



---

# User and Access Management Feature Guide for the QFX Series

Release  
15.1



---

Modified: 2016-06-28



# Table of Contents

	About the Documentation . . . . .	xi
	Documentation and Release Notes . . . . .	xi
	Supported Platforms . . . . .	xi
	Using the Examples in This Manual . . . . .	xi
	Merging a Full Example . . . . .	xii
	Merging a Snippet . . . . .	xii
	Documentation Conventions . . . . .	xiii
	Documentation Feedback . . . . .	xv
	Requesting Technical Support . . . . .	xv
	Self-Help Online Tools and Resources . . . . .	xv
	Opening a Case with JTAC . . . . .	xvi
<b>Part 1</b>	<b>User and Access Management Overview</b>	
<b>Chapter 1</b>	<b>Understanding the Software . . . . .</b>	<b>3</b>
	Understanding Junos OS Infrastructure and Processes . . . . .	3
	Routing Engine and Packet Forwarding Engine . . . . .	3
	Junos OS Processes . . . . .	4
	Understanding LLDP . . . . .	5
	Monitoring SNMP . . . . .	6
<b>Chapter 2</b>	<b>Understanding Access and Authentication Methods . . . . .</b>	<b>9</b>
	Understanding Junos OS Access Privilege Levels . . . . .	9
	Junos OS Login Class Permission Flags . . . . .	9
	Allowing or Denying Individual Commands for Junos OS Login Classes . . . . .	13
	Junos OS User Authentication Methods . . . . .	14
	Understanding Login Authentication . . . . .	15
	MAC RADIUS Authentication . . . . .	15
<b>Part 2</b>	<b>Configuring Access</b>	
<b>Chapter 3</b>	<b>Configuring and Managing Root Users . . . . .</b>	<b>19</b>
	Configuring Management Access . . . . .	19
	Configuring Access Privilege Levels . . . . .	19
	Configuring Login Tips . . . . .	20
	Recovering the Root Password . . . . .	20
	Example: Configuring a Plain-Text Password for Root Logins . . . . .	22
	Example: Configuring SSH Authentication for Root Logins . . . . .	24
	Understanding Troubleshooting Resources . . . . .	24
	Troubleshooting Overview . . . . .	26
	Recovering the Root Password . . . . .	28















# About the Documentation

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

## Documentation and Release Notes

---

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

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

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

## Supported Platforms

---

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

- [QFX Series](#)

## Using the Examples in This Manual

---

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

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







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

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto: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 J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

## Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>



## PART 1

# User and Access Management Overview

- [Understanding the Software on page 3](#)
- [Understanding Access and Authentication Methods on page 9](#)



## CHAPTER 1

# Understanding the Software

- [Understanding Junos OS Infrastructure and Processes on page 3](#)
- [Understanding LLDP on page 5](#)
- [Monitoring SNMP on page 6](#)

## Understanding Junos OS Infrastructure and Processes

---

Junos OS includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the switch.

Junos OS runs on the Routing Engine. The Routing Engine kernel coordinates communication among the Junos OS processes and provides a link to the Packet Forwarding Engine.

Using the Junos OS command-line interface (CLI), you configure switching features and set the properties of network interfaces. After activating a software configuration, use either the Junos Space or CLI user interface to monitor, manage operations, and diagnose protocol and network connectivity problems.

- [Routing Engine and Packet Forwarding Engine on page 3](#)
- [Junos OS Processes on page 4](#)

## Routing Engine and Packet Forwarding Engine

A switch has two primary software processing components:

- **Packet Forwarding Engine**—Processes packets; applies filters, routing policies, and other features; and forwards packets to the next hop along the route to their final destination.
- **Routing Engine**—Provides three main functions:
  - Creates the packet forwarding switch, which provides route lookup, filtering, and switching on incoming data packets, and then directs outbound packets to the appropriate interface for transmission to the network.
  - Maintains the routing tables used by the switch and controls the routing protocols that run on the switch.
  - Provides control and monitoring functions for the switch, including controlling power and monitoring system status.













Table 4 on page 10 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.

**Table 4: Login Class Permission Flags**

Permission Flag	Description
<b>access</b>	Can view the access configuration in configuration mode and with the <b>show configuration</b> operational mode command.
<b>access-control</b>	Can view and configure access information at the <b>[edit access]</b> hierarchy level.
<b>admin</b>	Can view user account information in configuration mode and with the <b>show configuration</b> operational mode command.
<b>admin-control</b>	Can view user accounts and configure them at the <b>[edit system login]</b> hierarchy level.
<b>all-control</b>	Can access all operational mode commands and configuration mode commands. Can modify configuration in all the configuration hierarchy levels.
<b>clear</b>	Can clear (delete) information learned from the network that is stored in various network databases by using the <b>clear</b> commands.
<b>configure</b>	Can enter configuration mode by using the <b>configure</b> command.
<b>control</b>	Can perform all control-level operations—all operations configured with the <b>-control</b> permission flags.
<b>field</b>	Can view field debug commands. Reserved for debugging support.
<b>firewall</b>	Can view the firewall filter configuration in configuration mode.
<b>firewall-control</b>	Can view and configure firewall filter information at the <b>[edit firewall]</b> hierarchy level.
<b>floppy</b>	Can read from and write to the removable media.
<b>flow-tap</b>	Can view the flow-tap configuration in configuration mode.
<b>flow-tap-control</b>	Can view the flow-tap configuration in configuration mode and can configure flow-tap configuration information at the <b>[edit services flow-tap]</b> hierarchy level.



Table 4: Login Class Permission Flags (*continued*)

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



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**.

- Related Documentation**
- [Configuring Access Privilege Levels on page 19](#)
  - [Access Privilege User Permission Flags Overview](#)

---

## 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.

- Related Documentation**
- [Configuring RADIUS Server Authentication](#)
  - [Configuring TACACS+ Authentication](#)
  - [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 67](#)

## Understanding Login Authentication

---

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.

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.

This topic covers:

- [MAC RADIUS Authentication on page 15](#)

## MAC RADIUS Authentication

You can configure MAC RADIUS authentication on interfaces that are connected to end devices.

The EAP method supported for MAC RADIUS authentication is EAP-MD5.

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.

### Related Documentation

- [Configuring RADIUS Authentication \(QFX Series or OCX Series\) on page 83](#)



## PART 2

# Configuring Access

- [Configuring and Managing Root Users on page 19](#)
- [Configuring and Managing User Accounts on page 31](#)





































**NOTE:** "!" and "," are punctuation characters, but are listed under "special characters".

Control characters are not recommended.

You can include the **plain-text-password** statement at the following hierarchy levels:

- [edit system diag-port-authentication]
- [edit system pic-console-authentication]
- [edit system root-authentication]
- [edit system login user *username* authentication]

The **change-type** statement specifies whether the password is checked for the following:

- The total number of character sets used (**character-set**)
- The total number of character set changes (**set-transitions**)

For example, the following password:

MyPassWd@2

has four character sets (uppercase letters, lowercase letters, special characters, and numbers) and seven character set changes (**M**–**y**, **y**–**P**, **P**–**a**, **a**–**s**, **s**–**W**, **W**–**d**, **d**–**@**, and **@**–**2**).

The **change-type** statement is optional. If you omit the **change-type** option, Junos-FIPS plain-text passwords are checked for character sets, and Junos OS plain-text passwords are checked for character set changes.

The **minimum-changes** statement specifies how many character sets or character set changes are required for the password. This statement is optional. If you do not use the **minimum-changes** statement, character sets are not checked for Junos OS. If the **change-type** statement is configured for the **character-set** option, then the **minimum-changes** value must be 5 or less, because Junos OS only supports five character sets.

The **format** statement specifies the hash algorithm (**md5**, **sha1**, **sha256**, **sha512** or **des**) for authenticating plain-text passwords. This statement is optional. For Junos OS, the default format is **md5**. For Junos-FIPS, only **sha1** is supported.



**NOTE:** Starting with Junos OS Release 13.3, the **sha1** does not enable secure, protected specification of passwords and we recommend that you do not use the **sha1** algorithm to configure passwords. Instead, you can use the **sha256** or **sha512** to specify passwords by using the 256-bit and 512-bit cryptographic hash algorithm respectively for a robust and reliable operation.

The **maximum-length** statement specifies the maximum number of characters allowed in a password. This statement is optional. By default, Junos OS passwords have no maximum; however, only the first 128 characters are significant. Junos-FIPS passwords







```

user alexander {
    full-name "Alexander the Great";
    uid 1002;
    class view;
    authentication {
        encrypted-password "$ABC123";
        ssh-dsa "8924 37 5678 5678@user.device";
        ssh-dsa "6273 94 9283@user.device";
    }
}
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;
}
}

```

- Related Documentation**
- [Junos OS User Accounts Overview](#)
  - [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)

## Example: Configuring User Permissions with Access Privilege Levels

Create two access privilege classes on the router or switch, one for configuring and viewing user accounts only and the second for configuring and viewing SNMP parameters only:

In this example, you create two custom login classes on the router or switch and assign access privileges to each class through permission flags. The first custom login class is called **user-accounts** and it only includes access privileges for configuring and viewing user accounts. The second custom login class is called **network-mgmt** and only includes access privileges for configuring SNMP parameters.

```

[edit]
system {
    login {
        class user-accounts {
            permissions [ configure admin admin-control ];
        }
        class network-mgmt {
            permissions [ configure snmp snmp-control ];
        }
    }
}

```

1. Create the **user-accounts** custom login class and give it control over user accounts with the **configure admin admin-control** permission flag.

```
[edit system login]
user@router# set class user-accounts permissions configure admin admin-control
```

2. Create the **network-mgmt** custom login class and use the **configure snmp snmp-control** permission flag to assign it SNMP configuration privileges.

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

3. Check your configuration by using the **show system login** command.

```
user@router# show system login
class user-accounts {
  permissions [ configure admin admin-control ];
}
class network-mgmt {
  permissions [ configure snmp snmp-control ];
}
```

**Related Documentation** • [Configuring Access Privilege Levels on page 19](#)

---

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

---

Each operational mode command has an access privilege level associated with it. Access privileges control the commands that each custom login class can execute, configure, and view. Custom login classes are groups of users who are assigned with customized levels of access to different commands and statements. This ensures that each group of users can only use commands appropriate to their function, preventing unauthorized users from executing sensitive commands that could potentially cause damage to the network.

In this example, you create three custom login classes on the router or switch and assign access privileges for operational mode commands through the **allow-commands** and **deny-commands** settings. Each custom login class uses the same set of permission flags as the default login class **operator**, but the login class is allowed or denied certain operational mode commands. The first custom login class is called **operator-and-boot** and it has access to the **request system reboot** operational mode command. The second custom login class is called **operator-no-set** and it is denied access to any **set** commands. The third login class is called **operator-and-install-but-no-bgp** and it has access to the **request system software add** and **show route** operational mode commands, but it is denied access to the **show bgp** command.

```
[edit]
system {
  login {
    class operator-and-boot {
      permissions [ clear network reset trace view ];
      allow-commands "request system reboot";
    }
    class operator-no-set {
      permissions [ clear network reset trace view ];
    }
  }
}
```

```

        deny-commands "set";
    }
    class operator-and-install-but-no-bgp {
        permissions [ clear network reset trace view ];
        allow-commands "(request system software add)|(show route$)";
        deny-commands "show bgp";
    }
}
}

```

1. Create the **operator-and-boot** custom login class, give it **operator** level permission flags, and authorize it to use the **request system reboot** command.

```

[edit system login]
user@router# set class operator-and-boot permissions clear network reset trace view
user@router# set class operator-and-boot allow-commands request system reboot

```

2. Create the **operator-no-set** custom login class, give it **operator** level permission flags, and deny it access to the **set** command.

```

[edit system login]
user@router# set class operator-no-set clear network reset trace view
user@router# set class operator-no-set deny-commands set

```

3. Create the **operator-and-install-but-no-bgp** custom login class, give it **operator** level permission flags, authorize it to use the **request system software add** and **show route** commands, and deny it access to the **show bgp** command.

```

[edit system login]
user@router# set class operator-and-install-but-no-bgp clear network reset trace view
user@router# set class operator-and-install-but-no-bgp request system software add show route
user@router# set class operator-and-install-but-no-bgp show bgp

```

4. Check your configuration by using the **show system login** command.

```

user@router# show system login
class operator-and-boot {
    permissions [ clear network reset trace view ];
    allow-commands "request system reboot";
}
class operator-no-set {
    permissions [ clear network reset trace view ];
    deny-commands "set";
}
class operator-and-install-but-no-bgp {
    permissions [ clear network reset trace view ];
    allow-commands "(request system software add)|(show route$)";
    deny-commands "show bgp";
}

```

#### Related Documentation

- *Specifying Access Privileges for Junos OS Operational Mode Commands*

## 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 on page 42](#)
- [Overview on page 42](#)
- [Configuration on page 42](#)

### 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-numeric**s, **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-numeric 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 create 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-numeric 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-numeric 1;
minimum-upper-cases 1;
minimum-lower-cases 1;
```

### Related Documentation

- [Special Requirements for Junos OS Plain-Text Passwords on page 34](#)
- *password (Login)*

---

## Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions to Prevent Unauthorized Access

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.

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. 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.

#### Related Documentation

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

## Understanding Troubleshooting Resources

This topic describes some of the troubleshooting resources available for the QFX Series or OCX Series. These resources include tools such as the Junos OS CLI, Junos Space applications, and the Advanced Insight Scripts (AI-Scripts).

Table 5 on page 24 provides a list of some of the troubleshooting resources.

**Table 11: Troubleshooting Resources on the QFX and OCX Series**

Troubleshooting Resource	Description	Documentation
Chassis alarms	Chassis alarms indicate a failure on the switch or one of its components. A chassis alarm count is displayed on the LCD panel on the front of the switch.	<i>Chassis Alarm Messages on a QFX3500 Device</i>
Chassis Status LEDs and Fan Tray LEDs	A blinking amber Power, Fan, or Fan Tray LED indicates a hardware component error. A blinking amber Status LED indicates a software error.	<i>Chassis Status LEDs on a QFX3500 Device</i>



Table 11: Troubleshooting Resources on the QFX and OCX Series (*continued*)

Troubleshooting Resource	Description	Documentation
Junos Space Service Now	This application enables you to display and manage information about problem events. When problems are detected on the switch by Advanced Insight Scripts (AI-Scripts) that are installed on the switch, the data is collected and sent to Service Now for your review and action.	<i>Service Automation</i>
Junos Space Service Insight	This application helps in accelerating operational analysis and managing the exposure to known issues. You can identify devices that are nearing their End Of Life (EOL) and also discover and prevent issues that could occur in your network. The functionality of Service Insight is dependent on the information sent from Service Now.	<i>Service Automation</i>
Juniper Networks Knowledge Base	You can search in this database for Juniper Networks product information, including alerts and troubleshooting tips.	<a href="http://kb.juniper.net">http://kb.juniper.net</a>

## Troubleshooting Overview

This topic provides a general guide to troubleshooting some typical problems you may encounter on your QFX Series or OCX Series product.

[Table 6 on page 26](#) provides a list of problem categories, summary of the symptom or problem, and recommended actions with links to the troubleshooting documentation.

Table 12: Troubleshooting on the QFX Series

Problem Category	Symptom or Problem	Recommended Action
Switch hardware components	LCD panel shows a chassis alarm count.	<i>See Chassis Alarm Messages on a QFX3500 Device.</i>
	Fan tray LED is blinking amber.	<i>See Fan Tray LED on a QFX3500 Device.</i>
	Chassis status LED for the power is blinking amber.	<i>See Chassis Status LEDs on a QFX3500 Device.</i>
	Chassis status LED for the fan (on the management board) is blinking amber.	Replace the management board as soon as possible. <i>See Chassis Status LEDs on a QFX3500 Device.</i>

Table 12: Troubleshooting on the QFX Series (*continued*)

Problem Category	Symptom or Problem	Recommended Action
Port configuration	Cannot configure a port as a Gigabit Ethernet port.	<p>Check whether the port is a valid Gigabit Ethernet port (6 through 41).</p> <p>See <i>QFX3500 Device Overview</i>.</p>
	Cannot configure a port as a Fibre Channel port.	<p>Check whether the port is a valid Fibre Channel port (0 through 5 and 42 through 47).</p> <p>See <i>QFX3500 Device Overview</i>.</p>
	Cannot configure a port as a 10-Gigabit Ethernet port.	<p>If the port is not a 40-Gbps QSFP+ interface, check whether the port is in the range of 0 through 5 or 42 through 47. If one of the ports in that block (0 through 5 or 42 through 47) is configured as a Fibre Channel port, then all ports in that block must also be configured as Fibre Channel ports.</p> <p>If the port is a 40-Gbps QSFP+ interface, make sure the configuration does not exceed the interface limit. Each 40-Gbps QSFP+ interface can be split into four 10-Gigabit Ethernet interfaces, but because port 0 is reserved, so you can only configure an additional fifteen 10-Gigabit Ethernet interfaces.</p> <p>See <i>QFX3500 Device Overview</i>.</p>
	Cannot configure a 40-Gbps QSFP+ interface.	<p>The 40-Gbps QSFP+ interfaces can only be used as 10-Gigabit Ethernet interfaces. Each 40-Gbps QSFP+ interface can be split into four 10-Gigabit Ethernet interfaces using a breakout cable. However, port 0 is reserved, so you can only configure an additional fifteen 10-Gigabit Ethernet interfaces.</p> <p>See <i>QFX3500 Device Overview</i>.</p>
External devices (USB devices)	Upgrading software from a USB device results in an upgrade failure, and the system enters an invalid state.	Unplug the USB device and reboot the switch.
Initial device configuration	Cannot configure management Ethernet ports.	<p>Configure the management ports from the console port. You cannot configure the management ports by directly connecting to them.</p> <p><b>NOTE:</b> The management ports are on the front panel of the QFX3500 switch. They are labeled <b>C0</b> and <b>C1</b> on the front panel. In the CLI they are referred to as <b>me0</b> and <b>me1</b>.</p> <p>See <i>Configuring a QFX3500 Device as a Standalone Switch</i>.</p>

Table 12: Troubleshooting on the QFX Series (*continued*)

Problem Category	Symptom or Problem	Recommended Action
Software upgrade and configuration	Failed software upgrade.	See <i>Recovering from a Failed Software Installation</i> .
	Active partition becomes inactive after upgrade.	
	Problem with the active configuration file.	See the following topics: <ul style="list-style-type: none"> <li>• <i>Loading a Previous Configuration File</i></li> <li>• <i>Reverting to the Default Factory Configuration</i></li> <li>• <i>Reverting to the Rescue Configuration</i></li> <li>• <i>Performing a Recovery Installation</i></li> </ul>
	Root password is lost or forgotten.	Recover the root password. See <a href="#">"Recovering the Root Password" on page 20</a> .
Network interfaces	An aggregated Ethernet interface is down.	See <i>Troubleshooting an Aggregated Ethernet Interface</i> .
	Interface on built-in network port is down.	See <i>Troubleshooting Network Interfaces</i> .
	Interface on port in which SFP or SFP+ transceiver is installed in an SFP+ uplink module is down.	
Ethernet switching	A MAC address entry in the Ethernet switching table is not updated after the device with that MAC address has been moved from one interface to another on the switch.	See <i>Troubleshooting Ethernet Switching</i> .
Firewall filter	Firewall configuration exceeded available Ternary Content Addressable Memory (TCAM) space.	See <i>Troubleshooting Firewall Filters</i> .

## Recovering the Root Password

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



**NOTE:** The root password cannot be recovered on a QFabric system.



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

To recover the root password:

1. Power off the switch by switching off the AC power outlet of the device or, if necessary, by pulling the power cords out of the device's power supplies.
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 device into the RJ-45-to-DB-9 serial port adapter supplied with the device.
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 device.
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 device by (if necessary) plugging the power cords into the device's power supply, or turning on the power to the device by switching on the AC power outlet the device is plugged into.

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

10. When the following prompt appears, press the Spacebar to access the device's bootstrap loader command prompt:  
  
Hit [Enter] to boot immediately, or space bar for command prompt.  
Booting [kernel] in 9 seconds...
11. At the following prompt, enter **boot -s** to start up the system in single-user mode.  
  
ok **boot -s**
12. At the following prompt, enter **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. For example:  
  
user@switch# **set system root-authentication plain-text-password**
15. At the following prompt, enter the new root password. For example:  
  
New password: **test1**  
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, enter **y** to reboot the device.

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

**Related Documentation**

- *Configuring the Root Password*

## PART 3

# Configuring Authentication

- [Configuring and Managing Local Password Authentication on page 53](#)
- [Configuring and Managing TACACS+ Authentication on page 67](#)
- [Configuring and Managing RADIUS Authentication on page 79](#)
- [Configuring and Managing RADIUS Accounting on page 93](#)
- [Configuring and Managing RADIUS Template Accounts on page 109](#)
- [Configuring and Managing VSAs for RADIUS and TACACS+ on page 111](#)



## CHAPTER 5

# Configuring and Managing Local Password Authentication

- [Junos OS User Accounts Overview on page 53](#)
- [Junos OS User Authentication Methods on page 55](#)
- [Junos OS Login Classes Overview on page 55](#)
- [Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 56](#)
- [Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands on page 57](#)
- [Special Requirements for Junos OS Plain-Text Passwords on page 58](#)
- [Configuring Junos OS User Accounts on page 61](#)
- [Configuring a Local Administrator Account on page 61](#)
- [Example: Creating Login Classes with Specific Privileges on page 62](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 63](#)
- [Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 65](#)

### Junos OS User Accounts Overview

---

User accounts provide one way for users to access the switch. (Users can access the switch without accounts if you configured RADIUS or TACACS+ servers, as described in [“Junos OS User Authentication Methods” on page 14.](#)) 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—(Optional)** Name that identifies the user. It must be unique within the switch. 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.







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

**Table 14: Configuration Mode Hierarchies—Common Regular Expression Operators**

Operator	Match
	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. For example, (show system alarms) (show system software).
^	At the beginning of an expression, used to denote where the command begins, where there might be some ambiguity.
\$	Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, <b>allow-commands "show interfaces\$"</b> means that the user can issue the <b>show interfaces</b> command but cannot issue <b>show interfaces detail</b> or <b>show interfaces extensive</b> .
[ ]	Range of letters or digits. To separate the start and end of a range, use a hyphen ( - ).
( )	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.
*	Zero or more terms.
+	One or more terms.
.	Any character except for a space " ".

**Related Documentation**

- *Specifying Access Privileges for Junos OS Configuration Mode Hierarchies*

## Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands

Use extended regular expressions to specify which operational mode commands are denied or allowed. [Table 10 on page 37](#) lists common regular expression operators that can be used in the operational mode commands. Command regular expressions implement the extended (modern) regular expressions as defined in POSIX 1003.2.

**Table 15: Common Regular Expression Operators to Allow or Deny Operational Mode Commands**

Operator	Match
	One of two or more terms separated by the pipe ( ) symbol. Each term must be a complete standalone expression enclosed in parentheses ( ), with no spaces between the pipe and the adjacent parentheses. For example, ( <b>show system alarms</b> ) (show system software).
^	At the beginning of an expression, used to denote where the command begins, and where there might be some ambiguity.
\$	Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, <b>allow-commands "show interfaces\$"</b> means that the user can issue the <b>show interfaces</b> command but cannot issue the <b>show interfaces detail</b> or <b>show interfaces extensive</b> command.
[ ]	Range of letters or digits. To separate the start and end of a range, use a hyphen ( - ).
( )	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 always be used in conjunction with pipe operators as explained above.

If a regular expression contains a syntax error, it becomes invalid, and although the user can log in, the permission granted or denied by the regular expression does not take effect. When regular expressions configured on TACACS+ or RADIUS servers merge with regular expressions configured on the router or switch, if the final expression has a syntax error, the overall result is an invalid regular expression. If a regular expression does not contain any operators, all varieties of the command are allowed. For example, if the following statement is included in the configuration, the user can issue the commands **show interfaces detail** and **show interfaces extensive** in addition to showing an individual interface:

```
allow-commands "show interfaces";
```

#### Related Documentation

- *Specifying Access Privileges for Junos OS Operational Mode Commands*

## Special Requirements for Junos OS Plain-Text Passwords

Junos OS has special requirements when you create plain-text passwords on a router or switch. [Table 8 on page 34](#) shows the default requirements.

**Table 16: Special Requirements for Plain-Text Passwords**

Junos OS	Junos-FIPS
The password must be between 6 and 128 characters long.	FIPS passwords must be between 10 and 20 characters long



The **change-type** statement is optional. If you omit the **change-type** option, Junos-FIPS plain-text passwords are checked for character sets, and Junos OS plain-text passwords are checked for character set changes.

The **minimum-changes** statement specifies how many character sets or character set changes are required for the password. This statement is optional. If you do not use the **minimum-changes** statement, character sets are not checked for Junos OS. If the **change-type** statement is configured for the **character-set** option, then the **minimum-changes** value must be 5 or less, because Junos OS only supports five character sets.

The **format** statement specifies the hash algorithm (**md5**, **sha1**, **sha256**, **sha512** or **des**) for authenticating plain-text passwords. This statement is optional. For Junos OS, the default format is **md5**. For Junos-FIPS, only **sha1** is supported.



**NOTE:** Starting with Junos OS Release 13.3, the **sha1** does not enable secure, protected specification of passwords and we recommend that you do not use the **sha1** algorithm to configure passwords. Instead, you can use the **sha256** or **sha512** to specify passwords by using the 256-bit and 512-bit cryptographic hash algorithm respectively for a robust and reliable operation.

The **maximum-length** statement specifies the maximum number of characters allowed in a password. This statement is optional. By default, Junos OS passwords have no maximum; however, only the first 128 characters are significant. Junos-FIPS passwords must be 20 characters or less. The range for Junos OS maximum-length passwords is from 20 to 128 characters.

The **minimum-length** statement specifies the minimum number of characters required for a password. This statement is optional. By default, Junos OS passwords must be at least 6 characters long, and Junos-FIPS passwords must be at least 10 characters long. The range is from 6 to 20 characters.

Changes to password requirements do not take effect until the configuration is committed. When requirements change, only newly created, plain-text passwords are checked; existing passwords are not checked against the new requirements.

The default configuration for Junos OS plain-text passwords is:

```
[edit system login]
passwords {
  change-type character-sets;
  format md5;
  minimum-changes 1;
  minimum-length 6;
}
```

The default configuration for Junos-FIPS plain-text passwords is:

```
[edit system login]
passwords {
  change-type set-transitions;
  format sha1;
```

```

maximum-length 20;
minimum-changes 3;
minimum-length 10;
}

```

- Related Documentation**
- [Changing the Requirements for Junos OS Plain-Text Passwords](#)
  - [Configuring the Root Password](#)

## Configuring Junos OS User Accounts

User accounts provide one way for users to access the router or switch. 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.

To create user accounts, include the **user** statement at the **[edit system login]** hierarchy level:

```

[edit system login]
user username {
  class class-name;
  class {
    (encrypted-password "password" | plain-text-password);
    ssh-rsa "public-key";
    ssh-dsa "public-key";
  }
  full-name complete-name;
  uid uid-value;
  class class-name;
}

```

- Related Documentation**
- [Example: Configuring User Accounts on page 38](#)
  - [Configuring a Local Administrator Account on page 61](#)
  - [Junos OS User Accounts Overview on page 31](#)
  - [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)

## 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 33](#)
- [Configuring Junos OS User Accounts by Using a Configuration Group](#)

---

## 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 Login Classes Overview on page 33](#)
- [Defining Junos OS Login Classes](#)
- [Configuring a Local Administrator Account on page 61](#)

## 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 [“Using Local Password Authentication” on page 68](#).

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 [“Overview of Template Accounts for RADIUS and TACACS+ Authentication”](#) on page 109.

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”



### Configuring Requirements for Plain-Text Passwords

---

**Step-by-Step Procedure** This example configures password requirements that require the user to create 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-numeric 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-numeric 1;
minimum-upper-cases 1;
minimum-lower-cases 1;
```

- Related Documentation**
- [Special Requirements for Junos OS Plain-Text Passwords on page 34](#)
  - *password (Login)*

## CHAPTER 6

# Configuring and Managing TACACS+ Authentication

- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 67](#)
- [Configuring TACACS+ Authentication \(QFX Series\) on page 72](#)
- [Juniper Networks Vendor-Specific TACACS+ Attributes on page 74](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 76](#)

## 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 the **authentication-order** is remote-server then local, Junos OS will retry the local server if the remote-server is unreachable or has timed out. However, if the remote-server rejects the authentication, Junos OS will not retry the authentication.

If none of the configured authentication methods accept the login credentials and if a reject response is received, the login attempt fails. If no response is received from any configured authentication method, the Junos OS consults local password authentication as a last resort.

## 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 17 on page 69](#) 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 17: Order of Authentication Attempts

Syntax	Order of Authentication Attempts
<b>authentication-order radius;</b>	<ol style="list-style-type: none"> <li>1. Try configured RADIUS authentication servers.</li> <li>2. If RADIUS server is available and authentication is accepted, grant access.</li> <li>3. If RADIUS server is available but authentication is rejected, deny access.</li> <li>4. If RADIUS servers are not available, try password authentication.</li> </ol> <p><b>NOTE:</b> If a RADIUS server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
<b>authentication-order [ radius password ];</b>	<ol style="list-style-type: none"> <li>1. Try configured RADIUS authentication servers.</li> <li>2. If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.</li> </ol>
<b>authentication-order [ radius tacplus ];</b>	<ol style="list-style-type: none"> <li>1. Try configured RADIUS authentication servers.</li> <li>2. If RADIUS server is available and authentication is accepted, grant access.</li> <li>3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers.</li> <li>4. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>5. If TACACS+ server is available but authentication is rejected, deny access.</li> <li>6. If both RADIUS and TACACS+ servers are not available, try password authentication.</li> </ol> <p><b>NOTE:</b> If either RADIUS or TACACS+ servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
<b>authentication-order [ radius tacplus password ];</b>	<ol style="list-style-type: none"> <li>1. Try configured RADIUS authentication servers.</li> <li>2. If RADIUS server is available and authentication is accepted, grant access.</li> <li>3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers.</li> <li>4. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>5. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.</li> </ol>

Table 17: Order of Authentication Attempts (*continued*)

Syntax	Order of Authentication Attempts
<b>authentication-order tacplus;</b>	<ol style="list-style-type: none"> <li>1. Try configured TACACS+ authentication servers.</li> <li>2. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>3. If TACACS+ server is available but authentication is rejected, deny access.</li> <li>4. If TACACS+ servers are not available, try password authentication.</li> </ol> <p><b>NOTE:</b> If a TACACS+ server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
<b>authentication-order [ tacplus password ];</b>	<ol style="list-style-type: none"> <li>1. Try configured TACACS+ authentication servers.</li> <li>2. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.</li> </ol>
<b>authentication-order [ tacplus radius ];</b>	<ol style="list-style-type: none"> <li>1. Try configured TACACS+ authentication servers.</li> <li>2. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers.</li> <li>4. If RADIUS server is available and authentication is accepted, grant access.</li> <li>5. If RADIUS server is available but authentication is rejected, deny access.</li> <li>6. If both TACACS+ and RADIUS servers are not available, try password authentication.</li> </ol> <p><b>NOTE:</b> If either TACACS+ or RADIUS servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
<b>authentication-order [ tacplus radius password ];</b>	<ol style="list-style-type: none"> <li>1. Try configured TACACS+ authentication servers.</li> <li>2. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers.</li> <li>4. If RADIUS server is available and authentication is accepted, grant access.</li> <li>5. If RADIUS servers fail to respond or return a reject response try password authentication, because it is explicitly configured in the authentication order.</li> </ol>

Table 17: Order of Authentication Attempts (*continued*)

Syntax	Order of Authentication Attempts
<code>authentication-order password;</code>	<ol style="list-style-type: none"> <li>1. Try to authenticate the user, using the password configured at the <code>[edit system login]</code> hierarchy level.</li> <li>2. If the authentication is accepted, grant access.</li> <li>3. If the authentication is rejected, deny access.</li> </ol>



**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.

#### Related Documentation

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 109](#)
- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 63](#)





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. 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 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 = "<allow-configuration-regex>"
  deny-commands = "<deny-commands-regex>"
  deny-configuration = "<deny-configuration-regex>"
}
```

This **service** statement can appear in a **user** or **group** statement.

### Related Documentation

- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 86](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 63](#)
- [Juniper Networks Vendor-Specific TACACS+ Attributes on page 74](#)
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 109](#)
- [Junos OS User Authentication Methods on page 14](#)

---

## 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 18 on page 75](#) lists the Juniper Networks VSAs you can configure.



Table 18: Juniper Networks Vendor-Specific TACACS+ Attributes (*continued*)

Name	Description	Length	String
<b>session-port</b>	Indicates the source port number of the established session.	size of integer	Integer

**Related Documentation**

- *Configuring TACACS+ Authentication*

### 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 [“Using Local Password Authentication” on page 68](#).

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;
    }
  }
}
```



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.

- Related Documentation**
- *Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication*

## CHAPTER 7

# Configuring and Managing RADIUS Authentication

- Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 79
- Configuring RADIUS Authentication (QFX Series or OCX Series) on page 83
- Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 86
- Example: Configuring RADIUS Authentication on page 88
- Example: Configuring RADIUS Template Accounts on page 89
- Configuring a Local Administrator Account on page 89
- Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 90

### 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 the **authentication-order** is remote-server then local, Junos OS will retry the local server if the remote-server is unreachable or has timed out. However, if the remote-server rejects the authentication, Junos OS will not retry the authentication.

If none of the configured authentication methods accept the login credentials and if a reject response is received, the login attempt fails. If no response is received from any configured authentication method, the Junos OS consults local password authentication as a last resort.

### 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 17 on page 69](#) 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 19: Order of Authentication Attempts

Syntax	Order of Authentication Attempts
<b>authentication-order radius;</b>	<ol style="list-style-type: none"> <li>1. Try configured RADIUS authentication servers.</li> <li>2. If RADIUS server is available and authentication is accepted, grant access.</li> <li>3. If RADIUS server is available but authentication is rejected, deny access.</li> <li>4. If RADIUS servers are not available, try password authentication.</li> </ol> <p><b>NOTE:</b> If a RADIUS server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
<b>authentication-order [ radius password ];</b>	<ol style="list-style-type: none"> <li>1. Try configured RADIUS authentication servers.</li> <li>2. If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.</li> </ol>
<b>authentication-order [ radius tacplus ];</b>	<ol style="list-style-type: none"> <li>1. Try configured RADIUS authentication servers.</li> <li>2. If RADIUS server is available and authentication is accepted, grant access.</li> <li>3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers.</li> <li>4. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>5. If TACACS+ server is available but authentication is rejected, deny access.</li> <li>6. If both RADIUS and TACACS+ servers are not available, try password authentication.</li> </ol> <p><b>NOTE:</b> If either RADIUS or TACACS+ servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
<b>authentication-order [ radius tacplus password ];</b>	<ol style="list-style-type: none"> <li>1. Try configured RADIUS authentication servers.</li> <li>2. If RADIUS server is available and authentication is accepted, grant access.</li> <li>3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers.</li> <li>4. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>5. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.</li> </ol>

Table 19: Order of Authentication Attempts (*continued*)

Syntax	Order of Authentication Attempts
<b>authentication-order tacplus;</b>	<ol style="list-style-type: none"> <li>1. Try configured TACACS+ authentication servers.</li> <li>2. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>3. If TACACS+ server is available but authentication is rejected, deny access.</li> <li>4. If TACACS+ servers are not available, try password authentication.</li> </ol> <p><b>NOTE:</b> If a TACACS+ server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
<b>authentication-order [ tacplus password ];</b>	<ol style="list-style-type: none"> <li>1. Try configured TACACS+ authentication servers.</li> <li>2. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.</li> </ol>
<b>authentication-order [ tacplus radius ];</b>	<ol style="list-style-type: none"> <li>1. Try configured TACACS+ authentication servers.</li> <li>2. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers.</li> <li>4. If RADIUS server is available and authentication is accepted, grant access.</li> <li>5. If RADIUS server is available but authentication is rejected, deny access.</li> <li>6. If both TACACS+ and RADIUS servers are not available, try password authentication.</li> </ol> <p><b>NOTE:</b> If either TACACS+ or RADIUS servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
<b>authentication-order [ tacplus radius password ];</b>	<ol style="list-style-type: none"> <li>1. Try configured TACACS+ authentication servers.</li> <li>2. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers.</li> <li>4. If RADIUS server is available and authentication is accepted, grant access.</li> <li>5. If RADIUS servers fail to respond or return a reject response try password authentication, because it is explicitly configured in the authentication order.</li> </ol>

Table 19: Order of Authentication Attempts (*continued*)

Syntax	Order of Authentication Attempts
<code>authentication-order password;</code>	<ol style="list-style-type: none"> <li>1. Try to authenticate the user, using the password configured at the <code>[edit system login]</code> hierarchy level.</li> <li>2. If the authentication is accepted, grant access.</li> <li>3. If the authentication is rejected, deny access.</li> </ol>



**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.

#### Related Documentation

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 109](#)
- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 63](#)

## 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 84](#)
- [Configuring MS-CHAPv2 for Password-Change Support on page 85](#)
- [Specifying a Source Address for the Junos OS to Access External RADIUS Servers on page 86](#)

## 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 [“Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 109](#).

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.

### Related Documentation

- [Example: Configuring RADIUS Authentication on page 88](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 63](#)
- [Juniper Networks Vendor-Specific RADIUS Attributes on page 98](#)
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 109](#)
- [Example: Configuring RADIUS Template Accounts on page 89](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 86](#)
- [Junos OS User Authentication Methods on page 14](#)

---

## 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.

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 | cmdn)**. You can specify **user-permissions** as a list of comma-separated values, and not as a regular expression.

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 98](#) and [“Juniper Networks Vendor-Specific TACACS+ Attributes” on page 74](#).



**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.

**Related  
Documentation**

- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 67](#)

---

## 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;
    }
  }
}

```

**Related Documentation**

- [Configuring RADIUS Server Authentication](#)

## Example: Configuring RADIUS Template Accounts

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;
    }
  }
}

```

**Related Documentation**

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 109](#)

## 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 33](#)
  - [Configuring Junos OS User Accounts by Using a Configuration Group](#)

---

## 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 [“Using Local Password Authentication” on page 68](#).

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 [“Overview of Template Accounts for RADIUS and TACACS+ Authentication”](#) on page 109.

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.

- Related Documentation**
- *Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication*

## CHAPTER 8

# Configuring and Managing RADIUS Accounting

- [Understanding RADIUS Accounting on page 93](#)
- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 94](#)
- [Juniper Networks Vendor-Specific RADIUS Attributes on page 98](#)
- [Configuring RADIUS System Accounting on page 101](#)
- [Configuring RADIUS Authentication \(QFX Series or OCX Series\) on page 103](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 106](#)
- [Example: Configuring RADIUS System Accounting on page 108](#)

## 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, 122.69.1.250.
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.

**Related Documentation** • [Configuring RADIUS System Accounting on page 101](#)

## 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 the **authentication-order** is remote-server then local, Junos OS will retry the local server if the remote-server is unreachable or has timed out. However, if the remote-server rejects the authentication, Junos OS will not retry the authentication.

If none of the configured authentication methods accept the login credentials and if a reject response is received, the login attempt fails. If no response is received from any configured authentication method, the Junos OS consults local password authentication as a last resort.

### 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 17 on page 69](#) 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 20: Order of Authentication Attempts

Syntax	Order of Authentication Attempts
<b>authentication-order radius;</b>	<ol style="list-style-type: none"> <li>1. Try configured RADIUS authentication servers.</li> <li>2. If RADIUS server is available and authentication is accepted, grant access.</li> <li>3. If RADIUS server is available but authentication is rejected, deny access.</li> <li>4. If RADIUS servers are not available, try password authentication.</li> </ol> <p><b>NOTE:</b> If a RADIUS server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
<b>authentication-order [ radius password ];</b>	<ol style="list-style-type: none"> <li>1. Try configured RADIUS authentication servers.</li> <li>2. If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.</li> </ol>
<b>authentication-order [ radius tacplus ];</b>	<ol style="list-style-type: none"> <li>1. Try configured RADIUS authentication servers.</li> <li>2. If RADIUS server is available and authentication is accepted, grant access.</li> <li>3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers.</li> <li>4. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>5. If TACACS+ server is available but authentication is rejected, deny access.</li> <li>6. If both RADIUS and TACACS+ servers are not available, try password authentication.</li> </ol> <p><b>NOTE:</b> If either RADIUS or TACACS+ servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
<b>authentication-order [ radius tacplus password ];</b>	<ol style="list-style-type: none"> <li>1. Try configured RADIUS authentication servers.</li> <li>2. If RADIUS server is available and authentication is accepted, grant access.</li> <li>3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers.</li> <li>4. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>5. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.</li> </ol>

Table 20: Order of Authentication Attempts (*continued*)

Syntax	Order of Authentication Attempts
<b>authentication-order tacplus;</b>	<ol style="list-style-type: none"> <li>1. Try configured TACACS+ authentication servers.</li> <li>2. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>3. If TACACS+ server is available but authentication is rejected, deny access.</li> <li>4. If TACACS+ servers are not available, try password authentication.</li> </ol> <p><b>NOTE:</b> If a TACACS+ server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
<b>authentication-order [ tacplus password ];</b>	<ol style="list-style-type: none"> <li>1. Try configured TACACS+ authentication servers.</li> <li>2. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.</li> </ol>
<b>authentication-order [ tacplus radius ];</b>	<ol style="list-style-type: none"> <li>1. Try configured TACACS+ authentication servers.</li> <li>2. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers.</li> <li>4. If RADIUS server is available and authentication is accepted, grant access.</li> <li>5. If RADIUS server is available but authentication is rejected, deny access.</li> <li>6. If both TACACS+ and RADIUS servers are not available, try password authentication.</li> </ol> <p><b>NOTE:</b> If either TACACS+ or RADIUS servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
<b>authentication-order [ tacplus radius password ];</b>	<ol style="list-style-type: none"> <li>1. Try configured TACACS+ authentication servers.</li> <li>2. If TACACS+ server is available and authentication is accepted, grant access.</li> <li>3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers.</li> <li>4. If RADIUS server is available and authentication is accepted, grant access.</li> <li>5. If RADIUS servers fail to respond or return a reject response try password authentication, because it is explicitly configured in the authentication order.</li> </ol>

Table 20: Order of Authentication Attempts (*continued*)

Syntax	Order of Authentication Attempts
<code>authentication-order password;</code>	<ol style="list-style-type: none"> <li>1. Try to authenticate the user, using the password configured at the <code>[edit system login]</code> hierarchy level.</li> <li>2. If the authentication is accepted, grant access.</li> <li>3. If the authentication is rejected, deny access.</li> </ol>



**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.

#### Related Documentation

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 109](#)
- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 63](#)

## 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 21 on page 99](#) lists the Juniper Networks VSAs you can configure.

**Table 21: 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.
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 <a href="#">"Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands"</a> on page 37.
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 <a href="#">"Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands"</a> on page 37.
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 <a href="#">"Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies"</a> on page 36.
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 <a href="#">"Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies"</a> on page 36.
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.

Table 21: Juniper Networks Vendor-Specific RADIUS Attributes (*continued*)

Name	Description	Type	Length	String
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	<p>Contains information the server uses to specify user permissions. This attribute is used only in Access-Accept packets.</p> <p><b>NOTE:</b> When the <b>Juniper-User-Permissions</b> attribute is configured to grant the Junos OS <b>maintenance</b> or <b>all</b> 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 <b>su root</b> command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions <b>maintenance</b> or <b>all</b>, 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.</p>	10	≥3	<p>One or more octets containing printable ASCII characters.</p> <p>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 <a href="#">Table 4 on page 10</a>.</p>
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.
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)*.

**Related Documentation**

- [Configuring RADIUS Server Authentication](#)

## 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 101](#)
2. [Specifying RADIUS Server Accounting and Auditing Events on page 101](#)
3. [Configuring RADIUS Server Accounting on page 102](#)

### 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]
destination {
  radius {
    server {
      server-address {
        accounting-port port-number;
        max-outstanding-requests value;
        port port-number;
        retry value;
        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;  
    max-outstanding-requests value;  
    port port-number;  
    retry value;  
    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.

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.

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;
        }
      }
    }
  }
}
```

## 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 104](#)
- [Configuring MS-CHAPv2 for Password-Change Support on page 105](#)
- [Specifying a Source Address for the Junos OS to Access External RADIUS Servers on page 106](#)

## 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 [“Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 109](#).

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.

### Related Documentation

- [Example: Configuring RADIUS Authentication on page 88](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 63](#)
- [Juniper Networks Vendor-Specific RADIUS Attributes on page 98](#)
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 109](#)
- [Example: Configuring RADIUS Template Accounts on page 89](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 86](#)
- [Junos OS User Authentication Methods on page 14](#)

---

## 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.

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 | cmdn)**. You can specify **user-permissions** as a list of comma-separated values, and not as a regular expression.

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 98](#) and [“Juniper Networks Vendor-Specific TACACS+ Attributes” on page 74](#).



**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.

**Related  
Documentation**

- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 67](#)

---

## Example: Configuring RADIUS System Accounting

---

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;
        }
      }
    }
  }
}
```

**Related  
Documentation**

- [Configuring RADIUS System Accounting on page 101](#)

## CHAPTER 9

# Configuring and Managing RADIUS Template Accounts

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 109](#)
- [Example: Configuring RADIUS Template Accounts on page 109](#)

## Overview of Template Accounts for RADIUS and TACACS+ Authentication

---

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.

### Related Documentation

- *[Understanding Remote Authentication Servers](#)*
- *[Configuring Remote Template Accounts for User Authentication](#)*
- *[Configuring Local User Template Accounts for User Authentication](#)*

## Example: Configuring RADIUS Template Accounts

---

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;  
    }  
}  
}
```

**Related Documentation**

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 109](#)

## CHAPTER 10

# Configuring and Managing VSAs for RADIUS and TACACS+

- [Understanding Vendor-Specific Attributes \(VSAs\) on page 111](#)
- [Juniper-Switching-Filter VSA Match Conditions and Actions on page 112](#)
- [Juniper Networks Vendor-Specific TACACS+ Attributes on page 114](#)

### Understanding Vendor-Specific Attributes (VSAs)

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.

#### **Related Documentation**

- [Configuring Firewall Filters](#)
- [Configuring RADIUS Authentication \(QFX Series or OCX Series\) on page 83](#)
- [Juniper-Switching-Filter VSA Match Conditions and Actions on page 112](#)

## Juniper-Switching-Filter VSA Match Conditions and Actions

Switching devices support the configuration of RADIUS server attributes specific to Juniper Networks, which are known as vendor-specific attributes (VSAs). 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 22 on page 112 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 22: Match Conditions

Option	Description
<b>destination-mac</b> <i>mac-address</i>	Destination media access control (MAC) address of the packet.
<b>source-vlan</b> <i>source-vlan</i>	Name of the source VLAN.
<b>source-dot1q-tag</b> <i>tag</i>	Tag value in the 802.1Q header, in the range 0 through 4095.
<b>destination-ip</b> <i>ip-address</i>	Address of the final destination node.
<b>ip-protocol</b> <i>protocol-id</i>	IPv4 protocol value. In place of the numeric value, you can specify one of the following text synonyms:  <b>ah</b> , <b>egp</b> (8), <b>esp</b> (50), <b>gre</b> (47), <b>icmp</b> (1), <b>igmp</b> (2), <b>ipip</b> (4), <b>ipv6</b> (41), <b>ospf</b> (89), <b>pim</b> (103), <b>rsvp</b> (46), <b>tcp</b> (6), or <b>udp</b> (17)

Table 22: Match Conditions (*continued*)

Option	Description
<b>source-port</b> <i>port</i>	TCP or User Datagram Protocol (UDP) source port field. Normally, you specify this match statement in conjunction with the <b>ip-protocol</b> 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 <b>destination-port</b> .
<b>destination-port</b> <i>port</i>	<p>TCP or UDP destination port field. Normally, you specify this match statement in conjunction with the <b>ip-protocol</b> 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):</p> <p>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)</p>

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 23 on page 113](#) shows the actions that you can specify in a term.

Table 23: Actions for VSAs

Option	Description
(allow   deny)	Accept a packet or discard a packet silently without sending an Internet Control Message Protocol (ICMP) message.
<b>forwarding-class</b> <i>class-of-service</i>	<p>(Optional) Classify the packet in one of the following forwarding classes:</p> <ul style="list-style-type: none"> <li>assured-forwarding</li> <li>best-effort</li> <li>expedited-forwarding</li> <li>network-control</li> </ul>
<b>loss-priority</b> (low   medium   high)	(Optional) Set the packet loss priority (PLP) to <b>low</b> , <b>medium</b> , or <b>high</b> . Specify both the forwarding class and the loss priority.

#### Related Documentation

- Filtering 802.1X Supplicants by Using RADIUS Server Attributes
- Understanding Dynamic Filters Based on RADIUS Attributes
- Understanding Vendor-Specific Attributes (VSAs) on page 111

## 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 18 on page 75](#) lists the Juniper Networks VSAs you can configure.

**Table 24: Juniper Networks Vendor-Specific TACACS+ Attributes**

Name	Description	Length	String
<b>local-user-name</b>	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.
<b>allow-commands</b>	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 <a href="#">Table 10 on page 37</a> .
<b>allow-configuration</b>	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 Configuration Mode Hierarchies" on page 36.
<b>deny-commands</b>	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 <a href="#">Table 10 on page 37</a> .
<b>deny-configuration</b>	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 <a href="#">Table 9 on page 37</a> .

Table 24: Juniper Networks Vendor-Specific TACACS+ Attributes (*continued*)

Name	Description	Length	String
<b>user-permissions</b>	<p>Contains information the server uses to specify user permissions.</p> <p><b>NOTE:</b> When the <b>user-permissions</b> attribute is configured to grant the Junos OS <b>maintenance</b> or <b>all</b> 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 <b>su root</b> command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions <b>maintenance</b> or <b>all</b>, 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.</p>	≥3	One or more octets containing printable ASCII characters. See <a href="#">Table 4 on page 10</a> .
<b>authentication-type</b>	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.
<b>session-port</b>	Indicates the source port number of the established session.	size of integer	Integer

**Related Documentation**

- *Configuring TACACS+ Authentication*



## PART 4

# Configuration Statements and Operational Commands

- [Configuration Statements on page 119](#)
- [Operational Commands on page 203](#)



## CHAPTER 11

# Configuration Statements

- [access](#) on page 121
- [accounting \(Access Profile\)](#) on page 122
- [accounting-options](#) on page 123
- [accounting-server](#) on page 125
- [accounting-stop-on-access-deny](#) on page 126
- [accounting-stop-on-failure](#) on page 127
- [advertisement-interval](#) on page 128
- [agent-address](#) on page 129
- [archival](#) on page 130
- [archive-sites \(Configuration File\)](#) on page 131
- [authentication-order](#) on page 132
- [authentication-server](#) on page 133
- [authorization](#) on page 134
- [categories](#) on page 135
- [client-list](#) on page 135
- [client-list-name](#) on page 136
- [clients](#) on page 136
- [commit-delay](#) on page 137
- [community \(SNMP\)](#) on page 138
- [configuration](#) on page 139
- [connection-limit](#) on page 140
- [contact](#) on page 141
- [disable \(LLDP\)](#) on page 141
- [falling-threshold \(Health Monitor\)](#) on page 142
- [filter-duplicates](#) on page 142
- [full-name](#) on page 143
- [health-monitor](#) on page 143
- [hold-multiplier](#) on page 144

- [idle-timeout \(Access\) on page 145](#)
- [interface \(LLDP\) on page 146](#)
- [interval \(Health Monitor\) on page 147](#)
- [lldp on page 148](#)
- [lldp-configuration-notification-interval on page 150](#)
- [location on page 150](#)
- [management-address on page 151](#)
- [name on page 152](#)
- [nas-ip-address on page 152](#)
- [nonvolatile on page 153](#)
- [oid on page 153](#)
- [order on page 154](#)
- [port \(RADIUS Server\) on page 155](#)
- [profile on page 156](#)
- [protocols on page 157](#)
- [protocol-version on page 170](#)
- [ptopo-configuration-maximum-hold-time on page 171](#)
- [ptopo-configuration-trap-interval on page 171](#)
- [radius on page 172](#)
- [radius-options \(edit system\) on page 173](#)
- [radius-server on page 174](#)
- [rate-limit on page 175](#)
- [remote-debug-permission on page 176](#)
- [retry on page 177](#)
- [rising-threshold \(Health Monitor\) on page 178](#)
- [root-login on page 179](#)
- [services \(Switches\) on page 180](#)
- [snmp on page 181](#)
- [ssh on page 185](#)
- [system on page 186](#)
- [tacplus-options on page 192](#)
- [targets on page 193](#)
- [traceoptions \(LLDP\) on page 194](#)
- [transfer-interval \(Configuration\) on page 196](#)
- [transfer-on-commit on page 197](#)
- [trap-group on page 198](#)
- [trap-options on page 199](#)

- [user \(Access\)](#) on page 200
- [version](#) on page 201

## access

<b>Syntax</b>	<pre> access {   address-assignment   pool <i>pool-name</i>   address-pool <i>pool-name</i>   profile <i>profile-name</i> {     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 [<i>server-addresses</i>];       authentication-server [<i>server-addresses</i>];     }   } } </pre>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p>
<b>Description</b>	<p>Configure authentication, authorization, and accounting (AAA) services.</p> <p>The statements are explained separately.</p>
<div>  <b>NOTE:</b> The [edit access] hierarchy is not available on QFabric systems. </div>	
<b>Default</b>	Not enabled
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring 802.1X RADIUS Accounting (CLI Procedure)</a></li> </ul>

## accounting (Access Profile)

---

<b>Syntax</b>	<pre>accounting {     accounting-stop-on-access-deny;     accounting-stop-on-failure;     order (radius   none); }</pre>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> ]
<b>Release Information</b>	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.
<b>Description</b>	Configure the authentication order for authentication, authorization, and accounting (AAA) services.
<b>Default</b>	Not enabled
<b>Options</b>	<b>none</b> —Use no authentication for specified subscribers.  <b>radius</b> —Use RADIUS authentication for specified subscribers.  The remaining statements are explained separately.



**NOTE:** The [edit access] hierarchy is not available on QFabric systems.

---

<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch</i></li><li>• <i>Configuring 802.1X RADIUS Accounting (CLI Procedure)</i></li><li>• <i>Understanding 802.1X and RADIUS Accounting on EX Series Switches</i></li><li>• <i>Configuring RADIUS Accounting</i></li><li>• <a href="#">Understanding RADIUS Accounting on page 93</a></li></ul>

## 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	<ul style="list-style-type: none"><li>• <a href="#">Understanding RADIUS Accounting on page 93</a></li><li>• <a href="#">Understanding Vendor-Specific Attributes (VSAs) on page 111</a></li><li>• <a href="#">Configuring RADIUS System Accounting on page 101</a></li><li>• <i>Configuring Remote Template Accounts for User Authentication</i></li><li>• <i>Configuring Local User Template Accounts for User Authentication</i></li></ul>

## accounting-server

<b>Syntax</b>	<code>accounting-server[server-addresses];</code>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius]
<b>Release Information</b>	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.
<b>Description</b>	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.
<b>Default</b>	Not enabled
<b>Options</b>	<i>server-addresses</i> —One or more addresses of RADIUS authentication servers.



**NOTE:** The [edit access] hierarchy is not available on QFabric systems.

<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>show network-access aaa statistics authentication</i></li> <li><i>Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch</i></li> <li><i>Understanding 802.1X and RADIUS Accounting on EX Series Switches</i></li> <li><a href="#">Understanding RADIUS Accounting on page 93</a></li> </ul>

## accounting-stop-on-access-deny

---

<b>Syntax</b>	accounting-stop-on-access-deny;
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> accounting]
<b>Release Information</b>	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.
<b>Description</b>	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.

---

<b>Default</b>	Not enabled
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch</i></li><li>• <i>Configuring 802.1X RADIUS Accounting (CLI Procedure)</i></li><li>• <i>show network-access aaa statistics authentication</i></li><li>• <i>Configuring RADIUS Accounting</i></li></ul>

## accounting-stop-on-failure

<b>Syntax</b>	accounting-stop-on-failure;
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> accounting]
<b>Release Information</b>	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.
<b>Description</b>	<p>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.</p> <p>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 <b>acct-stop-on-failure</b> 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.</p>
	<p> <b>NOTE:</b> The [edit access] hierarchy is not available on QFabric systems.</p>
<b>Default</b>	Not enabled
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch</i></li> <li>• <i>Configuring 802.1X RADIUS Accounting (CLI Procedure)</i></li> <li>• <i>Understanding 802.1X and RADIUS Accounting on EX Series Switches</i></li> <li>• <i>Configuring RADIUS Accounting</i></li> <li>• <a href="#">Understanding RADIUS Accounting on page 93</a></li> </ul>

## advertisement-interval

---

<b>Syntax</b>	<code>advertisement-interval seconds;</code>
<b>Hierarchy Level</b>	[edit protocols lldp], [edit routing-instances <i>routing-instance-name</i> protocols lldp]
<b>Release Information</b>	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.
<b>Description</b>	(MX Series and T Series routers only) Configure an interval for LLDP advertisement.
<b>Options</b>	<b>seconds</b> —Interval between LLDP advertisement. <b>Default:</b> 30 <b>Range:</b> 5 through 32768
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring LLDP</i></li><li>• <a href="#">show lldp on page 212</a></li><li>• <i>Configuring LLDP (CLI Procedure)</i></li><li>• <i>Understanding LLDP and LLDP-MED on EX Series Switches</i></li><li>• <i>transmit-delay</i></li><li>• <a href="#">Understanding LLDP on page 5</a></li></ul>


---

## agent-address



---

<b>Syntax</b>	agent-address outgoing-interface;
<b>Hierarchy Level</b>	[edit snmp trap-options]
<b>Release Information</b>	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.
<b>Description</b>	Set the agent address of all SNMPv1 traps generated by this router or switch. Currently, the only option is <b>outgoing-interface</b> , which sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.
<b>Options</b>	<b>outgoing-interface</b> —Value of the agent address of all SNMPv1 traps generated by this router or switch. The <b>outgoing-interface</b> option sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap. <b>Default:</b> Disabled (the agent address is not specified in SNMPv1 traps).
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Agent Address for SNMP Traps</i></li></ul>

## archival

<b>Syntax</b>	<pre> archival {   configuration {     archive-sites {       file://&lt;path&gt;/&lt;filename&gt;;       ftp://username@host:&lt;port&gt;url-path password password;       http://username@host:&lt;port&gt;url-path password password;       pasvftp://username@host:&lt;port&gt;url-path password password;       scp://username@host:&lt;port&gt;url-path password password;     }     transfer-interval interval;     transfer-on-commit;   } } </pre>
<b>Hierarchy Level</b>	[edit system]
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p>
<b>Description</b>	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.
<b>Options</b>	The remaining statements are explained separately.
<div style="display: flex; align-items: center;">  <div> <p><b>NOTE:</b> The [edit system archival] hierarchy is not available on QFabric systems.</p> </div> </div>	
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site</i></li> </ul>

## archive-sites (Configuration File)

<b>Syntax</b>	<pre>archive-sites {     file://&lt;path&gt;/&lt;filename&gt;;     ftp://username@host:&lt;port&gt;url-path password password;     http://username@host:&lt;port&gt;url-path password password;     pasvftp://username@host:&lt;port&gt;url-path password password;     scp://username@host:&lt;port&gt;url-path password password; }</pre>
<b>Hierarchy Level</b>	[edit system archival configuration]
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p>
<b>Description</b>	<p>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&lt;:password&gt;@[ipv6-host-address]&lt;:port&gt;/url-path"</p> <p>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.</p> <p>The destination filename is saved in the following format, where <i>n</i> corresponds to the number of the compressed configuration rollback file that has been archived:</p> <p><i>router-name_YYYYMMDD_HHMMSS_juniper.conf.n.gz</i></p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> <b>NOTE:</b> 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.</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> <b>NOTE:</b> The [edit system archival] hierarchy is not available on QFabric systems.</p> </div>
<b>Options</b>	<p>The prefix used in the configuration statement determines the form of transfer:</p> <p><b>file://</b> —transfer on a path to a named file</p> <p><b>ftp://</b> —transfer using active FTP server</p> <p><b>http://</b> —transfer using HTTP server</p>

**pasvftp://** —transfer to a device that only accepts passive FTP services

**scp://** —transfer to a known host using background SCP file transfers

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

**Related Documentation**

- *Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site*
- *Junos OS Commit Model for Router or Switch Configuration*
- [configuration on page 139](#)
- [transfer-on-commit on page 197](#)

---

## 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-server

---

<b>Syntax</b>	<code>authentication-server [server-addresses];</code>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius]
<b>Release Information</b>	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.
<b>Description</b>	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.
<b>Options</b>	<b>server-addresses</b> —Configure one or more RADIUS server addresses.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch</i></li><li>• <i>show network-access aaa statistics authentication</i></li></ul>

## authorization

---

<b>Syntax</b>	<code>authorization <i>authorization</i>;</code>
<b>Hierarchy Level</b>	[edit snmp community <i>community-name</i> ]
<b>Release Information</b>	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.
<b>Description</b>	Set the access authorization for SNMP <b>Get</b> , <b>GetBulk</b> , <b>GetNext</b> , and <b>Set</b> requests.
<b>Options</b>	<p><i>authorization</i>—Access authorization level:</p> <ul style="list-style-type: none"><li>• <b>read-only</b>—Enable <b>Get</b>, <b>GetNext</b>, and <b>GetBulk</b> requests.</li><li>• <b>read-write</b>—Enable all requests, including <b>Set</b> requests. You must configure a view to enable <b>Set</b> requests.</li></ul>
	<div> <b>NOTE:</b> The read-write option is not supported on the QFX3000 QFabric system.</div>
	<b>Default:</b> read-only
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the SNMP Community String</i></li></ul>

## categories

<b>Syntax</b>	<pre>categories {     category; }</pre>
<b>Hierarchy Level</b>	[edit snmp trap-group <i>group-name</i> ]
<b>Release Information</b>	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.
<b>Description</b>	Define the types of traps that are sent to the targets of the named trap group.
<b>Default</b>	If you omit the <b>categories</b> statement, all trap types are included in trap notifications.
<b>Options</b>	<b>category</b> —Name of a trap type: <b>authentication</b> , <b>chassis</b> , <b>configuration</b> , <b>link</b> , <b>remote-operations</b> , <b>rmon-alarm</b> , or <b>startup</b> .
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring SNMP Trap Groups</i></li> </ul>

## client-list

<b>Syntax</b>	<pre>client-list <i>client-list-name</i> {     ip-addresses; }</pre>
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	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.
<b>Description</b>	Define a list of SNMP clients.
<b>Options</b>	<b>client-list-name</b> —Name of the client list.  <b>ip-addresses</b> —IP addresses of the SNMP clients to be added to the client list,
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Adding a Group of Clients to an SNMP Community</i></li> </ul>

## client-list-name

---

<b>Syntax</b>	<code>client-list-name <i>client-list-name</i>;</code>
<b>Hierarchy Level</b>	[edit snmp community <i>community-name</i> ]
<b>Release Information</b>	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.
<b>Description</b>	Add a client list or prefix list to an SNMP community.
<b>Options</b>	<i>client-list-name</i> —Name of the client list or prefix list.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Adding a Group of Clients to an SNMP Community</i></li></ul>

## clients

---

<b>Syntax</b>	<pre>clients {     <i>address</i> &lt;restrict&gt;; }</pre>
<b>Hierarchy Level</b>	[edit snmp community <i>community-name</i> ]
<b>Release Information</b>	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.
<b>Description</b>	Specify the IPv4 or IPv6 addresses of the SNMP client hosts that are authorized to use this community.
<b>Default</b>	If you omit the <b>clients</b> statement, all SNMP clients using this community string are authorized to access the switch.
<b>Options</b>	<i>address</i> —Address of an SNMP client that is authorized to access this switch. You must specify an address, not a hostname. To specify more than one client, include multiple <i>address</i> options.  <i>restrict</i> —(Optional) Do not allow the specified SNMP client to access the switch.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring SNMP Communities</i></li></ul>


## commit-delay

---


<b>Syntax</b>	commit-delay <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit snmp nonvolatile]
<b>Release Information</b>	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.
<b>Description</b>	Configure the timer for the SNMP <b>Set</b> reply and start of the commit.
<b>Options</b>	<b><i>seconds</i></b> —Delay between an affirmative SNMP <b>Set</b> reply and start of the commit operation. <b>Default:</b> 5 seconds
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Commit Delay Timer</i></li></ul>

## community (SNMP)

---

<b>Syntax</b>	<pre>community <i>community-name</i> {     authorization <i>authorization</i>;     client-list-name <i>client-list-name</i>;     clients {         address restrict;     }     view <i>view-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	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.
<b>Description</b>	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.
<div> <b>NOTE:</b> The <b>authorization read-write</b> option is not supported on the QFX3000 QFabric system.</div>	
The SNMP client application specifies an SNMP community name in <b>Get</b> , <b>GetBulk</b> , <b>GetNext</b> , and <b>Set</b> SNMP requests.	
<b>Default</b>	If you omit the <b>community</b> statement, all SNMP requests are denied.
<b>Options</b>	<b><i>community-name</i></b> —Community string. If the name includes spaces, enclose it in quotation marks (" ").  The remaining statements are explained separately.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li><i>Configuring the SNMP Community String</i></li></ul>

## configuration

<b>Syntax</b>	<pre>configuration {   transfer-interval interval;   transfer-on-commit;   archive-sites {     file://&lt;path&gt;/&lt;filename&gt;;     ftp://username@host:&lt;port&gt;url-path password password;     http://username@host:&lt;port&gt;url-path password password;     pasvftp://username@host:&lt;port&gt;url-path password password;     scp://username@host:&lt;port&gt;url-path password password;   } }</pre>
<b>Hierarchy Level</b>	[edit system archival]
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p>
<b>Description</b>	Configure the router or switch to periodically transfer its currently active configuration (or after each commit).
<div>  <p><b>NOTE:</b> The [edit system archival] hierarchy is not available on QFabric systems.</p> </div>	
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site</i></li> <li>• <i>archive</i></li> <li>• <a href="#">archive-sites on page 131</a></li> <li>• <a href="#">transfer-interval on page 196</a></li> <li>• <a href="#">transfer-on-commit on page 197</a></li> </ul>

## connection-limit

<b>Syntax</b>	<code>connection-limit <i>limit</i>;</code>
<b>Hierarchy Level</b>	<code>[edit system services finger],</code> <code>[edit system services ftp],</code> <code>[edit system services netconf ssh],</code> <code>[edit system services ssh],</code> <code>[edit system services telnet],</code> <code>[edit system services xnm-clear-text],</code> <code>[edit system services xnm-ssl]</code>
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
<b>Description</b>	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).
<b>Options</b>	<p><b>limit</b>—(Optional) Maximum number of established connections per protocol (either IPv6 or IPv4).</p> <p><b>Range:</b> 1 through 250</p> <p><b>Default:</b> 75</p>



**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.

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

<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring clear-text or SSL Service for Junos XML Protocol Client Applications</i></li> <li>• <i>Configuring DTCP-over-SSH Service for the Flow-Tap Application</i></li> <li>• <i>Configuring Finger Service for Remote Access to the Router</i></li> <li>• <i>Configuring FTP Service for Remote Access to the Router or Switch</i></li> <li>• <i>Configuring SSH Service for Remote Access to the Router or Switch</i></li> <li>• <i>Configuring Telnet Service for Remote Access to a Router or Switch</i></li> </ul>
------------------------------	--

## contact

---

<b>Syntax</b>	<code>contact <i>contact</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp]</code>
<b>Release Information</b>	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.
<b>Description</b>	Define the value of the MIB II <b>sysContact</b> object, which is the contact person for the managed system.
<b>Options</b>	<b>contact</b> —Name of the contact person. If the name includes spaces, enclose it in quotation marks (" ").
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring the System Contact on a Device Running Junos OS</i></li> </ul>

## disable (LLDP)

---

<b>Syntax</b>	<code>disable;</code>
<b>Hierarchy Level</b>	<code>[edit protocols <a href="#">lldp</a>],</code> <code>[edit protocols <a href="#">interface lldp</a>]</code>
<b>Release Information</b>	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.
<b>Description</b>	Disable the LLDP configuration on the switch or on one or more interfaces.
<b>Default</b>	If you do not configure LLDP, it is disabled on the switch and on specific switch interfaces.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show lldp on page 212</a></li> <li>• <i>Configuring LLDP (CLI Procedure)</i></li> <li>• <i>Understanding LLDP and LLDP-MED on EX Series Switches</i></li> <li>• <i>Configuring LLDP</i></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul>

## falling-threshold (Health Monitor)

---

<b>Syntax</b>	<code>falling-threshold <i>percentage</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp health-monitor]</code>
<b>Release Information</b>	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.
<b>Description</b>	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.
<b>Options</b>	<b><i>percentage</i></b> —Lower threshold for the alarm entry. <b>Range:</b> 1 through 100 <b>Default:</b> 70 percent of the maximum possible value
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">rising-threshold on page 178</a></li><li>• <i>Configuring Health Monitoring</i></li></ul>

## filter-duplicates

---

<b>Syntax</b>	<code>filter-duplicates;</code>
<b>Hierarchy Level</b>	<code>[edit snmp]</code>
<b>Release Information</b>	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.
<b>Description</b>	Filter duplicate <b>Get</b> , <b>GetNext</b> , or <b>GetBulk</b> SNMP requests.
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Understanding the Implementation of SNMP on the QFabric System</i></li><li>• <i>Example: Configuring SNMP</i></li></ul>

## full-name

---

<b>Syntax</b>	<code>full-name <i>complete-name</i>;</code>
<b>Hierarchy Level</b>	[edit system login user]
<b>Release Information</b>	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.
<b>Description</b>	Configure the complete name of a user.
<b>Options</b>	<i>complete-name</i> —Full name of the user. If the name contains spaces, enclose it in quotation marks.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Junos OS User Accounts by Using a Configuration Group</i></li> <li>• <i>user</i></li> </ul>

## health-monitor

---

<b>Syntax</b>	<pre>health-monitor {   falling-threshold <i>percentage</i>;   interval <i>seconds</i>;   rising-threshold <i>percentage</i>; }</pre>
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	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.
<b>Description</b>	Configure health monitoring.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Health Monitoring</i></li> <li>• <i>Understanding Health Monitoring</i></li> </ul>

## hold-multiplier

---

<b>Syntax</b>	hold-multiplier <i>number</i> ;
<b>Hierarchy Level</b>	[edit protocols <a href="#">lldp</a> ]
<b>Release Information</b>	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.
<b>Description</b>	Specify the multiplier used in combination with the <a href="#">advertisement-interval</a> value to determine the length of time LLDP information is held before it is discarded. The default value is 4 (or 120 seconds).
<b>Default</b>	Disabled.
<b>Options</b>	<i>number</i> —A number used as a multiplier. <b>Range:</b> 2 through 10 <b>Default:</b> 4 (or 120 seconds)
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show lldp on page 212</a></li><li>• <i>Configuring LLDP (CLI Procedure)</i></li><li>• <i>Understanding LLDP and LLDP-MED on EX Series Switches</i></li><li>• <i>Configuring LLDP</i></li><li>• <a href="#">Understanding LLDP on page 5</a></li></ul>

## idle-timeout (Access)

<b>Syntax</b>	<code>idle-timeout seconds;</code>
<b>Hierarchy Level</b>	<code>[edit access group-profile <i>profile-name</i> ppp],</code> <code>[edit access profile <i>profile-name</i> client <i>client-name</i> ppp]</code>
<b>Release Information</b>	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.
<b>Description</b>	Configure the idle timeout for a user. The router might consider a PPP session to be idle because of the following reasons: <ul style="list-style-type: none"> <li>• There is no ingress traffic on the PPP session.</li> <li>• There is no egress traffic.</li> <li>• There is neither ingress or egress traffic on the PPP session.</li> <li>• There is no ingress or egress PPP control traffic. This is applicable only if keepalives are enabled.</li> </ul>
<b>Options</b>	<b>seconds</b> —Number of seconds a user can remain idle before the session is terminated. <b>Range:</b> 0 through 4,294,967,295 seconds <b>Default:</b> 0




**NOTE:** The `[edit access]` hierarchy is not available on QFabric systems.

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

<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring the Group Profile for Defining L2TP Attributes</i></li> <li>• <i>Configuring PPP Properties for a Client-Specific Profile</i></li> <li>• <i>Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile</i></li> </ul>
------------------------------	--

## interface (LLDP)

<b>Syntax</b>	<pre>interface (all   <i>interface-name</i>) {     disable;     power-negotiation {         disable;     } }</pre>
<b>Hierarchy Level</b>	[edit protocols <a href="#">lldp</a> ]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
<b>Description</b>	Configure Link Layer Discovery Protocol (LLDP) on all interfaces or on a specific interface.
	<div>  <p><b>NOTE:</b> On EX4300 switches, LLDP cannot be configured on the me0 or vme interface. Issuing the command <code>set protocols lldp interface me0</code> generates the following error message:</p> <pre>error: name: 'me0': Invalid interface error: statement creation failed: interface</pre> <p>Issuing the command <code>set protocols lldp interface vme</code> generates the following error message:</p> <pre>error: name: 'vme': Invalid interface error: statement creation failed: interface</pre> </div>
<b>Default</b>	None
<b>Options</b>	<p><b>all</b>—All interfaces on the switch.</p> <p><b><i>interface-name</i></b>—Name of a specific interface.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring LLDP (CLI Procedure)</a></li> <li>• <a href="#">Understanding LLDP and LLDP-MED on EX Series Switches</a></li> <li>• <a href="#">Configuring LLDP</a></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul>

## interval (Health Monitor)

---

<b>Syntax</b>	interval <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit snmp health-monitor]
<b>Release Information</b>	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.
<b>Description</b>	Configure the interval between sampling of the object being monitored by the health monitor.
<b>Options</b>	<i>seconds</i> —Time between samples, in seconds. <b>Range:</b> 1 through 2147483647 seconds <b>Default:</b> 300 seconds
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Health Monitoring</i></li></ul>

## 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;
    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;
}
```

**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.



**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 212](#)
- *Configuring LLDP (CLI Procedure)*
- *Configuring LLDP*
- [Understanding LLDP on page 5](#)
- *Understanding LLDP and LLDP-MED on EX Series Switches*

## lldp-configuration-notification-interval

---

<b>Syntax</b>	lldp-configuration-notification-interval <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit protocols <a href="#">lldp</a> ]
<b>Release Information</b>	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.
<b>Description</b>	Specify how often SNMP trap notifications are generated as a result of LLDP database changes. If the interval value is 0, trap notifications of database changes are disabled.
<b>Default</b>	SNMP trap notifications of LLDP database changes are disabled.
<b>Options</b>	<b><i>seconds</i></b> —Interval between trap notifications about LLDP database changes. <b>Range:</b> 0 through 3600
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show lldp on page 212</a></li></ul>

## location

---

<b>Syntax</b>	location <i>location</i> ;
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	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.
<b>Description</b>	Define the value of the MIB II <b>sysLocation</b> object, which is the physical location of the managed system.
<b>Options</b>	<b><i>location</i></b> —Location of the local system. You must enclose the name within quotation marks (" ").
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the System Location for a Device Running Junos OS</i></li></ul>

## management-address

<b>Syntax</b>	<code>management-address <i>ip-management-address</i>;</code>
<b>Hierarchy Level</b>	[edit protocols <a href="#">lldp</a> ]
<b>Release Information</b>	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.
<b>Description</b>	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.
<b>Default</b>	The LLDP Management Address TLV uses the IP address of the switch's management Ethernet interface ( <b>me0</b> ), or the IP address of the virtual management Ethernet (VME) interface if the switch is a Virtual Chassis member.
<b>Options</b>	<i>ip-management-address</i> —You can specify either an IPv4 or an IPv6 management address for the switch.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show lldp on page 212</a></li> <li>• <i>Understanding LLDP and LLDP-MED on EX Series Switches</i></li> <li>• <i>EX Series Switches Interfaces Overview</i></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul>

## name

---

<b>Syntax</b>	<code>name <i>name</i>;</code>
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	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.
<b>Description</b>	Set the system name from the command-line interface.
<b>Options</b>	<i>name</i> —System name override.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Different System Name</a></li></ul>

## nas-ip-address

---

<b>Syntax</b>	<code>nas-ip-address <i>ip-address</i>;</code>
<b>Hierarchy Level</b>	[edit system]
<b>Release Information</b>	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.
<b>Description</b>	Configure the NAS-IP address for outgoing RADIUS packets.
<b>Options</b>	<i>ip-address</i> —IP address of the network access server (NAS) that requests user authentication.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring RADIUS Server Authentication</a></li><li>• <a href="#">Configuring RADIUS Authentication (QFX Series or OCX Series) on page 83</a></li></ul>

## nonvolatile

<b>Syntax</b>	nonvolatile { <b>commit-delay</b> <i>seconds</i> ; }
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	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.
<b>Description</b>	Configure options for SNMP <b>Set</b> requests.  The statement is explained separately.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring the Commit Delay Timer</i></li> <li>• <i>commit-delay</i></li> </ul>

## oid

<b>Syntax</b>	oid <i>object-identifier</i> (exclude include);
<b>Hierarchy Level</b>	[edit snmp view <i>view-name</i> ]
<b>Release Information</b>	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.
<b>Description</b>	Specify an object identifier (OID) used to represent a subtree of MIB objects.
<b>Options</b>	<p><b>exclude</b>—Exclude the subtree of MIB objects represented by the specified OID.</p> <p><b>include</b>—Include the subtree of MIB objects represented by the specified OID.</p> <p><b>object-identifier</b>—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.</p>
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring MIB Views</i></li> </ul>

## order

---

<b>Syntax</b>	<code>order (radius   [ <i>accounting-order-data-list</i> ] );</code>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> accounting]
<b>Release Information</b>	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.
<b>Description</b>	Configure the order of authentication, authorization, and accounting (AAA) servers to use while sending accounting messages and updates.
<b>Default</b>	No order specified
<b>Options</b>	<b>radius</b> —RADIUS accounting for specified subscribers.  [ <i>accounting-order-data-list</i> ]— 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.

---

<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch</i></li><li>• <i>Configuring 802.1X RADIUS Accounting (CLI Procedure)</i></li><li>• <i>Configuring RADIUS Accounting</i></li></ul>

## port (RADIUS Server)


<b>Syntax</b>	<code>port <i>port-number</i>;</code>
<b>Hierarchy Level</b>	[edit system radius-server <i>address</i> ], [edit system accounting destination radius server <i>address</i> ]
<b>Release Information</b>	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.
<b>Description</b>	Configure the port number on which to contact the RADIUS server.
<b>Options</b>	<i>number</i> —Port number on which to contact the RADIUS server. <b>Default:</b> 1812 (as specified in RFC 2865)



**NOTE:** The [edit system accounting] hierarchy is not available on QFabric systems.

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring RADIUS Server Authentication</i></li> </ul>

## profile

<b>Syntax</b>	<pre> profile <i>profile-name</i> {     accounting (Access Profile) {         accounting-stop-on-access-deny;         accounting-stop-on-failure;         order ( radius   [ <i>accounting-order-data-list</i> ] );     }     authentication-order (Access Profile) [<i>authentication-method</i>];     radius {         accounting-server [<i>server-addresses</i>];         authentication-server [<i>server-addresses</i>];     } } </pre>
<b>Hierarchy Level</b>	[edit access]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
<b>Description</b>	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.
<b>Default</b>	Not enabled
<b>Options</b>	<p><b><i>profile-name</i></b>—Profile name of up to 32 characters.</p> <p>The remaining statements are explained separately.</p>
<div>  <b>NOTE:</b> The [edit access] hierarchy is not available on QFabric systems. </div>	
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch</i></li> <li>• <i>Configuring 802.1X RADIUS Accounting (CLI Procedure)</i></li> <li>• <i>Configuring RADIUS Accounting</i></li> </ul>

## 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 tll-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-interval milliseconds;
            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;
    credibility-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 (Spanning Trees);
  force-version (Spanning Trees) stp;
  vlan (Spanning Trees) vlan-id {
    bridge-priority (Spanning Trees) priority;
    forward-delay (Spanning Trees) seconds;
    hello-time (Spanning Trees) seconds;
    interface (Spanning Trees) (all | interface-name) {
      bpdu-timeout-action (Spanning Trees) {
        block (Spanning Trees);
        log (Spanning Trees);
      }
      cost (Spanning Trees) cost;
      disable (Spanning Trees);
      edge (Spanning Trees);
      mode (Spanning Trees) mode;
      no-root-port (Spanning Trees);
      priority (Spanning Trees) priority;
    }
    max-age (Spanning Trees) seconds;
    traceoptions (Spanning Trees) {
      file filename <files number > <size size > <no-stamp | world-readable |
        no-world-readable>;
      flag flag;
    }
  }
}
}
}

```

<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	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.
<b>Description</b>	Configure protocols.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	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

---

<b>Syntax</b>	<code>protocol-version <i>version</i>;</code>
<b>Hierarchy Level</b>	[edit system services ssh]
<b>Release Information</b>	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.
<b>Description</b>	Specify the secure shell (SSH) protocol version.
<b>Default</b>	<b>v2</b> —SSH protocol version 2 is the default, introduced in Junos OS Release 11.4.
<b>Options</b>	<b><i>version</i></b> —SSH protocol version: <b>v1</b> , <b>v2</b> , or both.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	• <a href="#">Configuring SSH Service for Remote Access to the Router or Switch</a>

## ptopo-configuration-maximum-hold-time


<b>Syntax</b>	<code>ptopo-configuration-maximum-hold-time <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit protocols <a href="#">lldp</a> ]
<b>Release Information</b>	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.
<b>Description</b>	Configure how long to maintain the physical topology database entries. The physical topology identifies the devices on the network and their physical interconnections.
<b>Options</b>	<b><i>seconds</i></b> —Time to maintain physical topology database entries. <b>Default:</b> 300 <b>Range:</b> 1 through 2147483647
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show lldp on page 212</a></li> <li>• <i>Understanding LLDP and LLDP-MED on EX Series Switches</i></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul>

## ptopo-configuration-trap-interval


<b>Syntax</b>	<code>ptopo-configuration-trap-interval <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit protocols <a href="#">lldp</a> ]
<b>Release Information</b>	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.
<b>Description</b>	Specify how often SNMP trap notifications are sent regarding changes in physical topology global statistics.
<b>Default</b>	SNMP trap notifications of changes in physical topology global statistics are disabled.
<b>Options</b>	<b><i>seconds</i></b> —Interval between SNMP trap notifications about physical topology global statistics. <b>Range:</b> 0 through 3600
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## radius

---


<b>Syntax</b>	<pre>radius {     accounting-server [server-addresses];     authentication-server [server-addresses]; }</pre>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> ]
<b>Release Information</b>	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.
<b>Description</b>	<p>Configure the RADIUS servers for authentication and for accounting. To configure multiple RADIUS servers, include multiple <b>radius</b> statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.</p> <p>The statements are explained separately.</p>
<div> <b>NOTE:</b> The [edit access] hierarchy is not available on QFabric systems.</div>	
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch</i></li><li>• <i>Configuring 802.1X RADIUS Accounting (CLI Procedure)</i></li><li>• <i>Filtering 802.1X Supplicants by Using RADIUS Server Attributes</i></li><li>• <i>Configuring RADIUS Accounting</i></li></ul>

## radius-options (edit system)

<b>Syntax</b>	<pre>radius-options {   attributes {     nas-ip-address <i>ip-address</i>;   }   enhanced-accounting;   password-protocol <i>mschap-v2</i>; }</pre>
<b>Hierarchy Level</b>	[edit system]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2.</p> <p>MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p>
	<p> <b>NOTE:</b> The <code>radius-options</code> statement is not available on QFabric systems.</p>
	<p><b>enhanced-accounting</b> statement introduced in Junos OS Release 14.1.</p>
<b>Description</b>	Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.
<b>Options</b>	<p><b>enhanced-accounting</b>—View the attribute values of a logged in user.</p> <p><b>nas-ip-address <i>ip-address</i></b>—IP address of the network access server (NAS) that requests user authentication.</p> <p><b>password-protocol <i>mschap-v2</i></b>—Protocol MS-CHAPv2, used for password authentication and password changing.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring MS-CHAPv2 for Password-Change Support</a></li> <li>• <a href="#">Configuring RADIUS System Accounting on page 101</a></li> <li>• <a href="#">enhanced-accounting</a></li> </ul>

## radius-server

---

<b>Syntax</b>	<pre>radius-server server-address {     accounting-port <i>port-number</i>;     port <i>number</i>;     retry <i>number</i>;     secret <i>password</i>;     source-address <i>source-address</i>;     timeout <i>seconds</i>; }</pre>
<b>Hierarchy Level</b>	[edit system]
<b>Release Information</b>	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.
<b>Description</b>	<p>Configure a RADIUS server for Point-to-Point Protocol (PPP).</p> <p>To configure multiple RADIUS servers, include multiple <b>radius-server</b> statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.</p>
<b>Options</b>	<p><b>server-address</b>—Address of the RADIUS authentication server.</p> <p>The remaining statements are explained separately.</p>
<div> <b>NOTE:</b> The <b>accounting-port</b> and <b>source-address</b> options are not available on QFabric systems.</div>	
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring RADIUS Authentication (QFX Series or OCX Series) on page 83</a></li><li>• <a href="#">accounting-port</a></li><li>• <a href="#">port on page 155</a></li><li>• <a href="#">retry on page 177</a></li><li>• <a href="#">secret</a></li><li>• <a href="#">source-address</a></li><li>• <a href="#">timeout</a></li></ul>

## rate-limit

<b>Syntax</b>	<code>rate-limit <i>limit</i>;</code>
<b>Hierarchy Level</b>	<code>[edit system services finger],</code> <code>[edit system services ftp],</code> <code>[edit system services netconf ssh],</code> <code>[edit system services ssh],</code> <code>[edit system services telnet],</code> <code>[edit system services tftp-server],</code> <code>[edit system services xnm-clear-text],</code> <code>[edit system services xnm-ssl]</code>
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
<b>Description</b>	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.
<b>Default</b>	150 connections
<b>Options</b>	<p><b>rate-limit <i>limit</i></b>—(Optional) Maximum number of connection attempts allowed per minute, per IP protocol (either IPv4 or IPv6).</p> <p><b>Range:</b> 1 through 250</p> <p><b>Default:</b> 150</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring clear-text or SSL Service for Junos XML Protocol Client Applications</i></li> </ul>

## remote-debug-permission

---

<b>Syntax</b>	remote-debug-permission (qfabric-admin   qfabric-operator   qfabric-user);
<b>Hierarchy Level</b>	[edit system login user <i>username</i> authentication] [edit system root-authentication]
<b>Release Information</b>	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.
<b>Description</b>	(QFabric systems only) Configure authentication classes that permit or deny user access to individual components of the QFabric system.
<b>Default</b>	qfabric-user
<b>Options</b>	<p><b>qfabric-admin</b>—Permits a user to log in to individual QFabric system components, view operations, and change component configurations.</p> <p><b>qfabric-operator</b>—Permits a user to log in to individual QFabric system components and view component operations.</p> <p><b>qfabric-user</b>—Prevents a user from logging in to individual QFabric system components.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Example: Configuring QFabric System Login Classes</i></li><li>• <a href="#">request component login on page 206</a></li><li>• <i>Understanding QFabric System Login Classes</i></li></ul>

## retry

<b>Syntax</b>	<code>retry number;</code>
<b>Hierarchy Level</b>	[edit system radius server <i>server-address</i> ], [edit system accounting destination radius server <i>server-address</i> ]
<b>Release Information</b>	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.
<b>Description</b>	Number of times the router or switch is allowed to try to contact a RADIUS authentication or accounting server.
<b>Options</b>	<i>number</i> —Number of retries allowed for contacting a RADIUS server. <b>Range:</b> 1 through 10 <b>Default:</b> 3



**NOTE:** The [edit system accounting] hierarchy is not available on QFabric systems.

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring RADIUS Authentication (QFX Series or OCX Series) on page 83</a></li> <li>• <i>Configuring RADIUS Accounting</i></li> <li>• <i>timeout</i></li> </ul>

## rising-threshold (Health Monitor)

---

<b>Syntax</b>	<code>rising-threshold <i>percentage</i>;</code>
<b>Hierarchy Level</b>	[edit snmp health-monitor]
<b>Release Information</b>	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.
<b>Description</b>	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.
<b>Options</b>	<b><i>percentage</i></b> —Upper threshold for the alarm entry. <b>Range:</b> 1 through 100 <b>Default:</b> 80 percent of the maximum possible value
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Health Monitoring</a></li><li>• <a href="#">falling-threshold on page 142</a></li></ul>

---

## root-login

---

<b>Syntax</b>	root-login (allow   deny   deny-password);
<b>Hierarchy Level</b>	[edit system services ssh]
<b>Release Information</b>	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.
<b>Description</b>	Control user access through SSH.
<b>Default</b>	Allow user access through SSH.
<b>Options</b>	<b>allow</b> —Allow users to log in to the router or switch as root through SSH. <b>deny</b> —Disable users from logging in to the router or switch as root through SSH. <b>deny-password</b> —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.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring SSH Service for Remote Access to the Router or Switch</i></li></ul>

## 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.

## snmp

```

Syntax  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);
}
}
}

```

<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	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.
<b>Description</b>	Configure SNMP.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Understanding the Implementation of SNMP</i></li> <li>• <i>Configuring SNMP</i></li> </ul>

## ssh

<b>Syntax</b>	<pre>ssh {   authentication-order [authentication-methods];   ciphers [ cipher-1 cipher-2 cipher-3 ...];   client-alive-count-max seconds;   client-alive-interval seconds;   connection-limit limit;   hostkey-algorithm &lt;algorithm no-algorithm&gt;;   key-exchange &lt;algorithm&gt;;   macs &lt;algorithm&gt;;   max-sessions-per-connection &lt;number&gt;;   no-passwords;   no-public-keys;   no-tcp-forwarding;   protocol-version [v1 v2];   rate-limit limit;   root-login (allow   deny   deny-password); } tcp-forwarding (JDM)</pre>
<b>Hierarchy Level</b>	[edit system services]
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p><b>client-alive-interval</b> and <b>client-alive-max-count</b> statements introduced in Junos OS Release 12.2.</p> <p><b>no-passwords</b> statement introduced in Junos OS Release 13.3.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p><b>no-public-keys</b> statement introduced in Junos OS release 15.1.</p> <p><b>tcp-forwarding</b> statement introduced in Junos OS Release 15.1X53-D50 for the NFX250 Network Services Platform.</p>
<b>Description</b>	<p>Allow SSH requests from remote systems to the local router or switch.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring SSH Service for Remote Access to the Router or Switch</i></li> </ul>

## 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-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-limit bucket-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 {
  announcement text;
  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;
    serveraddress <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.

## tacplus-options

---

<b>Syntax</b>	<pre>tacplus-options {   (exclude-cmd-attribute   no-cmd-attribute-value);   enhanced-accounting;   service-name <i>service-name</i>;   timestamp-and-timezone; }</pre>
<b>Hierarchy Level</b>	[edit system]
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p><b>no-cmd-attribute-value</b> and <b>exclude-cmd-attribute</b> options introduced in Junos OS Release 9.3.</p> <p>Statement introduced in Junos OS Release 11.1 for QFX Series.</p> <p><b>timestamp-and-timezone</b> option introduced in Junos OS Release 12.2.</p> <p><b>enhanced-accounting</b> option introduced in Junos OS Release 14.1.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p>
<b>Description</b>	Configure TACACS+ options for authentication and accounting.
<b>Options</b>	<p><b>enhanced-accounting</b>—View the attribute values of a logged in user.</p> <p><b>exclude-cmd-attribute</b>—Exclude the <b>cmd</b> attribute value completely from start and stop accounting records to enable logging of accounting records in the correct log file on a TACACS+ server.</p> <p><b>no-cmd-attribute-value</b>—Set the <b>cmd</b> 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.</p> <p><b>service-name <i>service-name</i></b>—Name of the authentication service used when you configure multiple TACACS+ servers to use the same authentication service.</p> <p><b>Default:</b> junos-exec</p> <p><b>timestamp-and-timezone</b>—Include this statement if you want start time, stop time, and timezone attributes included in start/stop accounting records.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring TACACS+ Authentication</i></li><li>• <i>Configuring TACACS+ System Accounting</i></li><li>• <a href="#">Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 67</a></li><li>• <i>enhanced-accounting</i></li></ul>

---

## targets

---

<b>Syntax</b>	<pre>targets {     address; }</pre>
<b>Hierarchy Level</b>	[edit snmp trap-group <i>group-name</i> ]
<b>Release Information</b>	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.
<b>Description</b>	Configure one or more systems to receive SNMP traps.
<b>Options</b>	<b>address</b> —IPv4 or IPv6 address of the system to receive traps. You must specify an address, not a hostname.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring SNMP Trap Groups</i></li></ul>

## traceoptions (LLDP)

<b>Syntax</b>	<pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable   no-world-readable&gt; &lt;no-stamp&gt;     &lt;replace&gt;;     flag <i>flag</i> &lt;disable&gt;; } </pre>
<b>Hierarchy Level</b>	[edit protocols <a href="#">lldp</a> ]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
<b>Description</b>	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.

<b>Default</b>	Tracing operations are disabled.
<b>Options</b>	<p><b>file <i>filename</i></b>—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 <code>/var/log</code>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and so on, until the maximum <b>xk</b> to specify KB, <b>xm</b> to specify MB, or <b>xg</b> 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—All tracing operations.</li> <li>• <b>configuration</b>—Trace configuration operations.</li> <li>• <b>interface</b>—Trace interface update events.</li> <li>• <b>netbios</b>—Trace NetBIOS events.</li> <li>• <b>packet</b>—Trace packet events.</li> <li>• <b>rtsock</b>—Trace routing socket operations.</li> <li>• <b>snmp</b>—Trace SNMP configuration operations.</li> </ul>

- **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:** **xk** to specify KB, **xm** to specify MB, or **xg** 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.

<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring LLDP-MED (CLI Procedure)</i></li> <li>• <i>Understanding LLDP and LLDP-MED on EX Series Switches</i></li> <li>• <i>Configuring LLDP</i></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul>

## transfer-interval (Configuration)

---

<b>Syntax</b>	<code>transfer-interval <i>interval</i>;</code>
<b>Hierarchy Level</b>	[edit system archival configuration]
<b>Release Information</b>	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.
<b>Description</b>	Configure the router or switch to periodically transfer its currently active configuration to an archive site.
<b>Options</b>	<b>interval</b> —Interval at which to transfer the current configuration to an archive site. <b>Range:</b> 15 through 2880 minutes



**NOTE:** The [edit system archival] hierarchy is not available on QFabric systems.

---

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site</i></li><li>• <i>archive</i></li><li>• <a href="#">configuration on page 139</a></li><li>• <a href="#">transfer-on-commit on page 197</a></li></ul>

## transfer-on-commit

<b>Syntax</b>	transfer-on-commit;
<b>Hierarchy Level</b>	[edit system archival configuration]
<b>Release Information</b>	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.
<b>Description</b>	Configure the router or switch to transfer its currently active configuration to an archive site each time you commit a candidate configuration.



**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, "ftp://username<:password>@[ipv6-host-address]<:port>/url-path" .



**NOTE:** The [edit system archival] hierarchy is not available on QFabric systems.

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site</i></li> <li>• <i>archive</i></li> <li>• <a href="#">configuration on page 139</a></li> <li>• <a href="#">transfer-interval on page 196</a></li> </ul>

## trap-group

---

<b>Syntax</b>	<pre>trap-group <i>group-name</i> {     categories {         <i>category</i>;     }     destination-port <i>port-number</i>;     routing-instance <i>instance</i>;     targets {         <i>address</i>;     }     version (all   v1   v2); }</pre>
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	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.
<b>Description</b>	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.
<b>Options</b>	<p><b><i>group-name</i></b>—Name of the trap group. If the name includes spaces, enclose it in quotation marks (" ").</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring SNMP Trap Groups</i></li></ul>

---

## trap-options

---

<b>Syntax</b>	<pre>trap-options {     agent-address outgoing-interface;     source-address address; }</pre>
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	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.
<b>Description</b>	<p>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.</p> <p>The remaining statements are explained separately.</p>
<b>Default</b>	Disabled
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring SNMP Trap Options</i></li></ul>

## user (Access)

---

<b>Syntax</b>	<pre>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" &lt;from hostname&gt;;     ssh-rsa "public-key" &lt;from hostname&gt;;   }   class class-name;   full-name "complete-name";   uid uid-value; }</pre>
<b>Hierarchy Level</b>	[edit system login]
<b>Release Information</b>	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.
<b>Description</b>	Configure access permission for individual users.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Junos OS User Accounts on page 61</a></li><li>• <i>class</i></li></ul>

---

## version

---

<b>Syntax</b>	version (all   v1   v2);
<b>Hierarchy Level</b>	[edit snmp trap-group <i>group-name</i> ]
<b>Release Information</b>	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.
<b>Description</b>	Specify the version number of SNMP traps.
<b>Default</b>	all—Send an SNMPv1 and SNMPv2 trap for every trap condition.
<b>Options</b>	all—Send an SNMPv1 and SNMPv2 trap for every trap condition.  v1—Send SNMPv1 traps only.  v2—Send SNMPv2 traps only.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring SNMP Trap Groups</i></li></ul>



## CHAPTER 12

# Operational Commands

- `clear lldp neighbors`
- `clear lldp statistics`
- `request component login`
- `show ethernet-switching interfaces`
- `show lldp`
- `show lldp local-information`
- `show lldp neighbors`
- `show lldp statistics`
- `show route instance`
- `show snmp statistics`
- `ssh`

## clear lldp neighbors

---

<b>Syntax</b>	<code>clear lldp neighbors &lt;interface <i>interface</i>&gt;</code>
<b>Release Information</b>	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.
<b>Description</b>	Clear the learned remote neighbor information on all or selected interfaces.
<b>Options</b>	<b>none</b> —Clear the remote neighbor information on all interfaces.  <b>interface <i>interface</i></b> —(Optional) Clear the remote neighbor information from the selected interface.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring LLDP</a></li><li>• <a href="#">Understanding LLDP on page 5</a></li></ul>
<b>List of Sample Output</b>	<a href="#">clear lldp neighbors on page 204</a> <a href="#">clear lldp neighbors interface on page 204</a>

### 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

---

<b>Syntax</b>	<code>clear lldp statistics</code> <code>&lt;interface <i>interface</i>&gt;</code>
<b>Release Information</b>	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.
<b>Description</b>	Clear LLDP statistics on one or more interfaces.
<b>Options</b>	<b>none</b> —Clears LLDP statistics on all interfaces.  <b>interface <i>interface-names</i></b> —(Optional) Clear LLDP statistics on an interface.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring LLDP</a></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">clear lldp statistics on page 205</a> <a href="#">clear lldp statistics interface on page 205</a>

### 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
```

## request component login

<b>Syntax</b>	<code>request component login <i>component-name</i></code>
<b>Release Information</b>	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.
<b>Description</b>	(QFabric systems only) Log in to a QFabric system component. To gain access to individual components by way of the <b>request component login</b> command, you must first provide the <b>qfabric-admin</b> or <b>qfabric-operator</b> class privilege to your user (for more information, see: <a href="#">remote-debug-permission</a> ).
<b>Options</b>	<b><i>component-name</i></b> —Specify the QFabric system component to which you wish to log in.
<b>Required Privilege Level</b>	admin
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">remote-debug-permission on page 176</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">request component login (with qfabric-admin Privileges) on page 206</a> <a href="#">request component login (with qfabric-operator Privileges) on page 207</a> <a href="#">request component login (with qfabric-user Privileges) on page 207</a>

## 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-ee3093,169.254.128.41' (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
```

```

tracertoute          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-ee3093,169.254.128.41' (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

```

## show ethernet-switching interfaces

<b>Syntax</b>	show ethernet-switching interfaces <brief   detail   summary> <interface <i>interface-name</i> >
<b>Release Information</b>	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.
<b>Description</b>	Display information about switched Ethernet interfaces.
<b>Options</b>	<p><b>none</b>—(Optional) Display brief information for Ethernet-switching interfaces.</p> <p><b>brief   detail   summary</b>—(Optional) Display the specified level of output.</p> <p><b>interface <i>interface-name</i></b>—(Optional) Display Ethernet-switching information for a specific interface.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Troubleshooting Ethernet Switching</i> <i>Understanding Bridging and VLANs</i></li> <li>• <i>Example: Setting Up Basic Bridging and a VLAN on the QFX Series</i></li> <li>• <i>Example: Setting Up Bridging with Multiple VLANs</i></li> <li>• <i>Understanding FCoE</i></li> <li>• <i>Interfaces Overview</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show ethernet-switching interfaces on page 209</a> <a href="#">show ethernet-switching interfaces summary on page 210</a> <a href="#">show ethernet-switching interfaces brief on page 210</a> <a href="#">show ethernet-switching interfaces detail on page 210</a> <a href="#">show ethernet-switching interfaces interface-name on page 211</a>
<b>Output Fields</b>	Table 25 on page 208 lists the output fields for the <b>show ethernet-switching interfaces</b> command. Output fields are listed in the approximate order in which they appear.

Table 25: show ethernet-switching interfaces Output Fields

Field Name	Field Description	Level of Output
<b>Interface</b>	Name of a switching interface.	All levels
<b>State</b>	Interface state. Values are <b>up</b> or <b>down</b> .	none, <b>brief</b> , <b>detail</b> , <b>summary</b>
<b>VLAN members</b>	Name of a VLAN.	none, <b>brief</b> , <b>detail</b> , <b>summary</b>

Table 25: show ethernet-switching interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Blocking</b>	Forwarding state of the interface: <ul style="list-style-type: none"> <li>• <b>blocked</b>—Traffic is not being forwarded on the interface.</li> <li>• <b>unblocked</b>—Traffic is forwarded on the interface.</li> <li>• <b>MAC limit exceeded</b>—The interface is temporarily disabled because of a MAC limiting error. The disabled interface is automatically restored to service when the disable timeout expires.</li> <li>• <b>MAC move limit exceeded</b>—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.</li> <li>• <b>Storm control in effect</b> —The interface is temporarily disabled because of a storm control error. The disabled interface is automatically restored to service when the disable timeout expires.</li> <li>• <b>Storm control shutdown in effect</b> —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.</li> </ul>	none, <b>brief</b> , <b>detail</b> , <b>summary</b>
<b>Index</b>	VLAN index internal to Junos OS software.	<b>detail</b>
<b>untagged   tagged</b>	Specifies whether the interface forwards IEEE802.1Q-tagged or untagged traffic.	<b>detail</b>

## Sample Output

### 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
```

## 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 \(CLI Procedure\)](#)
- [Configuring LLDP-MED \(CLI Procedure\)](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches](#)
- [Configuring LLDP](#)
- [Understanding LLDP on page 5](#)

**List of Sample Output** [show lldp \(EX3200 switches\) on page 215](#)  
[show lldp \(EX4300 switches\) on page 215](#)  
[show lldp detail \(EX4300 switches\) on page 216](#)

**Output Fields** [Table 26 on page 212](#) lists the output fields for the **show lldp** command. Output fields are listed in the approximate order in which they appear.

**Table 26: show lldp Output Fields**

Field Name	Field Description	Level of Output
LLDP	LLDP operating state. The state can be <b>enabled</b> or <b>disabled</b> .  <b>NOTE:</b> 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 <b>disabled</b> .	All levels

Table 26: show lldp Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Advertisement interval</b>	Frequency, in seconds, at which LLDP advertisements are sent.  This value is set by the <code>advertisement-interval</code> configuration statement.	All levels
<b>Transmit delay</b>	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 <code>transmit-delay</code> configuration statement.	All levels
<b>Hold timer</b>	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 multiplier value is set by the <code>hold-multiplier</code> configuration statement.	All levels
<b>Notification interval</b>	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 <code>lldp-configuration-notification-interval</code> configuration statement.	All levels
<b>Config Trap Interval</b>	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 <code>ptopo-configuration-trap-interval</code> configuration statement.	All levels
<b>Connection Hold timer</b>	Amount of time the system maintains dynamic topology entries.  This value is set by the <code>ptopo-configuration-maximum-hold-time</code> configuration statement.	All levels
<b>LLDP-MED</b>	LLDP-MED operating state. The state can be <b>Enabled</b> or <b>Disabled</b> .	All levels
<b>MED fast start count</b>	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 <code>fast-start</code> configuration statement.  <b>NOTE:</b> <code>fast-start</code> is not available on the QFX Series.	All levels
<b>Interface</b>	Name of the interface for which LLDP configuration information is being reported.	All levels
<b>Parent Interface</b>	Name of the aggregated Ethernet interface, if any, to which the interface belongs.	All levels

Table 26: show lldp Output Fields (*continued*)

Field Name	Field Description	Level of Output
LLDP	LLDP operating state. The state can be <b>Enabled</b> or <b>Disabled</b> .	All levels
Power Negotiation	LLDP power negotiation operating state. The state can be <b>Enabled</b> or <b>Disabled</b> .	All levels
Neighbor count	Total number of new LLDP neighbors detected since the last switch reboot.	<b>detail</b>
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.	<b>detail</b>
Vlan-name	VLAN name associated with the VLAN ID.	<b>detail</b>
LLDP basic TLVs supported	<p>Basic TLVs supported on the switch:</p> <ul style="list-style-type: none"> <li>• <b>Chassis identifier</b>—TLV that advertises the MAC address associated with the local system.</li> <li>• <b>Port identifier</b>—TLV that advertises the port identification for the specified port in the local system.</li> <li>• <b>Port description</b>—Interface name for the port.</li> <li>• <b>System name</b>—TLV that advertises the user-configured name of the local system.</li> <li>• <b>System description</b>—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.</li> <li>• <b>System capabilities</b>—TLV that advertises the primary functions performed by the system—for example, bridge or router.</li> <li>• <b>Management address</b>—TLV that advertises the IP management address of the local system.</li> </ul>	<b>detail</b>
Supported LLDP 802 TLVs	<p>802.3 TLVs supported on the switch:</p> <ul style="list-style-type: none"> <li>• <b>MAC/PHY configuration status</b>—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.</li> <li>• <b>Power via MDI</b>—TLV that advertises MDI power support, PSE power pair, and power class information.</li> <li>• <b>Link aggregation</b>—TLV that advertises if the interface is aggregated and its aggregated interface ID.</li> <li>• <b>Maximum frame size</b>—TLV that advertises the maximum transmission unit (MTU) of the interface sending LLDP frames.</li> <li>• <b>Port VLAN tag</b>—TLV that advertises the VLAN tag configured on the interface.</li> <li>• <b>Port VLAN name</b>—TLV that advertises the VLAN name configured on the interface.</li> </ul>	<b>detail</b>

Table 26: show lldp Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Supported LLDP MED TLVs</b>	<p>LLDP-MED TLVs supported on the switch:</p> <ul style="list-style-type: none"> <li>• <b>LLDP MED capabilities</b>—TLV that advertises the primary function of the port. The capabilities values range from 0 through 15: <ul style="list-style-type: none"> <li>• 0—Capabilities</li> <li>• 1—Network Policy</li> <li>• 2—Location Identification</li> <li>• 3—Extended Power via MDI-PSE</li> <li>• 4—Inventory</li> <li>• 5–15—Reserved</li> </ul> </li> <li>• <b>Network policy</b>—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.</li> <li>• <b>Endpoint location</b>—TLV that advertises the physical location of the endpoint.</li> <li>• <b>Extended power Via MDI</b>—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.</li> </ul>	<b>detail</b>

## 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	v100
xe-3/0/0.0	ae31.0	101	v101
xe-3/0/0.0	ae31.0	4000	v4000
xe-3/0/1.0	ae31.0	100	v100
xe-3/0/1.0	ae31.0	101	v101
xe-3/0/1.0	ae31.0	4000	v4000
xe-3/0/2.0	ae31.0	100	v100
xe-3/0/2.0	ae31.0	101	v101
xe-3/0/2.0	ae31.0	4000	v4000

**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 local-information

<b>Syntax</b>	show lldp local-information
<b>Release Information</b>	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.
<b>Description</b>	Display the information that the switch provides in Link Layer Discovery Protocol (LLDP) advertisements to its neighbors.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring LLDP (CLI Procedure)</i></li> <li>• <i>Understanding LLDP and LLDP-MED on EX Series Switches</i></li> <li>• <a href="#">management-address on page 151</a></li> <li>• <i>Configuring LLDP</i></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show lldp local-information (EX Series Switch) on page 218</a>
<b>Output Fields</b>	<a href="#">Table 27 on page 217</a> lists the output fields for the <b>show lldp local-information</b> command. Output fields are listed in the approximate order in which they appear.

**Table 27: show lldp local-information Output Fields**

Field Name	Field Description
<b>LLDP Local Information details</b>	<p>Information about the local system (the switch):</p> <ul style="list-style-type: none"> <li>• <b>Chassis ID</b>—MAC address associated with the switch.</li> <li>• <b>System name</b>—User-configured name of the switch.</li> <li>• <b>System descr</b>—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.</li> </ul>
<b>System Capabilities</b>	Capabilities (such as <b>bridge</b> or <b>router</b> ) that are supported or enabled on the system.
<b>Management Information</b>	<p>Details of the management information: <b>Port Name</b>, <b>Port Address</b> (such as 10.204.34.35), <b>Address Type</b> (such as <b>ipv4</b> or <b>ipv6</b>), <b>Port ID</b> (SNMP interface index), <b>Port ID Subtype</b>, and <b>Port Subtype</b>.</p> <p>The <b>Port Subtype</b> displays:</p> <ul style="list-style-type: none"> <li>• <b>ifindex(2)</b>—IP address of the switch's management Ethernet interface (<b>me0</b>) or virtual management Ethernet (<b>VME</b>) interface address (for a virtual chassis) is used to manage the switch.</li> <li>• <b>unknown(1)</b>—IP management address has been configured with set <b>protocols lldp management-address</b>.</li> </ul>

Table 27: show lldp local-information Output Fields (*continued*)

Field Name	Field Description
<b>Interface name</b>	Name of the local interface which is configured for either LLDP or LLDP-MED.
<b>Parent Interface</b>	Name of the aggregated Ethernet interface, if any, to which the local interface belongs.
<b>SNMP Index</b>	SNMP interface index.
<b>Interface description</b>	User-configured port description.
<b>Status</b>	Administrative status of the interface: either <b>up</b> or <b>down</b> .
<b>Tunneling</b>	Status of tunneling on the interface: either <b>enabled</b> or <b>disabled</b> .

## 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**

- [Configuring LLDP](#)
- [Understanding LLDP on page 5](#)

**List of Sample Output** [show lldp neighbors on page 222](#)  
[show lldp neighbors interface on page 222](#)

**Output Fields** [Table 28 on page 219](#) lists the output fields for the **show lldp neighbors** command. Output fields are listed in the approximate order in which they appear.

**Table 28: 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.
Port info	List of port information gathered from neighbors. This could be the port identifier or port description.

Table 28: show lldp neighbors Output Fields (*continued*)

Field Name	Field 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 <b>interface</b> option is used).
Local Information	Information about the local system (appears when the <b>interface</b> option is used).
Index	Local interface index (appears when the <b>interface</b> option is used).
Time to live	Number of seconds for which this information is valid (appears when the <b>interface</b> option is used).
Time mark	Date and timestamp of information (appears when the <b>interface</b> option is used).
Local Interface	Name of the local physical interface (appears when the <b>interface</b> option is used).
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the <b>interface</b> option is used).
Local Port ID	Local interface SNMP index (appears when the <b>interface</b> 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 <b>interface</b> option is used).
Neighbor Information	Information about a neighbor system on the interface (appears when the <b>interface</b> option is used).
Chassis type	Type of chassis identifier supplied, such as <b>MAC address</b> (appears when the <b>interface</b> option is used).
Chassis ID	Chassis identifier of the chassis type listed (appears when the <b>interface</b> option is used).
Port type	Type of port identifier supplied, such as <b>locally assigned</b> (appears when the <b>interface</b> option is used).
Port ID	Port identifier of the port type listed (appears when the <b>interface</b> option is used).
Port description	Port description (appears when the <b>interface</b> option is used).
System name	Name supplied by the system on the interface (appears when the <b>interface</b> option is used).

Table 28: show lldp neighbors Output Fields (*continued*)

Field Name	Field Description
<b>System Description</b>	Description supplied by the system on the interface (appears when the <b>interface</b> option is used).
<b>System capabilities</b>	Capabilities (such as <b>Bridge</b> , <b>Router</b> , and <b>Telephone</b> ) that are supported or enabled by the system on the interface (appears when the <b>interface</b> option is used).
<b>Management Info</b>	<p>Details of management information: <b>Type</b> (such as <b>ipv4</b> or <b>ipv6</b>), <b>Address</b> (such as <b>10.204.34.35</b>), <b>Port ID</b>, <b>Subtype</b>, <b>Interface Subtype</b>, and organization identifier (<b>OID</b>) (appears when the <b>interface</b> option is used).</p> <p>The <b>Interface Subtype</b> displays:</p> <ul style="list-style-type: none"> <li>• <b>ifIndex(2)</b>—IP address of the neighbor's management Ethernet interface (<b>me0</b>) or virtual management Ethernet (<b>VME</b>) interface address (for a virtual chassis) is used to manage the switch.</li> <li>• <b>unknown(1)</b>—Neighbor's IP management address has been configured with set <b>protocols lldp management-address</b>.</li> </ul>
<b>Media Info</b>	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 <b>Media endpoint class</b> (such as Class 3 for communication devices such as IP phones), <b>MED Hardware revision</b> , <b>MED Firmware revision</b> , <b>MED Software revision</b> , <b>MED Serial number</b> , <b>MED Manufacturer name</b> , or <b>MED Model name</b> .
<b>Organization Info</b>	One or more entries listing remote information by organizationally unique identifier ( <b>OUI</b> ), <b>Subtype</b> , <b>Index</b> , and <b>Info</b> (appears when the <b>interface</b> option is used).
<b>Age</b>	How long the neighbor has been identified (appears when the <b>interface</b> option is used and NetBIOS snooping is enabled on the switch).
<b>Local Interface</b>	Name of the local physical interface (appears when the <b>interface</b> option is used and NetBIOS snooping is enabled on the switch).
<b>Parent Interface</b>	Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the <b>interface</b> option is used and NetBIOS snooping is enabled on the switch).
<b>Chassis ID</b>	Chassis identifier of the chassis type listed (appears when the <b>interface</b> option is used and NetBIOS snooping is enabled on the switch).
<b>Port description</b>	Port description (appears when the <b>interface</b> option is used and NetBIOS snooping is enabled on the switch).
<b>System name</b>	NetBIOS name of the host (appears when the <b>interface</b> 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
```

LLDP 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-148p5-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 : 1.3.6.1.2.1.31.1.1.1.34

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 statistics

<b>Syntax</b>	<code>show lldp statistics</code> <code>&lt;interface <i>interface-ids</i>&gt;</code>
<b>Release Information</b>	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.
<b>Description</b>	Display LLDP statistics on all or selected interfaces.
<b>Options</b>	<b>none</b> —Display LLDP statistics on all interfaces and devices.  <b>interface <i>interface-ids</i></b> —(Optional) Display LLDP statistics on the selected devices.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring LLDP</a></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show lldp statistics on page 224</a>
<b>Output Fields</b>	<a href="#">Table 29 on page 224</a> lists the output fields for the <b>show lldp statistics</b> command. Output fields are listed in the approximate order in which they appear.

Table 29: show lldp statistics Output Fields

Field Name	Field Description	Level of Output
<b>Interface</b>	Name of an interface.	All levels
<b>Received</b>	Total number of LLDP frames received on an interface.	All levels
<b>Unknown-TLVs</b>	Number of unrecognized LLDP TLVs received on an interface.	All levels
<b>With Errors</b>	Number of LLDP frames received that contain errors.	All levels
<b>Discarded TLVs</b>	Number of LLDP TLVs received and then discarded on an interface.	All levels
<b>Transmitted</b>	Total number of LLDP frames transmitted on an interface.	All levels
<b>Untransmitted</b>	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 route instance

<b>Syntax</b>	show route instance <brief   detail   summary> <instance-name> <operational>
<b>Release Information</b>	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.
<b>Description</b>	(QFabric systems only) Display routing instance information.
<b>Options</b>	<p><b>none</b>—(Same as <b>brief</b>) Display standard information about all routing instances.</p> <p><b>brief   detail   summary</b>—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to <b>brief</b>. (These options are not available with the <b>operational</b> keyword.)</p> <p><b>instance-name</b>—(Optional) Display information for a specified routing instance.</p> <p><b>operational</b>—(Optional) Display operational routing instances.</p>
<b>Required Privilege Level</b>	view
<b>List of Sample Output</b>	<a href="#">show route instance on page 227</a> <a href="#">show route instance detail on page 227</a> <a href="#">show route instance operational on page 228</a> <a href="#">show route instance summary on page 228</a>
<b>Output Fields</b>	<a href="#">Table 30 on page 226</a> lists the output fields for the <b>show route instance</b> command. Output fields are listed in the approximate order in which they appear.

Table 30: show route instance Output Fields

Field Name	Field Description	Level of Output
Instance or <i>instance-name</i>	Name of the routing instance.	All levels
Operational Routing Instances	( <b>operational</b> keyword only) Names of all operational routing instances.	—
Type	Type of routing instance: <b>forwarding</b> or <b>virtual-router</b> .	All levels
State	State of the routing instance: <b>active</b> or <b>inactive</b> .	<b>detail</b>
Interfaces	Name of interfaces belonging to this routing instance.	<b>detail</b>
Tables	Tables (and number of routes) associated with this routing instance.	<b>detail</b>
Router ID	Identifier for the router.	<b>detail</b>

Table 30: show route instance Output Fields (*continued*)

Field Name	Field Description	Level of Output
Primary RIB	Primary table for this routing instance.	<b>brief none summary</b>
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
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: 3.3.3.7
  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 snmp statistics

---

<b>Syntax</b>	<code>show snmp statistics</code> <code>&lt;subagents&gt;</code>
<b>Release Information</b>	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 <b>subagents</b> introduced in Junos OS Release 14.2.
<b>Description</b>	Display statistics about Simple Network Management Protocol (SNMP) packets sent and received by the router or switch.
<b>Options</b>	<b>subagents</b> —(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.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>clear snmp statistics</i></li></ul>
<b>List of Sample Output</b>	<a href="#">show snmp statistics on page 235</a> <a href="#">show snmp statistics subagents on page 235</a>
<b>Output Fields</b>	<a href="#">Table 31 on page 231</a> describes the output fields for the <b>show snmp statistics</b> command. Output fields are listed in the approximate order in which they appear.

Table 31: show snmp statistics Output Fields

Field Name	Field Description
<b>Input</b>	<p>Information about received packets:</p> <ul style="list-style-type: none"> <li>• <b>Packets(snmplnPkts)</b>—Total number of messages delivered to the SNMP entity from the transport service.</li> <li>• <b>Bad versions—(snmplnBadVersions)</b> Total number of messages delivered to the SNMP entity that were for an unsupported SNMP version.</li> <li>• <b>Bad community names—(snmplnBadCommunityNames)</b> Total number of messages delivered to the SNMP entity that used an SNMP community name not known to the entity.</li> <li>• <b>Bad community uses—(snmplnBadCommunityUses)</b> 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.</li> <li>• <b>ASN parse errors—(snmplnASNParseErrs)</b> Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.</li> <li>• <b>Too big—(snmplnTooBigs)</b> Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <b>tooBig</b>.</li> <li>• <b>No such names—(snmplnNoSuchNames)</b> Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <b>noSuchName</b>.</li> <li>• <b>Bad values—(snmplnBadValues)</b> Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <b>badValue</b>.</li> <li>• <b>Read onlys—(snmplnReadOnlys)</b> Total number of valid SNMP PDUs delivered to the SNMP entity with an error status field of <b>readOnly</b>. Only incorrect implementations of SNMP generate this error.</li> </ul>

Table 31: show snmp statistics Output Fields (*continued*)

Field Name	Field Description
Input (continued)	<ul style="list-style-type: none"> <li>• <b>General errors—(snmpInGenErrs)</b> Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <b>genErr</b>.</li> <li>• <b>Total requests varbinds—(snmpInTotalReqVars)</b> Total number of MIB objects retrieved successfully by the SNMP entity as a result of receiving valid SNMP <b>GetRequest</b> and <b>GetNext</b> PDUs.</li> <li>• <b>Total set varbinds—(snmpInSetVars)</b> Total number of MIB objects modified successfully by the SNMP entity as a result of receiving valid SNMP <b>SetRequest</b> PDUs.</li> <li>• <b>Get requests—(snmpInGetRequests)</b> Total number of SNMP <b>GetRequest</b> PDUs that have been accepted and processed by the SNMP entity.</li> <li>• <b>Get nexts—(snmpInGetNexts)</b> Total number of SNMP <b>GetNext</b> PDUs that have been accepted and processed by the SNMP entity.</li> <li>• <b>Set requests—(snmpInSetRequests)</b> Total number of SNMP <b>SetRequest</b> PDUs that have been accepted and processed by the SNMP entity.</li> <li>• <b>Get responses—(snmpInGetResponses)</b> Total number of SNMP <b>GetResponse</b> PDUs that have been accepted and processed by the SNMP entity.</li> <li>• <b>Traps—(snmpInTraps)</b> Total number of SNMP traps generated by the SNMP entity.</li> <li>• <b>Silent drops—(snmpSilentDrops)</b> Total number of <b>GetRequest</b>, <b>GetNextRequest</b>, <b>GetBulkRequest</b>, <b>SetRequests</b>, and <b>InformRequest</b> 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.</li> <li>• <b>Proxy drops—(snmpProxyDrops)</b> Total number of <b>GetRequest</b>, <b>GetNextRequest</b>, <b>GetBulkRequest</b>, <b>SetRequests</b>, and <b>InformRequest</b> 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.</li> <li>• <b>Commit pending drops</b>—Number of SNMP packets for <b>Set</b> requests dropped because of a previous pending SNMP <b>Set</b> request on the committed configuration.</li> <li>• <b>Throttle drops</b>—Number of SNMP packets for any requests dropped reaching the throttle limit.</li> </ul>

Table 31: show snmp statistics Output Fields (*continued*)

Field Name	Field Description
V3 Input	<p>Information about SNMP version 3 packets:</p> <ul style="list-style-type: none"> <li>• <b>Unknown security models—(snmpUnknownSecurityModels)</b> 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.</li> <li>• <b>Invalid messages—(snmpInvalidMsgs)</b> Number of packets received by the SNMP engine that were dropped because there were invalid or inconsistent components in the SNMP message.</li> <li>• <b>Unknown pdu handlers—(snmpUnknownPDUHandlers)</b> 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.</li> <li>• <b>Unavailable contexts—(snmpUnavailableContexts)</b> Number of requests received for a context that is known to the SNMP engine, but is currently unavailable.</li> <li>• <b>Unknown contexts—(snmpUnknownContexts)</b> Total number of requests received for a context that is unknown to the SNMP engine.</li> <li>• <b>Unsupported security levels—(usmStatsUnsupportedSecLevels)</b> 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).</li> <li>• <b>Not in time windows—(usmStatsNotInTimeWindows)</b> Total number of packets received by the SNMP engine that were dropped because they appeared outside the authoritative SNMP engine's window.</li> <li>• <b>Unknown user names—(usmStatsUnknownUserNames)</b> 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.</li> <li>• <b>Unknown engine ids—(usmStatsUnknownEngineIDs)</b> 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.</li> <li>• <b>Wrong digests—(usmStatsWrongDigests)</b> Total number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value.</li> <li>• <b>Decryption errors—(usmStatsDecryptionErrors)</b> Total number of packets received by the SNMP engine that were dropped because they could not be decrypted.</li> </ul>

Table 31: show snmp statistics Output Fields (*continued*)

Field Name	Field Description
<b>Output</b>	<p>Information about transmitted packets:</p> <ul style="list-style-type: none"> <li>• <b>Packets—(snmpOutPkts)</b> Total number of messages passed from the SNMP entity to the transport service.</li> <li>• <b>Too big—(snmpOutTooBigs)</b> Total number of SNMP PDUs generated by the SNMP entity with an error status field of <b>tooBig</b>.</li> <li>• <b>No such names—(snmpOutNoSuchNames)</b> Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <b>noSuchName</b>.</li> <li>• <b>Bad values—(snmpOutBadValues)</b> Total number of SNMP PDUs generated by the SNMP entity with an error status field of <b>badValue</b>.</li> <li>• <b>General errors—(snmpOutGenErrs)</b> Total number of SNMP PDUs generated by the SNMP entity with an error status field of <b>genErr</b>.</li> <li>• <b>Get requests—(snmpOutGetRequests)</b> Total number of SNMP <b>GetRequest</b> PDUs generated by the SNMP entity.</li> <li>• <b>Get nexts—(snmpOutGetNexts)</b> Total number of SNMP <b>GetNext</b> PDUs generated by the SNMP entity.</li> <li>• <b>Set requests—(snmpOutSetRequests)</b> Total number of SNMP <b>SetRequest</b> PDUs generated by the SNMP entity.</li> <li>• <b>Get responses—(snmpOutGetResponses)</b> Total number of SNMP <b>GetResponse</b> PDUs generated by the SNMP entity.</li> <li>• <b>Traps—(snmpOutTraps)</b> Total number of SNMP traps generated by the SNMP entity.</li> </ul>

Table 32 on page 234 describes the output fields for the **show snmp statistics subagents** command. Output fields are listed in the approximate order in which they appear.

Table 32: show snmp statistics subagents Output Fields

Field Name	Field Description
<b>Subagent</b>	Location of the SNMP subagent.
<b>Request PDUs</b>	Number of PDUs requested by the SNMP manager.
<b>Response PDUs</b>	Number of response PDUs sent by the SNMP subagent.
<b>Request Variables</b>	Number of variable bindings on the PDUs requested by the SNMP manager.
<b>Response Variables</b>	Number of variable bindings on the PDUs sent by the SNMP subagent.
<b>Average Response Time</b>	Average time taken by the SNMP subagent to send statistics response.
<b>Maximum Response Time</b>	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 big: 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 big: 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



## ssh

**List of Syntax**   [Syntax on page 238](#)  
[Syntax \(EX Series Switch and the QFX Series\) on page 238](#)

**Syntax**   `ssh host`  
                   `<bypass-routing>`  
                   `<inet | inet6>`  
                   `<interface interface-name>`  
                   `<logical-system logical-system-name>`  
                   `<routing-instance routing-instance-name>`  
                   `<source address>`  
                   `<v1 | v2>`

**Syntax (EX Series Switch and the QFX Series)**   `ssh host`  
                   `<bypass-routing>`  
                   `<inet | inet6>`  
                   `<interface interface-name>`  
                   `<routing-instance routing-instance-name>`  
                   `<source address>`  
                   `<v1 | v2>`

**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.

**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.

**routing-instance** *routing-instance-name*—(Optional) Name of the routing instance for the SSH attempt.

**source address**—(Optional) Source address of the SSH connection.

**v1 | v2**—(Optional) Use SSH version 1 or 2, respectively, when connecting to a remote host.

**Additional Information** To configure an SSH (version 1) key for your user account, include the **authentication ssh-rsa** statement at the **[edit system login user *user-name*]** hierarchy level. 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. For details, see the .

**Required Privilege Level** network

**Related Documentation** • *Configuring SSH Host Keys for Secure Copying of Data*

**List of Sample Output** [ssh on page 239](#)

**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
% ...
```

