     TTY      FROM                              LOGIN@  IDLE WHAT
user1    p0       192.0.2.117                     2:54AM     39 -cli (cli)
user2    p1       192.0.2.116                     3:01AM      - -cli (cli)
user3    p2       192.0.2.97                      3:08AM     11 -cli (cli)
```

show system users no-resolve (QFX Series)

```
user@switch> show system users no-resolve
USER     TTY      FROM                              LOGIN@  IDLE WHAT
user1    p0       192.0.2.117                     2:54AM     39 -cli (cli)
user2    p1       192.0.2.116                     3:01AM      - -cli (cli)
user3    p2       192.0.2.97                      3:08AM     11 -cli (cli)
```

test access profile

Syntax test access profile *profile-name* user *username* password *password* <detail>

Release Information Command introduced in Junos OS Release 9.1.

Description Specify a profile to use to get information from a RADIUS server, which includes all the information from the **test access radius-server** command.

Options **detail**—(Optional) Show the RADIUS attributes returned by the server.

profile-name—Access profile name configured.

password—Password for the username.

username—User name to be authenticated to the RADIUS server.

Required Privilege Level view

List of Sample Output test access profile on page 1999
test access profile detail on page 1999

Output Fields Table 124 on page 1998 lists the output fields for the **test access profile** command. Output fields are listed in the approximate order in which they appear.

Table 124: test access profile Output Fields

Field Name	Field Description
Profile Name	Name of the configured access profile.
Client Username	The user name authenticated by the RADIUS server.
Client Password	The user password authenticated by the RADIUS server.
Num Servers	Number of RADIUS servers in the configured access profile.
Server List	List of RADIUS servers in the configure access profile.
IP Address	The IP address of the RADIUS server authenticated.
UDP Port	The RADIUS server port utilized during the authentication test.
Source Address	The source IP address of the client making the RADIUS request. If no address is shown, it defaults to the address of the outgoing interface.
Timeout	The RADIUS server timeout period.

Table 124: test access profile Output Fields (continued)

Field Name	Field Description
Retry Count	The number of authentication attempts allowed by the RADIUS server.
Secret	The shared secret used for authentication with the RADIUS server.
Status	The test result status (Accepted or Rejected) and the number of retransmits utilized during authentication.
Attempts	The number of authentication attempts on the RADIUS server.
Attribute List	The list of returned RADIUS attributes, sorted by the attribute name, and including parameter length and value. See your RADIUS server documentation for attribute descriptions.
(Attribute) Name	The name of the attribute.
(Attribute) Length	The attribute length in bytes.
(Attribute) Value	The attribute value.

Sample Output

test access profile

The following example uses the **test access profile** command to access and display basic information about the RADIUS server(s) shown in the resulting output:

```
user@host> test access profile alpha user TEST password TEST
```

```
user@host> test access profile alpha user TEST password TEST
Test Radius Profile Access
    Profile Name        : alpha
    Client Username     : TEST
    Client Password     : TEST
    Num Servers         : 5
                          Server List
                UDP       Source                  Retry
  IP Address    Port      Address         Timeout Count Secret        Status
 Attempts
1.1.1.1         1812      10.10.10.10     2       1     TEST          Timeout
 2
1.2.3.4         1812      Default         1       2     TEST          Timeout
 3
192.168.10.10   1812      Default         3       3     TEST          Accepted
 1
```

test access profile detail

The following example uses the **test access profile detail** command to access and display detailed information about the RADIUS server(s) shown in the resulting output:

user@host> **test access profile alpha user TEST password TEST detail**

```
user@host> test access profile alpha user TEST password TEST detail
Test Radius Profile Access Detailed
    Profile Name        : alpha
    Client Username     : TEST
    Client Password     : TEST
    Num Servers         : 5
                   Radius Server List

       IP Address           : 1.2.3.4
       UDP Port             : 1812
       Source Address       : 192.168.10.10
       Timeout              : 2
       Retry Count          : 1
       Secret               : TEST
       Status               : Timeout
       Attempts             : 2

       IP Address           : 1.2.3.5
       UDP Port             : 1812
       Source Address       : Default
       Timeout              : 1
       Retry Count          : 2
       Secret               : TEST
       Status               : Timeout
       Attempts             : 3

       IP Address           : 192.168.10.10
       UDP Port             : 1812
       Source Address       : Default
       Timeout              : 3
       Retry Count          : 3
       Secret               : TEST
       Status               : Accepted
       Attempts             : 1

                             Attribute List
  Name                                Length  Value
  Class                               52      SBR2CLÍ½¾¿ðÕ¾¿
  Acct-Interim-Interval               4       5
  Callback-Id                         12      123-456-789
  Callback-Number                     13      555-555-1212
  Class                               15      Class information
  Filter-Id                           4       999
  Filter-Id                           6       12345
  Framed-Compression                  4       0
  Framed-IP-Address                   4       1:2:3:4
  Framed-IP-Netmask                   4       255:255:255:255
  Framed-IPv6-Route                   15      1:2:3:4:5:6:7:8

  Framed-MTU                          4       1024
  Framed-Pool                         9       pool sbr
  Framed-Protocol                     4       1
  Framed-Route                        8       iproute
  Framed-Routing                      4       0
  Vendor-Specific                     11      583
  Idle-Timeout                        4       3
  Vendor-Specific                     10      a4c
  Vendor-Specific                     14      a4c
  Login-IP-Host                       4       10:1:1:1
```

```
Login-LAT-Group                  10      lat group
Login-LAT-Node                   9       lat node
Login-LAT-Port                   9       lat port
Login-LAT-Service                12      lat service
Login-Service                    4       0
Login-TCP-Port                   4       1812
Vendor-Specific                  10      137
Vendor-Specific                  38      137
Vendor-Specific                  10      137
Vendor-Specific                  9       137
Vendor-Specific                  16      137
Vendor-Specific                  10      137
Vendor-Specific                  10      137
Vendor-Specific                  10      137
Vendor-Specific                  9       137
Vendor-Specific                  10      137
Vendor-Specific                  10      137
Vendor-Specific                  10      137
Vendor-Specific                  10      137
Password-Retry                   4       3
Port-Limit                       4       100
Prompt                           4
Reply-Message                    18      Radius Server SB
Service-Type                     4       2
Session-Timeout                  4       10
Termination-Action               4       1
Tunnel-Assignment-ID             4
Tunnel-Client-Auth-ID            6
Tunnel-Client-Endpoint           4
Tunnel-Password                  19
Tunnel-Type                      4       12
MS BAP Usage                     4       0
MS-CHAP MPPE-Keys                32      -1234567890
MS-CHAP2 Success                 3       123456789
MS Filter                        10      ms-filter
MS Link Drop Time Limit          4       5
MS Link Utilization Threshold    4       6
MS MPPE Encryption Policy        4       1
MS MPPE Encryption Types         3       -556677889
MS Primary DNS Server            4       1:1:1:1
MS Primary NBNS Server           4       2:2:2:2
MS Secondary DNS Server          4       3:3:3:3
MS Secondary NBNS Server         4       4:4:4:4
```

test access radius-server

Syntax

test access radius-server *address* user *username* password *password* secret *secret*
<authentication-port *port*>
<retry *number*>
<source-address *address*>
<timeout *number*>

Release Information

Command introduced in Junos OS Release 9.1.

Description

Verify RADIUS server authentication parameters.

Options

address—RADIUS server under test IP address.

password—Password for the user.

secret—Secret shared with the RADIUS server.

user—User name to be authenticated to the RADIUS server.

authentication-port—(Optional) RADIUS server authentication port number (1through 65535).

retry—(Optional) Retry attempts (1through 10).

source-address—(Optional) Use an alternate address as the source address.

timeout—(Optional) Request timeout period (1through 90 seconds).

Required Privilege Level

view

List of Sample Output

test access radius-server user password secret on page 2003

Output Fields

Table 125 on page 2002 lists the output fields for the **test access radius-server** command. Output fields are listed in the approximate order in which they appear.

Table 125: test access radius-server Output Fields

Field Name	Field Description
Server	The IP address of the RADIUS server authenticated.
UDP port	The RADIUS server port utilized during the authentication test.
Source IP Address	"Default" is shown if the IP address is the same as that of the RADIUS server. Alternatively, an IP address specified for authentication is shown.
Server timeout	The RADIUS server timeout period.

Table 125: test access radius-server Output Fields (continued)

Field Name	Field Description
Sever retry count	The number of authentication attempts allowed by the RADIUS server.
Secret	The shared secret used for authentication with the RADIUS server.
Client Username	The user name authenticated by the RADIUS server.
Client Password	The user password authenticated by the RADIUS server.
Status	The test result status (**Accepted** or **Rejected**) and the number of retransmits utilized during authentication.

Sample Output

test access radius-server user password secret

The following example command tests RADIUS authentication with a specific server (172.28.30.95), user (JOHNDOE), secret (No1Knows), and password (JohnPass); and displays the resulting output:

```
user@host> test access radius-server 172.28.30.95 user JOHNDOE password JohnPass secret No1Knows
```

```
Test Radius Server Access
       Server              : 172.28.30.95
       UDP port            : 1812
       Source IP Address   : Default
       Server timeout      : 3
       Sever retry count   : 3
       Secret              : No1Knows
       Client Username     : JOHNDOE
       Client Password     : JohnPass
       Status              : Accepted, retransmits: 0
```