User and Access Management on the OCX Series

Release
14.1X53

Modified: 2017-01-12

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

User and Access Management on the OCX Series
14.1X53

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at 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:

- OCX1100

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**

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

Convention	Description	Examples
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** ***metric*****>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

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

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.

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 **Protocols>Ospf**.

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**. 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/

- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Introduction to User and Access Management

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

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.

Junos OS Processes

Junos OS running on the Routing Engine and Packet Forwarding Engine consists of multiple processes that are responsible for individual functions.

The separation of functions provides operational stability, because each process accesses its own protected memory space. In addition, because each process is a separate software package, you can selectively upgrade all or part of the Junos OS for added flexibility.

Table 3 on page 4 describes the primary Junos OS processes.

Table 3: Junos OS Processes

Process	Name	Description
Chassis process	chassisd	Detects hardware on the system that is used to configure network interfaces. Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered. Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully.
DNS server process	named-service	Resolves hostnames into addresses.
Dynamic Host Configuration Protocol (DHCP) process	dhcp-service	Enables a DHCP server to allocate network IP addresses and deliver configuration settings to client hosts without user intervention.
Ethernet switching process	eswd	Handles Layer 2 switching functionality such as MAC address learning, Spanning Tree Protocol, and access port security. Manages Ethernet switching interfaces, VLANs, and VLAN interfaces.
Firewall management process	firewall	Manages the firewall configuration and helps accept or reject packets that are transiting an interface on a switch.
Forwarding process	pfem	Defines how routing protocols operate on the partition. The overall performance of the partition is largely determined by the effectiveness of the forwarding process.
Interface process	dcd	Configures and monitors network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.
Integrated Local Management Interface (ILMI) process	ilmi	Provides bidirectional exchange of management information between two ATM interfaces across a physical connection.

Table 3: Junos OS Processes *(continued)*

Process	Name	Description
Link Management Protocol (LMP) process	link-management	Establishes and maintains LMP control channels.
Management process	mgd	Provides communication between the other processes and an interface to the configuration database. Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured. Interacts with the other processes when commands are issued through one of the user interfaces on the partition. If a process terminates or fails to start when called, the management process attempts to restart it a limited number of times to prevent thrashing and logs any failure information for further investigation.
Multicast snooping process	multicast-snooping	Makes Layer 2 devices, such as VLAN switches, aware of Layer 3 information, such as the media access control (MAC) addresses of members of a multicast group.
Secure Neighbor Discovery (SEND) protocol process	send	Protects Neighbor Discovery Protocol (NDP) messages.
Simple Network Management Protocol (SNMP) process	snmp	Enables the monitoring of network devices from a central location and provides the switch's SNMP master agent.
Tunnel OAM process	tunnel-oamd	Enables the Operation, Administration, and Maintenance of Layer 2 tunneled networks. Layer 2 protocol tunneling (L2PT) allows service providers to send Layer 2 protocol data units (PDUs) across the provider's cloud and deliver them to Juniper Networks EX Series Ethernet Switches that are not part of the local broadcast domain.
Virtual Router Redundancy Protocol (VRRP) process	vrrp	Enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts.

Related Documentation

- *Junos OS Baseline Network Operations Guide*
- *Junos OS Administration Library for Routing Devices*

Understanding LLDP

The device uses Link Layer Discovery Protocol (LLDP) to learn and distribute device information on network links. The information enables the switch to identify a variety of devices quickly. This quick identification results in a LAN that interoperates smoothly and efficiently.

LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include specifics, such as chassis and port identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in Junos OS.

The device supports the following basic TLVs:

- **Chassis Identifier**—The MAC address associated with the local system.
- **Port Identifier**—The port identification for the specified port in the local system.
- **Port Description**—The user-configured port description. The port description can be a maximum of 256 characters.
- **System Name**—The user-configured name of the local system. The system name can be a maximum of 256 characters.
- **System Description**—The system description containing information about the software and current image running on the system. This information cannot be configured, but is taken from the software.
- **System Capabilities**—The primary function performed by the system. The capabilities that system supports are defined; for example, bridge or router. This information cannot be configured, but is based on the model of the product.
- **Management Address**—The IP management address of the local system.

The device supports the following 802.3 TLVs:

- **Power via MDI**—A TLV that advertises media dependent interface (MDI) power support, power source equipment (PSE) power pair, and power class information.
- **MAC/PHY Configuration Status**—A TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information cannot be configured, but is based on the physical interface structure.
- **Link Aggregation**—A TLV that advertises whether the port is aggregated and its aggregated port ID.
- **Maximum Frame Size**—A TLV that advertises the Maximum Transmission Unit (MTU) of the interface sending LLDP frames.
- **Port Vlan**—A TLV that advertises the VLAN name configured on the interface.

Monitoring SNMP

There are several commands that you can access in Junos OS operational mode to monitor SNMP information. Some of the commands are:

- **show snmp health-monitor**, which displays the health monitor log and alarm information.
- **show snmp mib**, which displays information from the MIBs, such as device and system information.

- **show snmp statistics**, which displays SNMP statistics such as the number of packets, silent drops, and invalid output values.
- **show snmp rmon**, which displays the RMON alarm, event, history, and log information

The following example provides sample output from the **show snmp health-monitor** command:

```
user@switch> show snmp health-monitor
Alarm
Index  Variable description                          Value State

 32768 Health Monitor: root file system utilization
       jnxHrStoragePercentUsed.1                       58 active

 32769 Health Monitor: /config file system utilization
       jnxHrStoragePercentUsed.2                        0 active

 32770 Health Monitor: RE 0 CPU utilization
       jnxOperatingCPU.9.1.0.0                          0 active

 32773 Health Monitor: RE 0 Memory utilization
       jnxOperatingBuffer.9.1.0.0                      35 active

 32775 Health Monitor: jkernel daemon CPU utilization
       Init daemon                                      0 active
       Chassis daemon                                  50 active
       Firewall daemon                                  0 active
       Interface daemon                                 5 active
       SNMP daemon                                     11 active
       MIB2 daemon                                     42 active
       ...
```

The following example provides sample output from the **show snmp mib** command:

```
user@switch> show snmp mib walk system

sysDescr.0    = Juniper Networks, Inc. qfx3500s internet router, kernel
JUNOS 11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC builder@abc.example.net:
/volume/build/junos/11.1/production/20100926.0/obj-xlr/bsd/sys/compile/JUNIPER-xxxxx

Build date: 2010-09-26 06:00:10 U
sysObjectID.0 = jnxProductQFX3500
sysUpTime.0   = 24444184
sysContact.0  = J Smith
sysName.0     = Lab QFX3500
sysLocation.0 = Lab
sysServices.0 = 4
```

The following example provides sample output from the **show snmp statistics** command:

```
user@switch> show snmp statistics

SNMP statistics:
  Input:
    Packets: 0, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
```



```
Total request varbinds: 0, Total set varbinds: 0,
Get requests: 0, Get nexts: 0, Set requests: 0,
Get responses: 0, Traps: 0,
Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
Throttle drops: 0, Duplicate request drops: 0
Output:
Packets: 0, Too bigs: 0, No such names: 0,
Bad values: 0, General errors: 0,
Get requests: 0, Get nexts: 0, Set requests: 0,
Get responses: 0, Traps: 0
```

Related Documentation

- health-monitor on page 189
- *show snmp mib*
- show snmp statistics on page 275

CHAPTER 2

Understanding Access and Authentication Methods

Understanding Junos OS Access Privilege Levels

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

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

The following sections provide additional information about permissions:

Junos OS Login Class Permission Flags

The **permissions** statement specifies one or more of the permission flags listed in Table 4 on page 10. Permission flags are not cumulative, so for each class you must list all the permission flags needed, including **view** to display information and **configure** to enter configuration mode. Two forms of permissions control for individual parts of the configuration are:

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

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

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

Permission Flag	Description
flow-tap-operation	Can make flow-tap requests to the router or switch. For example, a Dynamic Tasking Control Protocol (DTCP) client must have **flow-tap-operation** permission to authenticate itself to the Junos OS as an administrative user. NOTE: The **flow-tap-operation** option is not included in the **all-control** permissions flag.
idp-profiler-operation	Can view profiler data.
interface	Can view the interface configuration in configuration mode and with the **show configuration** operational mode command.
interface-control	Can view chassis, class of service (CoS), groups, forwarding options, and interfaces configuration information. Can edit configuration at the following hierarchy levels: • **[edit chassis]** • **[edit class-of-service]** • **[edit groups]** • **[edit forwarding-options]** • **[edit interfaces]**
maintenance	Can perform system maintenance, including starting a local shell on the router or switch and becoming the superuser in the shell by using the **su root** command, and can halt and reboot the router or switch by using the **request system** commands.
network	Can access the network by using the **ping**, **ssh**, **telnet**, and **traceroute** commands.
pgcp-session-mirroring	Can view the **pgcp** session mirroring configuration.
pgcp-session-mirroring-control	Can modify the **pgcp** session mirroring configuration.
reset	Can restart software processes by using the **restart** command and can configure whether software processes are enabled or disabled at the **[edit system processes]** hierarchy level.
rollback	Can use the **rollback** command to return to a previously committed configuration other than the most recently committed one.
routing	Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.

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

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

Allowing or Denying Individual Commands for Junos OS Login Classes

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

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

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

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

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

Related Documentation

- Example: Configuring User Permissions with Access Privilege Levels on page 19
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 41
- *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 113

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

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 127

PART 2

Configuring Access

CHAPTER 3

Configuring and Managing Root Users

Configuring Management Access

To define the management access settings for the routing platform:

1. Next to Allow Telnet Access, select the check box to allow remote Telnet access to the routing platform.
2. Next to Allow SSH Access, selected the check box to allow remote SSH access to the routing platform.
3. Click **Apply** to apply the configuration.

Related Documentation

- Configuring Junos OS User Accounts on page 106
- Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 63
- Example: Configuring User Permissions with Access Privilege Levels on page 19

Example: Configuring User Permissions with Access Privilege Levels

This example shows how to view permissions for a user account and configure the user permissions with access privileges for a login class. This enables users to execute only those commands and configure and view only those statements for which they have

access privileges. This prevents unauthorized users from executing or configuring sensitive commands and statements that could potentially cause damage to the network.

Requirements

This example uses the following hardware and software components:

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

Before you begin:

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

  For information on configuring a TACACS+ server, see *Configuring TACACS+ Authentication*.

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

Overview

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

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

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

To configure user access privilege levels:

1. View permissions for a user account.

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

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

   ```
   [edit]
   ?
   ```

2. Configure user permissions with access privileges.

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

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

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

Configuration

Configuring User Permissions with Access Privilege Levels

Step-by-Step Procedure

To configure access privileges:

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

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

```
message
  show                  Show system information
  ssh                   Start secure shell on another host
  start                 Start shell
  telnet                Telnet to another host
  test                  Perform diagnostic debugging
  traceroute            Trace route to remote host
```

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

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

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

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

Results

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

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

Verification

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

- Verifying SNMP Configuration on page 22
- Verifying non-SNMP Configuration on page 23

Verifying SNMP Configuration

Purpose Verify that SNMP configuration can be executed.

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

```
[edit snmp]
user@host# set name device1
user@host# set description switch1
user@host# set location Lab1
```

```
user@host# set contact example.com
user@host# commit
```

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

Verifying non-SNMP Configuration

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

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

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

Related Documentation

- Understanding Junos OS Access Privilege Levels on page 9
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 41

Configuring Login Tips

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

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

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

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

Related Documentation

- *Defining Junos OS Login Classes*

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: ABC123
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*

Example: Configuring a Plain-Text Password for Root Logins

This example shows how to configure a plain-text password for the root-level user (whose username is *root*). Configuring a plain-text password is one way to protect access to the root level by unauthorized users. You must prevent unauthorized users from gaining access to superuser commands that can be used to alter your system configuration.

Requirements

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

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

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

Overview

Junos OS is preinstalled on the router. When the router is powered on, it is ready to be configured. Initially, you log in as the root-level user with no password. To set the root

password, you have several options. This example shows how to enter a plain-text password that Junos OS then encrypts for you.

Configuration

CLI Quick Configuration

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

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

Configuring a Plain-Text Password for User Root

Step-by-Step Procedure

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

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

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

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

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

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

Results

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

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

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

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

Verification

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

Purpose

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

Action

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

```
user@host> show configuration system
```

```
root-authentication {
    encrypted-password "$ABC123"; ## SECRET-DATA
}
```

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

Related Documentation

- *root-authentication*
- Special Requirements for Junos OS Plain-Text Passwords on page 38
- *Configuring Special Requirements for Plain-Text Passwords*
- *Changing the Requirements for Junos OS Plain-Text Passwords*

Example: Configuring SSH Authentication for Root Logins

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

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

Related Documentation

- *Configuring the Root Password*
- Special Requirements for Junos OS Plain-Text Passwords on page 38

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 27 provides a list of some of the troubleshooting resources.

Table 5: 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.	*Chassis Alarm Messages on a QFX3500 Device*

Table 5: Troubleshooting Resources on the QFX and OCX Series *(continued)*

Troubleshooting Resource	Description	Documentation
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.	*Chassis Status LEDs on a QFX3500 Device*
Interface alarms	A predefined alarm (red or yellow) for an interface type is triggered when an interface of that type goes down.	*Interface Alarm Messages*
System alarms	A predefined alarm is triggered by a missing rescue configuration or problem with the software license.	*Understanding Alarms*
System log messages	The system log includes details of system and user events, including errors. Specify the severity and type of system log messages you wish to view or save, and configure the output to be sent to local or remote hosts.	• *Overview of Single-Chassis System Logging Configuration* • *Junos OS System Log Configuration Statements*
Junos OS operational mode commands	Operational mode commands can be used to monitor switch performance and current activity on the network. For example, use the **traceroute monitor** command to locate points of failure in a network.	• *Monitoring System Process Information* • *Monitoring System Properties* • *traceroute monitor*
Junos OS automation scripts (event scripts)	Event scripts can be used to automate network troubleshooting and management tasks.	*Automation Scripting Feature Guide*
Junos OS XML operational tags	XML operational tags are equivalent in function to operational mode commands in the CLI, which you can use to retrieve status information for a device.	*Junos XML API Operational Developer Reference*
NETCONF XML management protocol	The NETCONF XML management protocol defines basic operations that are equivalent to Junos OS CLI configuration mode commands. Client applications use the protocol operations to display, edit, and commit configuration statements (among other operations), just as administrators use CLI configuration mode commands such as **show**, **set**, and **commit** to perform those operations.	*NETCONF XML Management Protocol Developer Guide*
SNMP MIBs and traps	MIBs enable the monitoring of network devices from a central location. For example, use the Traceroute MIB to monitor devices remotely.	• *SNMP MIBs Support* • *SNMP Traps Support* • *Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS*

Table 5: Troubleshooting Resources on the QFX and OCX Series *(continued)*

Troubleshooting Resource	Description	Documentation
AI-Scripts and Advanced Insight Manager (AIM)	AI-Scripts installed on the switch can automatically detect and monitor faults on the switch, and depending on the configuration on the AIM application, send notifications of potential problems and submit problem reports to Juniper Support Systems.	*Advanced Insight Scripts (AI-Scripts) Release Notes*
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.	*Service Automation*
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.	*Service Automation*
Juniper Networks Knowledge Base	You can search in this database for Juniper Networks product information, including alerts and troubleshooting tips.	http://kb.juniper.net

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 29 provides a list of problem categories, summary of the symptom or problem, and recommended actions with links to the troubleshooting documentation.

Table 6: Troubleshooting on the QFX Series

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

Table 6: Troubleshooting on the QFX Series *(continued)*

Problem Category	Symptom or Problem	Recommended Action
Port configuration	Cannot configure a port as a Gigabit Ethernet port.	Check whether the port is a valid Gigabit Ethernet port (6 through 41). See *QFX3500 Device Overview*.
	Cannot configure a port as a Fibre Channel port.	Check whether the port is a valid Fibre Channel port (0 through 5 and 42 through 47). See *QFX3500 Device Overview*.
	Cannot configure a port as a 10-Gigabit Ethernet port.	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. 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. See *QFX3500 Device Overview*.
	Cannot configure a 40-Gbps QSFP+ interface.	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. See *QFX3500 Device Overview*.
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.	Configure the management ports from the console port. You cannot configure the management ports by directly connecting to them. NOTE: The management ports are on the front panel of the QFX3500 switch. They are labeled **C0** and **C1** on the front panel. In the CLI they are referred to as **me0** and **me1**. See *Configuring a QFX3500 Device as a Standalone Switch*.

Table 6: Troubleshooting on the QFX Series *(continued)*

Problem Category	Symptom or Problem	Recommended Action
Software upgrade and configuration	Failed software upgrade.	See *Recovering from a Failed Software Installation*.
	Active partition becomes inactive after upgrade.	
	Problem with the active configuration file.	See the following topics: • *Loading a Previous Configuration File* • *Reverting to the Default Factory Configuration* • *Reverting to the Rescue Configuration* • *Performing a Recovery Installation*
	Root password is lost or forgotten.	Recover the root password. See "Recovering the Root Password" on page 23.
Network interfaces	An aggregated Ethernet interface is down.	See *Troubleshooting an Aggregated Ethernet Interface*.
	Interface on built-in network port is down.	See *Troubleshooting Network Interfaces*.
	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 *Troubleshooting Ethernet Switching*.
Firewall filter	Firewall configuration exceeded available Ternary Content Addressable Memory (TCAM) space.	See *Troubleshooting Firewall Filters*.

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: ABC123
    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*

CHAPTER 4

Configuring and Managing User Accounts

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.
- User identifier (UID)—(Optional) Numeric identifier that is associated with the user account name. The identifier must be in the range from 100 through 64,000 and must be unique within the switch. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.
- You must ensure that the UID is unique. However, it is possible to assign the same UID to different users. If you do this, the CLI displays a warning when you commit the configuration and then assigns the duplicate UID.
- User's access privilege—(Required) One of the login classes you defined in the **class** statement at the **[edit system login]** hierarchy level, or one of the default classes listed in "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 41.
- Authentication method or methods and passwords that the user can use to access the switch—(Optional) You can use SSH or a Message Digest 5 (MD5) password, or you can enter a plain-text password that Junos OS encrypts using MD5-style encryption before entering it in the password database. For each method, you can specify the user's password. If you configure the **plain-text-password** option, you are prompted to enter and confirm the password:

  [edit system login user *user-name*]
  user@switch# **set authentication plain-text-password**
  New password: *type password here*
  Retype new password: *retype password here*

  The default requirements for plain-text passwords are:

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

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

For SSH authentication, you can also copy the contents of an SSH key file into the configuration.

To load an SSH key file, use the **load-key-file** statement. This statement loads RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys.

If you load the SSH keys file, the contents of the file are copied into the configuration immediately after you enter the **load-key-file** statement. To view the SSH key entries, use the configuration mode **show** command. For example:

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

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

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

Related Documentation

- Configuring Junos OS User Accounts on page 106
- Junos OS Login Classes Overview on page 37

Junos OS Login Classes Overview

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

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

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

The Junos operating system (Junos OS) contains a few predefined login classes, which are listed in Table 7 on page 37. The predefined login classes cannot be modified.

Table 7: Predefined System Login Classes

Login Class	Permission Flag Set
operator	clear, network, reset, trace, and view
read-only	view
superuser or **super-user**	all

Table 7: Predefined System Login Classes *(continued)*

Login Class	Permission Flag Set
unauthorized	None

NOTE:

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

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

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

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

Related Documentation

- *Defining Junos OS Login Classes*

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 38 shows the default requirements.

Table 8: 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
You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.	You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
Valid passwords must contain at least one change of case or character class.	Passwords must use at least three of the five defined character classes (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters).

You can change the requirements for plain-text passwords.

Junos OS supports the following five character classes for plain-text passwords:

- Lowercase letters
- Uppercase letters

- Numbers
- Punctuation
- Special characters: ! @ # $ % ^ & * , +< >

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**, **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. Instead, you can use the sha256 or sha512 to specify passwords. Using a 256-bit or 512-bit cryptographic hash algorithm results in 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;
}
```

Release History Table

Release	Description
13.3	Starting with Junos OS Release 13.3, the **sha1** does not enable secure, protected specification of passwords. Instead, you can use the **sha256** or **sha512** to specify passwords.

Related Documentation

- *Changing the Requirements for Junos OS Plain-Text Passwords*
- *Configuring the Root Password*

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

This topic contains the following sections:

Understanding Regular Expressions

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

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

Table 9 on page 42 differentiates the local and remote authentication configuration using regular expressions.

Table 9: Sample Local and Remote Authentication Configuration Using Regular Expressions

Local Configuration	Remote Configuration

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

NOTE:

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

Specifying Regular Expressions

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

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

Regular expressions for commands and configuration statements should be specified in the same manner as executing the complete command or statement.
Table 10 on page 43 lists the regular expressions for configuring access privileges for the **[edit interfaces]** and **[edit vlans]** statement hierarchies, and for the **delete interfaces** command.

Table 10: Specifying Regular Expressions

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

Table 10: Specifying Regular Expressions *(continued)*

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

Regular Expressions Operators

Table 11 on page 45 lists common regular expression operators that you can use for allowing or denying operational and configuration modes.

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

Table 11: Common Regular Expression Operators

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

Table 11: Common Regular Expression Operators *(continued)*

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

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

Regular Expression Examples

Table 12 on page 47 lists the regular expressions used to allow configuration options under two configuration hierarchies—**[edit system ntp server]** and **[edit protocols rip]**—as an example for specifying regular expressions.

NOTE: Table 12 on page 47 does not provide a comprehensive list of all regular expressions and keywords for all configuration statements and hierarchies. The regular expressions listed in the table are supported in Junos OS Release 16.1, and are validated only for the **[edit system ntp server]** and **[edit protocols rip]** statement hierarchies.

Table 12: Regular Expressions Examples

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

Table 12: Regular Expressions Examples *(continued)*

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

Related Documentation

- *Example: Configuring User Permissions with Access Privileges for Operational Mode Commands, Configuration Statements, and Hierarchies*
- *Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies*
- Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 63
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 41

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

This topic contains the following sections:

Understanding Regular Expressions

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

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

Table 9 on page 42 differentiates the local and remote authentication configuration using regular expressions.

Table 13: Sample Local and Remote Authentication Configuration Using Regular Expressions

Local Configuration	Remote Configuration

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

NOTE:

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

Specifying Regular Expressions

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

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

Regular expressions for commands and configuration statements should be specified in the same manner as executing the complete command or statement.
Table 10 on page 43 lists the regular expressions for configuring access privileges for the **[edit interfaces]** and **[edit vlans]** statement hierarchies, and for the **delete interfaces** command.

Table 14: Specifying Regular Expressions

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

Table 14: Specifying Regular Expressions *(continued)*

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

Regular Expressions Operators

Table 11 on page 45 lists common regular expression operators that you can use for allowing or denying operational and configuration modes.

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

Table 15: Common Regular Expression Operators

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

Table 15: Common Regular Expression Operators *(continued)*

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

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

Regular Expression Examples

Table 12 on page 47 lists the regular expressions used to allow configuration options under two configuration hierarchies—**[edit system ntp server]** and **[edit protocols rip]**—as an example for specifying regular expressions.

NOTE: Table 12 on page 47 does not provide a comprehensive list of all regular expressions and keywords for all configuration statements and hierarchies. The regular expressions listed in the table are supported in Junos OS Release 16.1, and are validated only for the **[edit system ntp server]** and **[edit protocols rip]** statement hierarchies.

Table 16: Regular Expressions Examples

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

Table 16: Regular Expressions Examples *(continued)*

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

Related Documentation

- *Example: Configuring User Permissions with Access Privileges for Operational Mode Commands, Configuration Statements, and Hierarchies*
- *Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies*
- Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 63
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 41

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Related Documentation

- *Example: Configuring User Permissions with Access Privileges for Operational Mode Commands, Configuration Statements, and Hierarchies*
- *Specifying Access Privileges for Junos OS Configuration Mode Hierarchies*
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 41
- *Defining Junos OS Login Classes*
- Understanding Junos OS Access Privilege Levels on page 9

Example: Configuring User Accounts

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

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

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

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

Requirements

This example uses the following hardware and software components:

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

Before you begin:

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

  For information on configuring a TACACS+ server, see *Configuring TACACS+ Authentication*.

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

Overview

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

The access privileges for each login class are defined by one or more permission flags specified in the **permissions** statement. Permission flags are used to grant a user access to operational mode commands, statements, and configuration hierarchies. Permission flags are not cumulative, so for each login class you must list all the permission flags needed, including **view** to display information and **configure** to enter configuration mode. By specifying a specific permission flag on the user's login class, you grant the user access to the corresponding commands, statements, and configuration hierarchies. To grant

access to all commands and configuration statements, use the **all** permissions flag. The permission flags provide read-only ("plain" form) and read and write (form that ends in -control) capability for a permission type.

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

To configure user access privilege levels:

1. View permissions for a user account.

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

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

   ```
   [edit]
   ?
   ```

2. Configure user permissions with access privileges.

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

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

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

Configuration

Configuring User Permissions with Access Privilege Levels

Step-by-Step Procedure

To configure access privileges:

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

   ```
   [edit]
   user@host> ?
     Possible completions:
       clear                Clear information in the system
       configure            Manipulate software configuration information
       file                 Perform file operations
       help                 Provide help information
       load                 Load information from file
       monitor              Show real-time debugging information
       mtrace               Trace multicast path from source to receiver
       op                   Invoke an operation script
       ping                 Ping remote target
       quit                 Exit the management session
   ```

```
  request              Make system-level requests
  restart              Restart software process
  save                 Save information to file
  set                  Set CLI properties, date/time, craft interface
message
  show                 Show system information
  ssh                  Start secure shell on another host
  start                Start shell
  telnet               Telnet to another host
  test                 Perform diagnostic debugging
  traceroute           Trace route to remote host
```

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

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

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

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

Results

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

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

Verification

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

- Verifying SNMP Configuration on page 62
- Verifying non-SNMP Configuration on page 63

Verifying SNMP Configuration

Purpose Verify that SNMP configuration can be executed.

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

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

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

Verifying non-SNMP Configuration

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

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

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

Related Documentation

- Understanding Junos OS Access Privilege Levels on page 9
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 41

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

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

Requirements

This example uses the following hardware and software components:

- One Juniper Networks device
- One TACACS+ (or RADIUS) server

- Junos OS build running on the Juniper Networks device

Before you begin:

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

  For information on configuring a TACACS+ server, see *Configuring TACACS+ Authentication*.

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

Overview and Topology

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

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

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

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

Configuration Notes

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

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

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

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

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

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

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

- Regular expressions for **allow-commands** and **deny-commands** statements can also include the **commit**, **load**, **rollback**, **save**, **status**, and **update** commands.

- If the regular expression contains any spaces, operators, or wildcard characters, enclose the expression in quotation marks. Regular expressions are not case-sensitive, for example, **allow-commands** *"show interfaces"*;

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

  Incorrect configuration:

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

  Correct configuration:

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

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

  For example:

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


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

Topology

Figure 1: Configuring TACACS+ Server Authentication

Figure 1 on page 66 illustrates a simple topology, where Router R1 is a Juniper Networks device and has a TCP connection established with a TACACS+ server.

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

The purpose of each login class is as follows:

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

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

Configuration

CLI Quick Configuration

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

R1

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

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

Configuring Authentication Parameters for Router R1

Step-by-Step Procedure

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

To configure Router R1 authentication:

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

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

2. Establish R1 connection with the TACACS+ server.

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

3. Configure RADIUS server authentication parameters.

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

4. Configure R1 accounting configuration parameters.

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

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

Step-by-Step Procedure

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

1. Configure Class1 custom login class and assign operator-level user permissions. For information on the predefined system login classes, see the "Junos OS Login Classes Overview" on page 37.

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

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

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

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

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

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

Step-by-Step Procedure

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

1. Configure the Class2 custom login class and assign operator-level user permissions. For information on the predefined system login classes, see the "Junos OS Login Classes Overview" on page 37.

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

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

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

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

   ```
   user@R1# set login user User2 uid 2002
   user@R1# set login user User2 class Class2
   ```

```
user@R1# set login user User2 authentication encrypted-password "$ABC123"
```

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

Step-by-Step Procedure

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

1. Configure the Class3 custom login class and assign superuser-level user permissions. For information on the predefined system login classes, see the "Junos OS Login Classes Overview" on page 37.

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

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

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

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

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

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

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

Results

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

```
user@R1# show system
authentication-order [ tacplus radius password ];
radius-server {
  10.209.1.66 secret "$ABC123";
}
tacplus-server {
  10.209.1.66;
}
radius-options {
  enhanced-accounting;
}
tacplus-options {
  enhanced-accounting;
}
accounting {
  events [ login change-log interactive-commands ];
  traceoptions {
```

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

Verification

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

- Verifying Class1 Configuration on page 71
- Verifying Class2 Configuration on page 72
- Verifying Class3 Configuration on page 72

Verifying Class1 Configuration

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

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

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

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

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

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

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

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

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

Verifying Class2 Configuration

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

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

```
User2@R1> ping 10.209.1.66
ping 10.209.1.66
PING 10.209.1.66 (10.209.1.66): 56 data bytes
64 bytes from 10.209.1.66: icmp_seq=0 ttl=52 time=212.521 ms
64 bytes from 10.209.1.66: icmp_seq=1 ttl=52 time=212.844 ms
64 bytes from 10.209.1.66: icmp_seq=2 ttl=52 time=211.304 ms
64 bytes from 10.209.1.66: icmp_seq=3 ttl=52 time=210.963 ms
^C
--- 10.209.1.66 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 210.963/211.908/212.844/0.792 ms
```

From the CLI prompt, check the available permissions.

```
User2@R1> ?
Possible completions:
  clear               Clear information in the system
  file                Perform file operations
  help                Provide help information
  load                Load information from file
  monitor             Show real-time debugging information
  mtrace              Trace multicast path from source to receiver
  op                  Invoke an operation script
  ping                Ping remote target
  quit                Exit the management session
  request             Make system-level requests
  restart             Restart software process
  save                Save information to file
  show                Show system information
  ssh                 Start secure shell on another host
  start               Start shell
  telnet              Telnet to another host
  test                Perform diagnostic debugging
  traceroute          Trace route to remote host
```

From the CLI prompt, execute any set command.

```
User2@R1> set
            ^
unknown command.
```

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

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

Verifying Class3 Configuration

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

Action From the CLI prompt, check the available permissions.

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

From the operational mode, enter configuration mode.

```
User3@R1> configure
Entering configuration mode

[edit]
User3@R1#
```

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

Related Documentation

- Understanding Junos OS Access Privilege Levels on page 9
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 41
- *Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies*
- *Example: Configuring User Permissions with Access Privileges for Operational Mode Commands, Configuration Statements, and Hierarchies*

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 74
- Overview on page 74
- Configuration on page 74

Requirements

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

Overview

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

Configuration

CLI Quick Configuration

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

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

Configuring Requirements for Plain-Text Passwords

Step-by-Step Procedure

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

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

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

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

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

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

   ```
   [edit system login password]
   ```

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

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

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

Results

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

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

Related Documentation

- Special Requirements for Junos OS Plain-Text Passwords on page 38
- *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 27 provides a list of some of the troubleshooting resources.

Table 17: 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.	*Chassis Alarm Messages on a QFX3500 Device*
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.	*Chassis Status LEDs on a QFX3500 Device*
Interface alarms	A predefined alarm (red or yellow) for an interface type is triggered when an interface of that type goes down.	*Interface Alarm Messages*
System alarms	A predefined alarm is triggered by a missing rescue configuration or problem with the software license.	*Understanding Alarms*

Table 17: Troubleshooting Resources on the QFX and OCX Series *(continued)*

Troubleshooting Resource	Description	Documentation
System log messages	The system log includes details of system and user events, including errors. Specify the severity and type of system log messages you wish to view or save, and configure the output to be sent to local or remote hosts.	• *Overview of Single-Chassis System Logging Configuration* • *Junos OS System Log Configuration Statements*
Junos OS operational mode commands	Operational mode commands can be used to monitor switch performance and current activity on the network. For example, use the **traceroute monitor** command to locate points of failure in a network.	• *Monitoring System Process Information* • *Monitoring System Properties* • *traceroute monitor*
Junos OS automation scripts (event scripts)	Event scripts can be used to automate network troubleshooting and management tasks.	*Automation Scripting Feature Guide*
Junos OS XML operational tags	XML operational tags are equivalent in function to operational mode commands in the CLI, which you can use to retrieve status information for a device.	*Junos XML API Operational Developer Reference*
NETCONF XML management protocol	The NETCONF XML management protocol defines basic operations that are equivalent to Junos OS CLI configuration mode commands. Client applications use the protocol operations to display, edit, and commit configuration statements (among other operations), just as administrators use CLI configuration mode commands such as **show**, **set**, and **commit** to perform those operations.	*NETCONF XML Management Protocol Developer Guide*
SNMP MIBs and traps	MIBs enable the monitoring of network devices from a central location. For example, use the Traceroute MIB to monitor devices remotely.	• *SNMP MIBs Support* • *SNMP Traps Support* • *Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS*
AI-Scripts and Advanced Insight Manager (AIM)	AI-Scripts installed on the switch can automatically detect and monitor faults on the switch, and depending on the configuration on the AIM application, send notifications of potential problems and submit problem reports to Juniper Support Systems.	*Advanced Insight Scripts (AI-Scripts) Release Notes*
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.	*Service Automation*

Table 17: Troubleshooting Resources on the QFX and OCX Series *(continued)*

Troubleshooting Resource	Description	Documentation
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.	*Service Automation*
Juniper Networks Knowledge Base	You can search in this database for Juniper Networks product information, including alerts and troubleshooting tips.	http://kb.juniper.net

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 29 provides a list of problem categories, summary of the symptom or problem, and recommended actions with links to the troubleshooting documentation.

Table 18: Troubleshooting on the QFX Series

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

Table 18: Troubleshooting on the QFX Series *(continued)*

Problem Category	Symptom or Problem	Recommended Action
Port configuration	Cannot configure a port as a Gigabit Ethernet port.	Check whether the port is a valid Gigabit Ethernet port (6 through 41). See *QFX3500 Device Overview*.
	Cannot configure a port as a Fibre Channel port.	Check whether the port is a valid Fibre Channel port (0 through 5 and 42 through 47). See *QFX3500 Device Overview*.
	Cannot configure a port as a 10-Gigabit Ethernet port.	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. 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. See *QFX3500 Device Overview*.
	Cannot configure a 40-Gbps QSFP+ interface.	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. See *QFX3500 Device Overview*.
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.	Configure the management ports from the console port. You cannot configure the management ports by directly connecting to them. NOTE: The management ports are on the front panel of the QFX3500 switch. They are labeled **C0** and **C1** on the front panel. In the CLI they are referred to as **me0** and **me1**. See *Configuring a QFX3500 Device as a Standalone Switch*.

Table 18: Troubleshooting on the QFX Series *(continued)*

Problem Category	Symptom or Problem	Recommended Action
Software upgrade and configuration	Failed software upgrade.	See *Recovering from a Failed Software Installation*.
	Active partition becomes inactive after upgrade.	
	Problem with the active configuration file.	See the following topics: • *Loading a Previous Configuration File* • *Reverting to the Default Factory Configuration* • *Reverting to the Rescue Configuration* • *Performing a Recovery Installation*
	Root password is lost or forgotten.	Recover the root password. See "Recovering the Root Password" on page 23.
Network interfaces	An aggregated Ethernet interface is down.	See *Troubleshooting an Aggregated Ethernet Interface*.
	Interface on built-in network port is down.	See *Troubleshooting Network Interfaces*.
	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 *Troubleshooting Ethernet Switching*.
Firewall filter	Firewall configuration exceeded available Ternary Content Addressable Memory (TCAM) space.	See *Troubleshooting Firewall Filters*.

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: ABC123
    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

CHAPTER 5

Configuring and Managing Local Password Authentication

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.

- User identifier (UID)—(Optional) Numeric identifier that is associated with the user account name. The identifier must be in the range from 100 through 64,000 and must be unique within the switch. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.
- You must ensure that the UID is unique. However, it is possible to assign the same UID to different users. If you do this, the CLI displays a warning when you commit the configuration and then assigns the duplicate UID.
- User's access privilege—(Required) One of the login classes you defined in the **class** statement at the **[edit system login]** hierarchy level, or one of the default classes listed in "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 41.
- Authentication method or methods and passwords that the user can use to access the switch—(Optional) You can use SSH or a Message Digest 5 (MD5) password, or you can enter a plain-text password that Junos OS encrypts using MD5-style encryption before entering it in the password database. For each method, you can specify the user's password. If you configure the **plain-text-password** option, you are prompted to enter and confirm the password:

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

  The default requirements for plain-text passwords are:

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

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

For SSH authentication, you can also copy the contents of an SSH key file into the configuration.

To load an SSH key file, use the **load-key-file** statement. This statement loads RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys.

If you load the SSH keys file, the contents of the file are copied into the configuration immediately after you enter the **load-key-file** statement. To view the SSH key entries, use the configuration mode **show** command. For example:

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

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

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

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

Related Documentation

- Configuring Junos OS User Accounts on page 106
- Junos OS Login Classes Overview on page 37

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 113

Junos OS Login Classes Overview

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

- Access privileges that users have when they are logged in to the router or switch

- Commands and statements that users can and cannot specify
- How long a login session can be idle before it times out and the user is logged out

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

The Junos operating system (Junos OS) contains a few predefined login classes, which are listed in Table 7 on page 37. The predefined login classes cannot be modified.

Table 19: Predefined System Login Classes

Login Class	Permission Flag Set
operator	clear, network, reset, trace, and view
read-only	view
superuser or **super-user**	all
unauthorized	None

NOTE:

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

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

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

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

Related Documentation

- *Defining Junos OS Login Classes*

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

This topic contains the following sections:

Understanding Regular Expressions

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

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

Table 9 on page 42 differentiates the local and remote authentication configuration using regular expressions.

Table 20: Sample Local and Remote Authentication Configuration Using Regular Expressions

Local Configuration	Remote Configuration

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

NOTE:

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

Specifying Regular Expressions

WARNING: When you specify regular expression for commands and configuration statements, pay close attention to the following examples, as regular expression with invalid syntax might not produce the desired results, even if the configuration is committed without any error.

Regular expressions for commands and configuration statements should be specified in the same manner as executing the complete command or statement.
Table 10 on page 43 lists the regular expressions for configuring access privileges for the **[edit interfaces]** and **[edit vlans]** statement hierarchies, and for the **delete interfaces** command.

Table 21: Specifying Regular Expressions

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

Table 21: Specifying Regular Expressions *(continued)*

Statement	Regular Expression	Configuration Notes
[edit vlans] The **set** command for VLANs is executed as follows: [edit] user@host# **set vlans** *vlan-name* **vlan-id** *vlan-id*	Here, the **set vlans** statement is incomplete by itself, and requires the **vlan-id** option to execute the statement. As a result, the regular expression required for allowing the **set vlans** configuration must specify the entire executable string with the **.*** operator in place of statement variables: [edit system login class *class-name*] user@host# **set permissions** *configure* user@host# **set allow-configuration** *"vlans .* vlan-id .*"*	• The **.*** operator denotes everything from the specified point onward for that particular command or statement. In this example, it denotes any VLAN name with any VLAN ID. • Other valid options under the **[edit vlans]** statement hierarchy can be included in the regular expression, for example: [edit system login class *class-name*] user@host# **set permissions** *configure* user@host# **set allow-configuration-regexps** *["vlans .* vlan-id .*" "vlans .* vlan-id .* description .*" "vlans .* vlan-id .* filter .*"]*

Regular Expressions Operators

Table 11 on page 45 lists common regular expression operators that you can use for allowing or denying operational and configuration modes.

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

Table 22: Common Regular Expression Operators

Operator	Match	Example
|	One of two or more terms separated by the pipe. Each term must be a complete standalone expression enclosed in parentheses ( ), with no spaces between the pipe and the adjacent parentheses.	[edit system login class *test*] user@host# **set permissions** *configure* user@host# **set allow-commands** *"(ping)|(traceroute)|(show system alarms)|(show system software)"* user@host# **set deny-configuration** *"(access)|(access-profile)|(accounting-options)|(applications)|(apply-groups)|(bridge-domains)|(chassis)|(class-of-service)"* With the above configuration, the users assigned to the test login class have operational mode access restricted to only the commands specified in the **allow-commands** statement, and access to the configuration mode, excluding the hierarchy levels specified in the **deny-configuration** statement.

Table 22: Common Regular Expression Operators *(continued)*

Operator	Match	Example
^	At the beginning of an expression, used to denote where the command begins, where there might be some ambiguity.	[edit system login class *test*] user@host# **set permissions** *interface* user@host# **set permissions** *interface-control* user@host# **set allow-commands** *"(^show) (log|interfaces|policer))|(^monitor)"* With the above configuration, the users assigned to the test login class have access to configuring and viewing interface configuration from the operational and configuration mode. The **allow-commands** statement specifies access to commands that begin with **show** and **monitor** keywords. For the first filter, the commands specified include the **show log**, **show interfaces**, and **show policer** commands. The second filter specifies all commands starting with the **monitor** keyword, such as **monitor interfaces** or **monitor traffic** commands.
$	Character at the end of a command. Used to denote a command that must be matched exactly up to that point.	[edit system login class *test*] user@host# **set permissions** *interface* user@host# **set allow-commands** *"(show interfaces$)"* With the above configuration, the users assigned to the test login class can view the interface configuration in the configuration mode and with the **show configuration** operational mode command with the interface user permission. However, the regular expression specified in the **allow-commands** statement restricts the users to execute only the **show interfaces** command and denies access to the command extensions, such as **show interfaces detail** or **show interfaces extensive**.
[ ]	Range of letters or digits. To separate the start and end of a range, use a hyphen (-).	[edit system login class *test*] user@host# **set permissions** *clear* user@host# **set permissions** *configure* user@host# **set permissions** *network* user@host# **set permissions** *trace* user@host# **set permissions** *view* user@host# **set allow-configuration-regexps** *["interfaces [gx]e-.* unit [0-9]* description .*"]* With the above configuration, the users assigned to the test login class have operator-level user permissions, and have access to configure interfaces within the specified range of interface name and unit number (0 through 9).
( )	A group of commands, indicating a complete, standalone expression to be evaluated. The result is then evaluated as part of the overall expression. Parentheses must be used in conjunction with pipe operators, as explained.	[edit system login class *test*] user@host# **set permissions** *all* user@host# **set allow-commands** *"(clear)|(configure)"* user@host# **deny-commands** *"(mtrace)|(start)|(delete)"* With the above configuration, users assigned to the test login class have superuser-level permissions, and have access to the commands specified in the **allow-commands** statement.

Table 22: Common Regular Expression Operators *(continued)*

Operator	Match	Example
*	Zero or more terms.	[edit system login class *test*] user@host# **set permissions *configure*** user@host# **set deny-configuration *"(system login class m*)"*** With the above configuration, users assigned to the test login class whose login username begins with **m** are denied configuration access.
+	One or more terms.	[edit system login class *test*] user@host# **set permissions *configure*** user@host# **set deny-configuration *"(system login class m+)"*** With the above configuration, users assigned to the test login class whose login username begins with **m** are denied configuration access.
.	Any character except for a space " ".	[edit system login class *test*] user@host# **set permissions *configure*** user@host# **set deny-configuration *"(system login class m.)"*** With the above configuration, users assigned to the test login class whose login username begins with **m** are denied configuration access.
.*	Everything from the specified point onward.	[edit system login class *test*] user@host# **set permissions *configure*** user@host# **set deny-configuration *"(system login class m .*)"*** With the above configuration, users assigned to the test login class whose login username begins with **m** are denied configuration access. Similarly, the **deny-configuration "protocols .*"** statement denies all configuration access under the **[edit protocols]** hierarchy level. NOTE: • The *****, **+**, and **.** operations can be achieved by using **.***. • The **deny-commands .*** and **deny-configuration .*** statements deny access to all operational mode commands and configuration hierarchies, respectively.

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

Regular Expression Examples

Table 12 on page 47 lists the regular expressions used to allow configuration options under two configuration hierarchies—**[edit system ntp server]** and **[edit protocols rip]**—as an example for specifying regular expressions.

NOTE: Table 12 on page 47 does not provide a comprehensive list of all regular expressions and keywords for all configuration statements and hierarchies. The regular expressions listed in the table are supported in Junos OS Release 16.1, and are validated only for the **[edit system ntp server]** and **[edit protocols rip]** statement hierarchies.

Table 23: Regular Expressions Examples

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

Table 23: Regular Expressions Examples *(continued)*

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

Related Documentation

- *Example: Configuring User Permissions with Access Privileges for Operational Mode Commands, Configuration Statements, and Hierarchies*
- *Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies*
- Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 63
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 41

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

This topic contains the following sections:

Understanding Regular Expressions

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

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

Table 9 on page 42 differentiates the local and remote authentication configuration using regular expressions.

Table 24: Sample Local and Remote Authentication Configuration Using Regular Expressions

Local Configuration	Remote Configuration

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

NOTE:

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

Specifying Regular Expressions

WARNING: When you specify regular expression for commands and configuration statements, pay close attention to the following examples, as regular expression with invalid syntax might not produce the desired results, even if the configuration is committed without any error.

Regular expressions for commands and configuration statements should be specified in the same manner as executing the complete command or statement. Table 10 on page 43 lists the regular expressions for configuring access privileges for the **[edit interfaces]** and **[edit vlans]** statement hierarchies, and for the **delete interfaces** command.

Table 25: Specifying Regular Expressions

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

Table 25: Specifying Regular Expressions *(continued)*

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

Regular Expressions Operators

Table 11 on page 45 lists common regular expression operators that you can use for allowing or denying operational and configuration modes.

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

Table 26: Common Regular Expression Operators

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

Table 26: Common Regular Expression Operators *(continued)*

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

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

Regular Expression Examples

Table 12 on page 47 lists the regular expressions used to allow configuration options under two configuration hierarchies—**[edit system ntp server]** and **[edit protocols rip]**—as an example for specifying regular expressions.

NOTE: Table 12 on page 47 does not provide a comprehensive list of all regular expressions and keywords for all configuration statements and hierarchies. The regular expressions listed in the table are supported in Junos OS Release 16.1, and are validated only for the **[edit system ntp server]** and **[edit protocols rip]** statement hierarchies.

Table 27: Regular Expressions Examples

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

Table 27: Regular Expressions Examples *(continued)*

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

Related Documentation

- *Example: Configuring User Permissions with Access Privileges for Operational Mode Commands, Configuration Statements, and Hierarchies*
- *Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies*
- Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 63
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies on page 41

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 38 shows the default requirements.

Table 28: 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
You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.	You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
Valid passwords must contain at least one change of case or character class.	Passwords must use at least three of the five defined character classes (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters).

You can change the requirements for plain-text passwords.

Junos OS supports the following five character classes for plain-text passwords:

- Lowercase letters
- Uppercase letters
- Numbers
- Punctuation
- Special characters: ! @ # $ % ^ & * , +< >

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**, **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. Instead, you can use the sha256 or sha512 to specify passwords. Using a 256-bit or 512-bit cryptographic hash algorithm results in 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;
}
```

Release History Table

Release	Description
13.3	Starting with Junos OS Release 13.3, the **sha1** does not enable secure, protected specification of passwords. Instead, you can use the **sha256** or **sha512** to specify passwords.

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 59
- Configuring a Local Administrator Account on page 106
- Junos OS User Accounts Overview on page 35
- *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 37
- *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 37
- *Defining Junos OS Login Classes*
- Configuring a Local Administrator Account on page 106

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 114.

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 155.

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*

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

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

Requirements

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

Overview

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

Configuration

CLI Quick Configuration

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

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

Configuring Requirements for Plain-Text Passwords

Step-by-Step Procedure

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

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

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

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

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

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

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

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

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

Results

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

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

Related Documentation

- Special Requirements for Junos OS Plain-Text Passwords on page 38
- *password (Login)*

CHAPTER 6

Configuring and Managing TACACS+ Authentication

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 29 on page 115 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 29: Order of Authentication Attempts

Syntax	Order of Authentication Attempts
authentication-order radius;	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS server is available but authentication is rejected, deny access. 4. If RADIUS servers are not available, try password authentication. NOTE: If a RADIUS server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [radius password];	1. Try configured RADIUS authentication servers. 2. If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.
authentication-order [radius tacplus];	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 5. If TACACS+ server is available but authentication is rejected, deny access. 6. If both RADIUS and TACACS+ servers are not available, try password authentication. NOTE: If either RADIUS or TACACS+ servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [radius tacplus password];	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 5. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.

Table 29: Order of Authentication Attempts *(continued)*

Syntax	Order of Authentication Attempts
authentication-order tacplus;	1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ server is available but authentication is rejected, deny access. 4. If TACACS+ servers are not available, try password authentication. NOTE: If a TACACS+ server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [tacplus password];	1. Try configured TACACS+ authentication servers. 2. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.
authentication-order [tacplus radius];	1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 5. If RADIUS server is available but authentication is rejected, deny access. 6. If both TACACS+ and RADIUS servers are not available, try password authentication. NOTE: If either TACACS+ or RADIUS servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [tacplus radius password];	1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 5. If RADIUS servers fail to respond or return a reject response try password authentication, because it is explicitly configured in the authentication order.

Table 29: Order of Authentication Attempts *(continued)*

Syntax	Order of Authentication Attempts
authentication-order password;	1. Try to authenticate the user, using the password configured at the **[edit system login]** hierarchy level. 2. If the authentication is accepted, grant access. 3. If the authentication is rejected, deny access.

NOTE: If SSH public keys are configured, SSH user authentication first tries to perform public key authentication before using the authentication methods configured in the **authentication-order** statement. If you want SSH logins to use the authentication methods configured in the authentication-order statement without first trying to perform public key authentication, do not configure SSH public keys.

In a routing matrix based on a TX Matrix router, the authentication order must be configured only at the configuration groups **re0** and **re1**. The authentication order must not be configured at the **[edit system]** hierarchy. This is because the authentication order for the routing matrix is controlled on the switch-card chassis (or TX Matrix router) or switch-fabric chassis (for TX Matrix Plus router) only.

In Junos OS Release 10.0 and later, the superuser (belonging to the super-user login class) is also authenticated based on the authentication order that is configured for TACACS+, RADIUS, or password authentication using the **authentication-order** statement. For example, if the only configured authentication order is TACACS+, the superuser can only be authenticated by the TACACS+ server and password authentication cannot be used as an alternative. However, in Junos OS Release 9.6 and earlier, the superuser can use password authentication to login, even if password authentication is not configured explicitly using the **authentication-order** statement.

Related Documentation

- Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 155
- *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 108

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 30 on page 118 lists the Juniper Networks VSAs you can configure.

Table 30: Juniper Networks Vendor-Specific TACACS+ Attributes

Name	Description	Length	String
local-user-name	Indicates the name of the user template used by this user when logging in to a device.	≥3	One or more octets containing printable ASCII characters.
allow-commands	Contains an extended regular expression that enables the user to run operational mode commands in addition to those commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 41.
allow-configuration	Contains an extended regular expression that enables the user to run configuration mode commands in addition to those commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 41.
deny-commands	Contains an extended regular expression that denies the user permission to run operational mode commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 41.
deny-configuration	Contains an extended regular expression that denies the user permission to run configuration mode commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 11 on page 45.

Table 30: Juniper Networks Vendor-Specific TACACS+ Attributes *(continued)*

Name	Description	Length	String
user-permissions	Contains information the server uses to specify user permissions. NOTE: When the **user-permissions** attribute is configured to grant the Junos OS **maintenance** or **all** permissions on an IPv4 or IPv6 TACACS+ server, the UNIX wheel group membership is not automatically added to a user's list of group memberships. Some operations such as running the **su root** command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions **maintenance** or **all**, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account.	≥3	One or more octets containing printable ASCII characters. See Table 4 on page 10.
authentication-type	Indicates the authentication method (local database, or TACACS+ server) used to authenticate a user. If the user is authenticated using a local database, the attribute value shows 'local'. If the user is authenticated using TACACS+ server, the attribute value shows 'remote'.	≥5	One or more octets containing printable ASCII characters.
session-port	Indicates the source port number of the established session.	size of integer	Integer

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 114.

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 155.

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 7

Configuring and Managing RADIUS Authentication

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 29 on page 115 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 31: Order of Authentication Attempts

Syntax	Order of Authentication Attempts
authentication-order radius;	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS server is available but authentication is rejected, deny access. 4. If RADIUS servers are not available, try password authentication. NOTE: If a RADIUS server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [radius password];	1. Try configured RADIUS authentication servers. 2. If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.
authentication-order [radius tacplus];	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 5. If TACACS+ server is available but authentication is rejected, deny access. 6. If both RADIUS and TACACS+ servers are not available, try password authentication. NOTE: If either RADIUS or TACACS+ servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [radius tacplus password];	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 5. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.

Table 31: Order of Authentication Attempts *(continued)*

Syntax	Order of Authentication Attempts
authentication-order tacplus;	1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ server is available but authentication is rejected, deny access. 4. If TACACS+ servers are not available, try password authentication. NOTE: If a TACACS+ server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [tacplus password];	1. Try configured TACACS+ authentication servers. 2. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.
authentication-order [tacplus radius];	1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 5. If RADIUS server is available but authentication is rejected, deny access. 6. If both TACACS+ and RADIUS servers are not available, try password authentication. NOTE: If either TACACS+ or RADIUS servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [tacplus radius password];	1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 5. If RADIUS servers fail to respond or return a reject response try password authentication, because it is explicitly configured in the authentication order.

Table 31: Order of Authentication Attempts *(continued)*

Syntax	Order of Authentication Attempts
authentication-order password;	1. Try to authenticate the user, using the password configured at the **[edit system login]** hierarchy level. 2. If the authentication is accepted, grant access. 3. If the authentication is rejected, deny access.

NOTE: If SSH public keys are configured, SSH user authentication first tries to perform public key authentication before using the authentication methods configured in the **authentication-order** statement. If you want SSH logins to use the authentication methods configured in the authentication-order statement without first trying to perform public key authentication, do not configure SSH public keys.

In a routing matrix based on a TX Matrix router, the authentication order must be configured only at the configuration groups **re0** and **re1**. The authentication order must not be configured at the **[edit system]** hierarchy. This is because the authentication order for the routing matrix is controlled on the switch-card chassis (or TX Matrix router) or switch-fabric chassis (for TX Matrix Plus router) only.

In Junos OS Release 10.0 and later, the superuser (belonging to the super-user login class) is also authenticated based on the authentication order that is configured for TACACS+, RADIUS, or password authentication using the **authentication-order** statement. For example, if the only configured authentication order is TACACS+, the superuser can only be authenticated by the TACACS+ server and password authentication cannot be used as an alternative. However, in Junos OS Release 9.6 and earlier, the superuser can use password authentication to login, even if password authentication is not configured explicitly using the **authentication-order** statement.

Related Documentation

- Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 155
- *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 108

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

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 155.

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 132
- Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 108
- Juniper Networks Vendor-Specific RADIUS Attributes on page 142
- Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 155
- Example: Configuring RADIUS Template Accounts on page 133
- Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 130
- 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 | cmd*n*)**. 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 142 and "Juniper Networks Vendor-Specific TACACS+ Attributes" on page 117.

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 113

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 155

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 37
- *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 114.

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 155.

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

Devices support IETF RFC 2866, *RADIUS Accounting*. Configuring RADIUS accounting on the device supports collecting statistical data about users logging in to or out from a LAN and sending the data to a RADIUS accounting server. The statistical data gathered can be used for general network monitoring, analyzing and tracking usage patterns, or billing a user based upon the amount of time or type of services accessed.

To configure RADIUS accounting, specify one or more RADIUS accounting servers to receive the statistical data from the device, and select the type of accounting data to be collected.

The RADIUS accounting server you specify can be the same server used for RADIUS authentication, or it can be a separate RADIUS server. You can specify a list of RADIUS accounting servers. If the primary server (the first one configured) is unavailable, each RADIUS server in the list is tried in the order in which they are configured in the Junos OS.

The RADIUS accounting process between the device and a RADIUS server works like this:

1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. For example, on FreeRADIUS, the default port is 1813.
2. The device forwards an *accounting-request* packet containing an event record to the accounting server. The event record associated with this supplicant contains an *Acct-Status-Type* attribute whose value indicates the beginning of user service for this supplicant. When the supplicant's session ends, the accounting request contains an *Acct-Status-Type* attribute value indicating the end of user service. The RADIUS accounting server records this as a stop-accounting record containing session information and the length of the session.
3. The RADIUS accounting server logs these events in a file as start-accounting or stop-accounting records. On FreeRADIUS, the filename is the server's address; for example, 192.0.2.0.
4. The accounting server sends an *accounting-response* packet back to the device confirming it has received the accounting request.
5. If the device does not receive a response from the server, it continues to send accounting requests until an accounting response is returned from the accounting server.

The statistics collected through this process can be displayed from the RADIUS server; to see those statistics, the user accesses the log file configured to receive them.

Related Documentation

- Configuring RADIUS System Accounting on page 145

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 29 on page 115 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 32: Order of Authentication Attempts

Syntax	Order of Authentication Attempts
authentication-order radius;	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS server is available but authentication is rejected, deny access. 4. If RADIUS servers are not available, try password authentication. NOTE: If a RADIUS server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [radius password];	1. Try configured RADIUS authentication servers. 2. If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.
authentication-order [radius tacplus];	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 5. If TACACS+ server is available but authentication is rejected, deny access. 6. If both RADIUS and TACACS+ servers are not available, try password authentication. NOTE: If either RADIUS or TACACS+ servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [radius tacplus password];	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 5. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.

Table 32: Order of Authentication Attempts *(continued)*

Syntax	Order of Authentication Attempts
authentication-order tacplus;	1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ server is available but authentication is rejected, deny access. 4. If TACACS+ servers are not available, try password authentication. NOTE: If a TACACS+ server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [tacplus password];	1. Try configured TACACS+ authentication servers. 2. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.
authentication-order [tacplus radius];	1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 5. If RADIUS server is available but authentication is rejected, deny access. 6. If both TACACS+ and RADIUS servers are not available, try password authentication. NOTE: If either TACACS+ or RADIUS servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.
authentication-order [tacplus radius password];	1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 5. If RADIUS servers fail to respond or return a reject response try password authentication, because it is explicitly configured in the authentication order.

Table 32: Order of Authentication Attempts *(continued)*

Syntax	Order of Authentication Attempts
authentication-order password;	1. Try to authenticate the user, using the password configured at the **[edit system login]** hierarchy level. 2. If the authentication is accepted, grant access. 3. If the authentication is rejected, deny access.

NOTE: If SSH public keys are configured, SSH user authentication first tries to perform public key authentication before using the authentication methods configured in the **authentication-order** statement. If you want SSH logins to use the authentication methods configured in the authentication-order statement without first trying to perform public key authentication, do not configure SSH public keys.

In a routing matrix based on a TX Matrix router, the authentication order must be configured only at the configuration groups **re0** and **re1**. The authentication order must not be configured at the **[edit system]** hierarchy. This is because the authentication order for the routing matrix is controlled on the switch-card chassis (or TX Matrix router) or switch-fabric chassis (for TX Matrix Plus router) only.

In Junos OS Release 10.0 and later, the superuser (belonging to the super-user login class) is also authenticated based on the authentication order that is configured for TACACS+, RADIUS, or password authentication using the **authentication-order** statement. For example, if the only configured authentication order is TACACS+, the superuser can only be authenticated by the TACACS+ server and password authentication cannot be used as an alternative. However, in Junos OS Release 9.6 and earlier, the superuser can use password authentication to login, even if password authentication is not configured explicitly using the **authentication-order** statement.

Related Documentation

- Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 155
- *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 108

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 33 on page 143 lists the Juniper Networks VSAs you can configure.

Table 33: 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 "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 41.
Juniper-Deny-Commands	Contains an extended regular expression that denies the user permission to run operation mode commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	3	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 41.
Juniper-Allow-Configuration	Contains an extended regular expression that enables the user to run configuration mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	4	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 41.

Table 33: Juniper Networks Vendor-Specific RADIUS Attributes *(continued)*

Name	Description	Type	Length	String
Juniper-Deny-Configuration	Contains an extended regular expression that denies the user permission to run configuration commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	5	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 41.
Juniper-Interactive-Command	Indicates the interactive command entered by the user. This attribute is used only in Accounting-Request packets.	8	≥3	One or more octets containing printable ASCII characters.
Juniper-Configuration-Change	Indicates the interactive command that results in a configuration (database) change. This attribute is used only in Accounting-Request packets.	9	≥3	One or more octets containing printable ASCII characters.
Juniper-User-Permissions	Contains information the server uses to specify user permissions. This attribute is used only in Access-Accept packets. NOTE: When the **Juniper-User-Permissions** attribute is configured to grant the Junos OS **maintenance** or **all** permissions on a RADIUS server, the UNIX wheel group membership is not automatically added to a user's list of group memberships. Some operations such as running the **su root** command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions **maintenance** or **all**, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account.	10	≥3	One or more octets containing printable ASCII characters. The string is a list of permission flags separated by a space. The exact name of each flag must be specified in its entirety. See Table 4 on page 10.

Table 33: Juniper Networks Vendor-Specific RADIUS Attributes *(continued)*

Name	Description	Type	Length	String
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 145
2. Specifying RADIUS Server Accounting and Auditing Events on page 146
3. Configuring RADIUS Server Accounting on page 146

Configuring Auditing of User Events on a RADIUS Server

To audit user events, include the following statements at the **[edit system accounting]** hierarchy level:

```
[edit system accounting]
events [ events ];
destination {
    radius {
        server {
            server-address {
                accounting-port port-number;
                secret password;
                source-address address;
                retry number;
                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;
    secret password;
    source-address address;
    retry number;
    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.

Starting with Junos OS Release 14.1, you can configure the **enhanced-accounting** statement to view the attribute values of a logged in user. If you use the **enhanced-accounting** statement at the **[edit system radius-options]** hierarchy level, the RADIUS attributes such as access method, remote port, and access privileges can be audited. You can limit the number of attribute values to be displayed for auditing by using the **enhanced-avs-max** *<number>* statement at the **[edit system accounting]** hierarchy level.

```
[edit system radius-options]
enhanced-accounting;

[edit system accounting]
enhanced-avs-max <number>;
```

When a Juniper Networks router or switch is configured with RADIUS accounting, it sends **Accounting-Start** and **Accounting-Stop** messages to the RADIUS server. These messages contain information about user activities such as software logins, configuration changes, and interactive commands. This information is typically used for monitoring a network, collecting usage statistics, and ensuring that users are billed properly.

The following example shows three servers (10.5.5.5, 10.6.6.6, and 10.7.7.7) configured for RADIUS accounting:

```
system {
    accounting {
        events [ login change-log interactive-commands ];
        destination {
            radius {
                server {
                    10.5.5.5 {
                        accounting-port 3333;
                        secret $ABC123;
                        source-address 10.1.1.1;
                        retry 3;
                        timeout 3;
```

```
            }
            10.6.6.6 secret $ABC123;
            10.7.7.7 secret $ABC123;
          }
        }
      }
    }
  }
```

Release History Table

Release	Description
14.1	Starting with Junos OS Release 14.1, you can configure the **enhanced-accounting** statement to view the attribute values of a logged in user.

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 148
- Configuring MS-CHAPv2 for Password-Change Support on page 149
- Specifying a Source Address for the Junos OS to Access External RADIUS Servers on page 150

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 155.

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 132
- Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 108
- Juniper Networks Vendor-Specific RADIUS Attributes on page 142
- Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 155
- Example: Configuring RADIUS Template Accounts on page 133
- Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 130
- 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 | cmd*n*)**. 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 142 and "Juniper Networks Vendor-Specific TACACS+ Attributes" on page 117.

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 113

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 145

CHAPTER 9

Configuring and Managing RADIUS Template Accounts

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 155

CHAPTER 10

Configuring and Managing VSAs for RADIUS and TACACS+

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 127
- Juniper-Switching-Filter VSA Match Conditions and Actions on page 158

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 34 on page 158 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 34: Match Conditions

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

Table 34: Match Conditions *(continued)*

Option	Description
source-port *port*	TCP or User Datagram Protocol (UDP) source port field. Normally, you specify this match statement in conjunction with the **ip-protocol** match statement to determine which protocol is being used on the port. In place of the numeric field, you can specify one of the text options listed under **destination-port**.
destination-port *port*	TCP or UDP destination port field. Normally, you specify this match statement in conjunction with the **ip-protocol** match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify one of the following text synonyms (the port numbers are also listed): **afs (1483)**, **bgp (179)**, **biff (512)**, **bootpc (68)**, **bootps (67)**, **cvspserver (2401)**, **cmd (514)**, **dhcp (67)**, **domain (53)**, **eklogin (2105)**, **ekshell (2106)**, **exec (512)**, **finger (79)**, **ftp (21)**, **ftp-data (20)**, **http (80)**, **https (443)**, **ident (113)**, **imap (143)**, **kerberos-sec (88)**, **klogin (543)**, **kpasswd (761)**, **krb-prop (754)**, **krbupdate (760)**, **kshell (544)**, **ldap (389)**, **login (513)**, **mobileip-agent (434)**, **mobilip-mn (435)**, **msdp (639)**, **netbios-dgm (138)**, **netbios-ns (137)**, **netbios-ssn (139)**, **nfsd (2049)**, **nntp (119)**, **ntalk (518)**, **ntp (123)**, **pop3 (110)**, **pptp (1723)**, **printer (515)**, **radacct (1813)**, **radius (1812)**, **rip (520)**, **rkinit (2108)**, **smtp (25)**, **snmp (161)**, **snmptrap (162)**, **snpp (444)**, **socks (1080)**, **ssh (22)**, **sunrpc (111)**, **syslog (514)**, **telnet (23)**, **tacacs-ds (65)**, **talk (517)**, **tftp (69)**, **timed (525)**, **who (513)**, **xdmcp (177)**, **zephyr-clt (2103)**, **zephyr-hm (2104)**

When you define one or more terms that specify the filtering criteria, you also define the action to take if the packet matches all criteria. Table 35 on page 159 shows the actions that you can specify in a term.

Table 35: Actions for VSAs

Option	Description
(**allow** | **deny**)	Accept a packet or discard a packet silently without sending an Internet Control Message Protocol (ICMP) message.
forwarding-class *class-of-service*	(Optional) Classify the packet in one of the following forwarding classes: • **assured-forwarding** • **best-effort** • **expedited-forwarding** • **network-control**
loss-priority (**low** | **medium** | **high**)	(Optional) Set the packet loss priority (PLP) to **low**, **medium**, or **high**. Specify both the forwarding class and the loss priority.

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 157

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 33 on page 143 lists the Juniper Networks VSAs you can configure.

Table 36: 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 "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 41.
Juniper-Deny-Commands	Contains an extended regular expression that denies the user permission to run operation mode commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	3	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 41.
Juniper-Allow-Configuration	Contains an extended regular expression that enables the user to run configuration mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	4	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 41.

Table 36: Juniper Networks Vendor-Specific RADIUS Attributes *(continued)*

Name	Description	Type	Length	String
Juniper-Deny-Configuration	Contains an extended regular expression that denies the user permission to run configuration commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	5	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 41.
Juniper-Interactive-Command	Indicates the interactive command entered by the user. This attribute is used only in Accounting-Request packets.	8	≥3	One or more octets containing printable ASCII characters.
Juniper-Configuration-Change	Indicates the interactive command that results in a configuration (database) change. This attribute is used only in Accounting-Request packets.	9	≥3	One or more octets containing printable ASCII characters.
Juniper-User-Permissions	Contains information the server uses to specify user permissions. This attribute is used only in Access-Accept packets. NOTE: When the **Juniper-User-Permissions** attribute is configured to grant the Junos OS **maintenance** or **all** permissions on a RADIUS server, the UNIX wheel group membership is not automatically added to a user's list of group memberships. Some operations such as running the **su root** command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions **maintenance** or **all**, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account.	10	≥3	One or more octets containing printable ASCII characters. The string is a list of permission flags separated by a space. The exact name of each flag must be specified in its entirety. See Table 4 on page 10.

Table 36: Juniper Networks Vendor-Specific RADIUS Attributes *(continued)*

Name	Description	Type	Length	String
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*

PART 4

Configuration Statements and Operational Commands

CHAPTER 11

Configuration Statements

- user (Access) on page 247
- version on page 248

access

Syntax

```
access {
  address-assignment
  pool pool-name
  address-poolpool-name
  profile profile-name {
    accounting (Access Profile) {
      accounting-stop-on-access-deny;
      accounting-stop-on-failure;
      (authentication-order (Access Profile) (ldap radius | none);
      order (radius | none);
    }
    radius {
      accounting-server [server-addresses];
      authentication-server [server-addresses];
    }
  }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure authentication, authorization, and accounting (AAA) services.

The statements are explained separately.

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

Default Not enabled

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

Related Documentation

- *Configuring 802.1X RADIUS Accounting (CLI Procedure)*

accounting (Access Profile)

Syntax

```
accounting {
  accounting-stop-on-access-deny;
  accounting-stop-on-failure;
  order (radius | none);
}
```

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure the authentication order for authentication, authorization, and accounting (AAA) services.

Default Not enabled

Options **none**—Use no authentication for specified subscribers.

radius—Use RADIUS authentication for specified subscribers.

The remaining statements are explained separately.

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

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

Related Documentation

- *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*
- *Configuring 802.1X RADIUS Accounting (CLI Procedure)*
- *Understanding 802.1X and RADIUS Accounting on Switches*
- Understanding RADIUS Accounting on page 137

accounting-options

Syntax

```
accounting-options {
  class-usage-profile profile-name {
    destination-classes {
      destination-class-name;
    }
    file filename;
    interval minutes;
    source-classes {
      source-class-name;
    }
  }
  file filename {
    archive-sites {
      site-name;
    }
    files number;
    nonpersistent;
    size bytes;
    start-time time;
    transfer-interval minutes;
  }
  filter-profile profile-name {
    counters {
      counter-name;
    }
    file filename;
    interval minutes;
  }
  interface-profile profile-name {
    fields {
      input-bytes;
      input-errors;
      input-multicast;
      input-packets;
      input-unicast;
      output-bytes;
      output-errors;
      output-multicast;
      output-packets;
      output-unicast;
      rpf-check-bytes;
      rpf-check-packets;
      rpf-check6-bytes;
      rpf-check6-packets;
      unsupported-protocol;
    }
    file filename;
    interval minutes;
  }
  mib-profile profile-name {
    file filename;
    interval minutes;
```

```
    object-names {
      mib-object-name;
    }
    operation (get | get-next | walk);
  }
  policy-decision-statistics-profile profile-name {
    application-aware-access-list-fields {
      address;
      application;
      application-group;
      input-bytes;
      input-interface;
      input-packets;
      mask;
      output-bytes;
      output-packets;
      subscriber-name;
      timestamp;
      vrf-name;
    }
    file filename;
  }
  routing-engine-profile profile-name {
    fields {
      field-name;
    }
    file filename;
    interval minutes;
  }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure options for accounting statistics collection.

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

Related Documentation

- Understanding RADIUS Accounting on page 137
- Understanding Vendor-Specific Attributes (VSAs) on page 157
- Configuring RADIUS System Accounting on page 145
- *Configuring Remote Template Accounts for User Authentication*
- *Configuring Local User Template Accounts for User Authentication*

accounting-server

Syntax accounting-server[*server-addresses*];

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure the Remote Authentication Dial-In User Service (RADIUS) server for authentication. To configure multiple RADIUS servers, include multiple server addresses. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

Default Not enabled

Options ***server-addresses***—One or more addresses of RADIUS authentication servers.

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

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

Related Documentation

- *show network-access aaa statistics authentication*
- *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*
- *Understanding 802.1X and RADIUS Accounting on Switches*
- Understanding RADIUS Accounting on page 137

accounting-stop-on-access-deny

Syntax accounting-stop-on-access-deny;

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure the authentication order for authentication, authorization, and accounting (AAA) services to send an Acct-Stop message if the AAA server denies access to a supplicant.

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

Default Not enabled

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

Related Documentation

- *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*
- *Configuring 802.1X RADIUS Accounting (CLI Procedure)*
- *show network-access aaa statistics authentication*

accounting-stop-on-failure

Syntax accounting-stop-on-failure;

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure RADIUS accounting to send an Acct-Stop message when a subscriber session has been successfully authenticated and authorized, but then fails before an Acct-Start message is sent. By default, an Acct-Stop message is sent only if an Acct-Start message has been exchanged with the accounting server.

Consider a situation where RADIUS address pools are used to assign IP/IPv6 addresses. After a subscriber session is successfully authenticated, the RADIUS server authorizes the session by assigning an IP address from the RADIUS address pool and conveying that address in the Framed-IP-Address attribute. If a negotiation failure occurs at this point, the session is terminated before activating. The Acct-Start message is never sent because it is initiated by session activation. By default, an Acct-Stop message cannot be sent because the Acct-Start is never sent. However, if the **acct-stop-on-failure** statement is configured, the negotiation failure causes the Acct-Stop message to be sent, which explicitly notifies the RADIUS server that the session is disconnected and that it can free the allocated IP address back to the pool.

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

Default Disabled

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

Related Documentation

- *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*
- *Configuring 802.1X RADIUS Accounting (CLI Procedure)*
- *Understanding 802.1X and RADIUS Accounting on Switches*
- Understanding RADIUS Accounting on page 137

advertisement-interval

Syntax advertisement-interval *seconds*;

Hierarchy Level [edit protocols lldp],
[edit routing-instances *routing-instance-name* protocols lldp]

Release Information Statement introduced in Junos OS Release 9.6 for MX Series and T Series routers.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure an interval for LLDP advertisement.

For switches configured for Link Layer Discovery Protocol, configure the frequency at which LLDP advertisements are sent.

The **advertisement-interval** value must be greater than or equal to four times the **transmit-delay** value, or an error will be returned when you attempt to commit the configuration.

NOTE: The default value of **transmit-delay** is 2 seconds. If you configure the **advertisement-interval** as less than 8 seconds and you do not configure a value for **transmit-delay**, the default value of **transmit-delay** is automatically changed to 1 second in order to satisfy the requirement that the **advertisement-interval** value must be greater than or equal to four times the **transmit-delay** value.

Default Disabled.

Options ***seconds***—Interval between LLDP advertisement.
Default: 30
Range: 5 through 32768

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

Related Documentation

- *Configuring LLDP*
- show lldp on page 258
- *Configuring LLDP (CLI Procedure)*
- *Understanding LLDP and LLDP-MED on EX Series Switches*
- *transmit-delay*
- Understanding LLDP on page 5

agent-address

Syntax agent-address outgoing-interface;

Hierarchy Level [edit snmp trap-options]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Set the agent address of all SNMPv1 traps generated by this router or switch. Currently, the only option is **outgoing-interface**, which sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

Options

outgoing-interface—Value of the agent address of all SNMPv1 traps generated by this router or switch. The **outgoing-interface** option sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

Default: Disabled (the agent address is not specified in SNMPv1 traps).

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

Related Documentation

- *Configuring the Agent Address for SNMP Traps*

archival

Syntax

```
archival {
  configuration {
    archive-sites {
      file://<path>/<filename>;
      ftp://username@host:<port>url-path password password;
      http://username@host:<port>url-path password password;
      pasvftp://username@host:<port>url-path password password;
      scp://username@host:<port>url-path password password;
    }
    transfer-interval interval;
    transfer-on-commit;
  }
}
```

Hierarchy Level [edit system]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure copying of the currently active configuration to an archive site. An archive site can be a file, or an FTP, HTTP, or SCP location.

Options The remaining statements are explained separately.

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

Required Privilege Level

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

Related Documentation

- *Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site*

archive-sites (Configuration File)

Syntax

```
archive-sites {
  file://<path>/<filename>;
  ftp://username@host:<port>url-path password password;
  http://username@host:<port>url-path password password;
  pasvftp://username@host:<port>url-path password password;
  scp://username@host:<port>url-path password password;
}
```

Hierarchy Level [edit system archival configuration]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Specify where to transfer the current configuration files. When specifying a URL in a Junos OS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([ ]). For example, **"scp://*username*<:*password*>@[*ipv6-host-address*]<:*port*>/*url-path*"**

If you specify more than one archive site, the router or switch attempts to transfer the configuration files to the first archive site in the list, moving to the next only if the transfer fails.

The destination filename is saved in the following format, where *n* corresponds to the number of the compressed configuration rollback file that has been archived:

***router-name_YYYYMMDD_HHMMSS*_juniper.conf.*n*.gz**

NOTE: The time included in the destination filename is always in Coordinated Universal Time (UTC) regardless of whether the time on the router or switch is configured as UTC or the local time zone. The default time zone on the router or switch is UTC.

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

Options The prefix used in the configuration statement determines the form of transfer:

file:// —transfer on a path to a named file

ftp:// —transfer using active FTP server

http://—transfer using HTTP server

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 185
- transfer-on-commit on page 244

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

Syntax authentication-server [*server-addresses*];

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

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

Options ***server-addresses***—Configure one or more RADIUS server addresses.

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

Related Documentation

- *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*
- *show network-access aaa statistics authentication*

authorization

Syntax authorization *authorization*;

Hierarchy Level [edit snmp community *community-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Set the access authorization for SNMP **Get**, **GetBulk**, **GetNext**, and **Set** requests.

Options ***authorization***—Access authorization level:

- **read-only**—Enable **Get**, **GetNext**, and **GetBulk** requests.
- **read-write**—Enable all requests, including **Set** requests. You must configure a view to enable **Set** requests.

NOTE: **The read-write option is not supported on the QFX3000 QFabric system.**

Default: read-only

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

Related Documentation

- *Configuring the SNMP Community String*

categories

Syntax

```
categories {
  category;
}
```

Hierarchy Level [edit snmp trap-group *group-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Define the types of traps that are sent to the targets of the named trap group.

Default If you omit the **categories** statement, all trap types are included in trap notifications.

Options ***category***—Name of a trap type: **authentication**, **chassis**, **configuration**, **link**, **remote-operations**, **rmon-alarm**, or **startup**.

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

Related Documentation

- *Configuring SNMP Trap Groups*

client-list

Syntax

```
client-list client-list-name {
  ip-addresses;
}
```

Hierarchy Level [edit snmp]

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 Define a list of SNMP clients.

Options ***client-list-name***—Name of the client list.

ip-addresses—IP addresses of the SNMP clients to be added to the client list,

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

Related Documentation

- *Adding a Group of Clients to an SNMP Community*

client-list-name

Syntax client-list-name *client-list-name*;

Hierarchy Level [edit snmp community *community-name*]

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 Add a client list or prefix list to an SNMP community.

Options ***client-list-name***—Name of the client list or prefix list.

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

Related Documentation
- *Adding a Group of Clients to an SNMP Community*

clients

Syntax
```
clients {
  address <restrict>;
}
```

Hierarchy Level [edit snmp community *community-name*]

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 Specify the IPv4 or IPv6 addresses of the SNMP client hosts that are authorized to use this community.

Default If you omit the **clients** statement, all SNMP clients using this community string are authorized to access the switch.

Options ***address***—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 ***address*** options.

restrict—(Optional) Do not allow the specified SNMP client to access the switch.

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

Related Documentation
- *Configuring SNMP Communities*

commit-delay

Syntax commit-delay *seconds*;

Hierarchy Level [edit snmp nonvolatile]

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 timer for the SNMP **Set** reply and start of the commit.

Options ***seconds***—Delay between an affirmative SNMP **Set** reply and start of the commit operation.

Default: 5 seconds

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

Related Documentation

- *Configuring the Commit Delay Timer*

community (SNMP)

Syntax

```
community community-name {
  authorization authorization;
  client-list-name client-list-name;
  clients {
    address restrict;
  }
  view view-name;
}
```

Hierarchy Level [edit snmp]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Define an SNMP community. An SNMP community authorizes SNMP clients based on the source IP address of incoming SNMP request packets. A community also defines which MIB objects are available and the operations (read-only or read-write) allowed on those objects.

NOTE: The **authorization read-write** option is not supported on the QFX3000 QFabric system.

The SNMP client application specifies an SNMP community name in **Get**, **GetBulk**, **GetNext**, and **Set** SNMP requests.

Default If you omit the **community** statement, all SNMP requests are denied.

Options ***community-name***—Community string. If the name includes spaces, enclose it in quotation marks (" ").

The remaining statements are explained separately.

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

Related Documentation

- *Configuring the SNMP Community String*

configuration

Syntax

```
configuration {
  transfer-interval interval;
  transfer-on-commit;
  archive-sites {
    file://<path>/<filename>;
    ftp://username@host:<port>url-path password password;
    http://username@host:<port>url-path password password;
    pasvftp://username@host:<port>url-path password password;
    scp://username@host:<port>url-path password password;
  }
}
```

Hierarchy Level [edit system archival]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure the router or switch to periodically transfer its currently active configuration (or after each commit).

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

Options The remaining statements are explained separately.

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

Related Documentation

- *Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site*
- *archive*
- archive-sites on page 177
- transfer-interval on page 243
- transfer-on-commit on page 244

connection-limit

Syntax connection-limit *limit*;

Hierarchy Level [edit system services finger],
[edit system services ftp],
[edit system services netconf ssh],
[edit system services ssh],
[edit system services telnet],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure the maximum number of connections sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).

Options ***limit***—(Optional) Maximum number of established connections per protocol (either IPv6 or IPv4).

Range: 1 through 250

Default: 75

NOTE: The actual number of maximum connections depends on the availability of system resources, and might be fewer than the configured **connection-limit** value if the system resources are limited.

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

Related Documentation

- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*
- *Configuring DTCP-over-SSH Service for the Flow-Tap Application*
- *Configuring Finger Service for Remote Access to the Router*
- *Configuring FTP Service for Remote Access to the Router or Switch*
- *Configuring SSH Service for Remote Access to the Router or Switch*
- *Configuring Telnet Service for Remote Access to a Router or Switch*

contact

Syntax contact *contact*;

Hierarchy Level [edit snmp]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Define the value of the MIB II **sysContact** object, which is the contact person for the managed system.

Options ***contact***—Name of the contact person. If the name includes spaces, enclose it in quotation marks (" ").

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

Related Documentation
- *Configuring the System Contact on a Device Running Junos OS*

disable (LLDP)

Syntax disable;

Hierarchy Level [edit protocols lldp],
[edit protocols interface lldp]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Disable the LLDP configuration on the switch or on one or more interfaces.

Default If you do not configure LLDP, it is disabled on the switch and on specific switch interfaces.

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

Related Documentation
- show lldp on page 258
- *Configuring LLDP (CLI Procedure)*
- *Understanding LLDP and LLDP-MED on EX Series Switches*
- *Configuring LLDP*
- Understanding LLDP on page 5

falling-threshold (Health Monitor)

Syntax falling-threshold *percentage*;

Hierarchy Level [edit snmp health-monitor]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Set the lower threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options ***percentage***—Lower threshold for the alarm entry.
Range: 1 through 100
Default: 70 percent of the maximum possible value

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

Related Documentation
- rising-threshold on page 225
- *Configuring Health Monitoring*

filter-duplicates

Syntax filter-duplicates;

Hierarchy Level [edit snmp]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Filter duplicate **Get**, **GetNext**, or **GetBulk** SNMP requests.

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

Related Documentation
- *Understanding the Implementation of SNMP on the QFabric System*
- *Example: Configuring SNMP*

full-name

Syntax full-name *complete-name*;

Hierarchy Level [edit system login user]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure the complete name of a user.

Options ***complete-name***—Full name of the user. If the name contains spaces, enclose it in quotation marks.

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

Related Documentation
- *Configuring Junos OS User Accounts by Using a Configuration Group*
- *user*

health-monitor

Syntax
```
health-monitor {
  falling-threshold percentage;
  interval seconds;
  rising-threshold percentage;
}
```

Hierarchy Level [edit snmp]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure health monitoring.

The remaining statements are explained separately.

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

Related Documentation
- *Configuring Health Monitoring*
- *Understanding Health Monitoring*

hold-multiplier

Syntax hold-multiplier *number*;

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for QFX Series.

Description Specify the multiplier used in combination with the advertisement-interval value to determine the length of time LLDP information is held before it is discarded. The default value is 4 (or 120 seconds).

Default Disabled.

Options ***number***—A number used as a multiplier.
Range: 2 through 10
Default: 4 (or 120 seconds)

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

Related Documentation

- show lldp on page 258
- *Configuring LLDP (CLI Procedure)*
- *Understanding LLDP and LLDP-MED on EX Series Switches*
- *Configuring LLDP*
- Understanding LLDP on page 5

idle-timeout (Access)

Syntax idle-timeout *seconds*;

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

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

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

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

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

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

Default: 0

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

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

Related Documentation

- *Configuring the Group Profile for Defining L2TP Attributes*
- *Configuring PPP Properties for a Client-Specific Profile*
- *Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile*

interface (LLDP)

Syntax

```
interface (all | interface-name) {
  disable;
  power-negotiation {
    disable;
  }
}
```

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure Link Layer Discovery Protocol (LLDP) on all interfaces or on a specific interface.

NOTE: On EX4300 switches, LLDP cannot be configured on the me0 or vme interface. Issuing the command **set protocols lldp interface me0** generates the following error message:

```
error: name: 'me0': Invalid interface
error: statement creation failed: interface
```

Issuing the command **set protocols lldp interface vme** generates the following error message:

```
error: name: 'vme': Invalid interface
error: statement creation failed: interface
```

Default None

Options **all**—All interfaces on the switch.

interface-name—Name of a specific interface.

The remaining statements are explained separately.

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

Related Documentation

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

interval (Health Monitor)

Syntax interval *seconds*;

Hierarchy Level [edit snmp health-monitor]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the interval between sampling of the object being monitored by the health monitor.

Options ***seconds***—Time between samples, in seconds.

Range: 1 through 2147483647 seconds

Default: 300 seconds

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

Related Documentation

- *Configuring Health Monitoring*

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 258
- *Configuring LLDP (CLI Procedure)*
- *Configuring LLDP*
- Understanding LLDP on page 5
- *Understanding LLDP and LLDP-MED on EX Series Switches*

lldp-configuration-notification-interval

Syntax lldp-configuration-notification-interval *seconds*;

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 9.6 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify how often SNMP trap notifications are generated as a result of LLDP database changes. If the interval value is 0, trap notifications of database changes are disabled.

Default SNMP trap notifications of LLDP database changes are disabled.

Options ***seconds***—Interval between trap notifications about LLDP database changes.
Range: 0 through 3600

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 258

location

Syntax location *location*;

Hierarchy Level [edit snmp]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Define the value of the MIB II **sysLocation** object, which is the physical location of the managed system.

Options ***location***—Location of the local system. You must enclose the name within quotation marks (" ").

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

Related Documentation
- *Configuring the System Location for a Device Running Junos OS*

management-address

Syntax management-address *ip-management-address*;

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 9.5 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify the management address to be used in LLDP Management Address type, length, and value (TLV) messages. The Management Address TLV typically contains the IPv4 or IPv6 management addresses of the local system. Only out-of-band management addresses must be used for the management-address. Other remote managers can use this address to obtain information related to the local device.

Default The LLDP Management Address TLV uses the IP address of the switch's management Ethernet interface (**me0**), or the IP address of the virtual management Ethernet (VME) interface if the switch is a Virtual Chassis member.

Options ***ip-management-address***—You can specify either an IPv4 or an IPv6 management address for the switch.

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

Related Documentation

- show lldp on page 258
- *Understanding LLDP and LLDP-MED on EX Series Switches*
- *EX Series Switches Interfaces Overview*
- Understanding LLDP on page 5

name

Syntax name *name*;

Hierarchy Level [edit snmp]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Set the system name from the command-line interface.

Options ***name***—System name override.

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

Related Documentation
- *Configuring a Different System Name*

nas-ip-address

Syntax nas-ip-address *ip-address*;

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the NAS-IP address for outgoing RADIUS packets.

Options **ip-address**—IP address of the network access server (NAS) that requests user authentication.

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

Related Documentation
- *Configuring RADIUS Server Authentication*
- Configuring RADIUS Authentication (QFX Series or OCX Series) on page 127

nonvolatile

Syntax

```
nonvolatile {
  commit-delay seconds;
}
```

Hierarchy Level [edit snmp]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure options for SNMP **Set** requests.

The statement is explained separately.

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

Related Documentation

- *Configuring the Commit Delay Timer*
- *commit-delay*

oid

Syntax oid *object-identifier* (exclude| include);

Hierarchy Level [edit snmp view *view-name*]

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 Specify an object identifier (OID) used to represent a subtree of MIB objects.

Options **exclude**—Exclude the subtree of MIB objects represented by the specified OID.

include—Include the subtree of MIB objects represented by the specified OID.

object-identifier—OID used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name.

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

Related Documentation

- *Configuring MIB Views*

order

Syntax order (radius | [*accounting-order-data-list*]);

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the order of authentication, authorization, and accounting (AAA) servers to use while sending accounting messages and updates.

Default No order specified

Options **radius**—RADIUS accounting for specified subscribers.

[*accounting-order-data-list*]— Set of data listing the authentication order to be used, enclosed by brackets. This can be any combination of the authentication methods, up to and including a full list of the entire authentication order.

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

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

Related Documentation

- *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*
- *Configuring 802.1X RADIUS Accounting (CLI Procedure)*

port (RADIUS Server)

Syntax port *port-number*;

Hierarchy Level [edit system radius-server *address*],
[edit system accounting destination radius server *address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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

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

Default: 1812 (as specified in RFC 2865)

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

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

Related Documentation

- *Configuring RADIUS Server Authentication*

profile

Syntax

```
profile profile-name {
  accounting (Access Profile) {
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    order (radius | [ accounting-order-data-list ];
  }
  authentication-order (Access Profile) [authentication-method];
  radius {
    accounting-server [server-addresses];
    authentication-server [server-addresses];
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure an access profile. The access profile contains the entire authentication, authorization, and accounting (AAA) configuration that aids in handling AAA requests, including the authentication method and order, AAA server addresses, and AAA accounting.

Default Not enabled.

Options ***profile-name***—Profile name of up to 32 characters.

The remaining statements are explained separately.

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

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

Related Documentation

- *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*
- *Configuring 802.1X RADIUS Accounting (CLI Procedure)*

protocol-version

Syntax protocol-version [v1 v2];

Hierarchy Level [edit system services ssh]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Specify the Secure Shell (SSH) protocol version.

Default **v2**—SSH protocol version 2 is the default, introduced in Junos OS Release 11.4.

Options SSH protocol version **v1**, **v2**, or both.

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

Related Documentation

- *Configuring SSH Service for Remote Access to the Router or Switch*

protocols

Syntax

```
protocols {
  bgp {
    disable;
    accept-remote-nexthop;
    advertise-external <conditional>;
    advertise-inactive;
    (advertise-peer-as | no-advertise-peer-as);
    authentication-algorithm (aes-128-cmac-96 | hmac-sha-1-96 | md5);
    authentication-key key;
    authentication-key-chain key-chain;
    bfd-liveness-detection {
      authentication {
        algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
          meticulous-keyed-sha-1 | simple-password);
        key-chain key-chain-name;
        loose-check;
      }
      detection-time {
        threshold milliseconds;
      }
      hold-down-interval milliseconds;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      session-mode (automatic | multihop | single-hop);
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (1 | automatic);
    }
    cluster cluster-identifier;
    damping;
    description text-description;
    export [ policy-names ];
    family family-name {
      ... the family subhierarchies appear after the main [edit protocols bgp] hierarchy ...
    }
    graceful-restart {
      disable;
      restart-time seconds;
      stale-routes-time seconds;
    }
    group group-name {
      ... the group subhierarchy appears after the main [edit protocols bgp] hierarchy ...
    }
    hold-time seconds;
    import [ policy-names ];
    include-mp-next-hop;
    keep (all | none);
    local-address address;
```

```
    local-as autonomous-system <loops number> < alias> <private>;
    local-preference local-preference;
    log-updown;
    metric-out (metric | igp (delay-med-update | offset) | minimum-igp offset);
    mtu-discovery;
    multihop {
      no-nexthop-change;
      ttl ttl-value;
    }
    no-aggregator-id;
    no-client-reflect;
    out-delay seconds;
    outbound-route-filter {
      bgp-orf-cisco-mode;
      prefix-based {
        accept {
          inet;
          inet6;
        }
      }
    }
    passive;
    path-selection {
      always-compare-med;
      as-path-ignore;
      cisco-non-deterministic;
      external-router-id;
      med-plus-igp {
        igp-multiplier number;
        med-multiplier number;
      }
    }
    peer-as autonomous-system;
    preference preference;
    remove-private;
    tcp-mss segment-size;
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
  }
  dcbx {
    disable;
    interface (interface-name | all) {
      disable;
      application-map application-map-name;
      applications {
        no-auto-negotiation;
      }
      enhanced-transmission-selection {
        no-auto-negotiation;
        no-recommendation-tlv;
        recommendation-tlv {
          no-auto-negotiation;
        }
```

```
      }
      dcbx-version (auto-negotiate | ieee-dcbx | dcbx-version-1.01);
      priority-flow-control {
        no-auto-negotiation;
      }
    }
  }
  iccp {
    authentication-key string;
    local-ip-addr local-ip-addr;
    peer ip-address{
      authentication-key string;
      backup-liveness-detection {
        backup-peer-ip ip-address;
      }
      liveness-detection {
        detection-time {
          threshold milliseconds;
        }
        minimum-intervalmilliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        version (Liveness Detection) (1 | automatic);
      }
      local-ip-addr ipv4-address;
      session-establishment-hold-time seconds;
    }
    session-establishment-hold-time seconds;
    traceoptions {
      file <filename> <files number> <match regular-expression> <microsecond-stamp>
        <size size> <world-readable | no-world-readable>;
      flag flag;
      no-remote-trace;
    }
  }
  igmp-snooping {
    traceoptions {
      file filename <files number> <size size> <world-readable | no-world-readable> <match
        regex>;
      flag flag (detail | disable | receive | send);
    }
    vlan vlan-name {
      disable;
      }
      interface interface-name {
        group-limit limit;
        multicast-router-interface;
        static {
          group ip-address;
        }
      }
```

```
        robust-count number;
    }
}
isis {
    disable;
    export [ policy-names ];
    ignore-attached-bit;
    interface interface-name {
        bfd-liveness-detection {
            authentication {
                algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
                    meticulous-keyed-sha-1 | simple-password);
                key-chain key-chain-name;
                loose-check;
            }
            detection-time {
                threshold milliseconds;
            }
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (1 | automatic);
        }
        checksum;
        csnp-interval (seconds | disable);
        disable;
        hello-padding (adaptive | loose | strict);
        level (1 | 2) {
            disable;
            hello-authentication-key key;
            hello-authentication-type authentication;
            hello-interval seconds;
            hold-time seconds;
            ipv4-multicast-metric number;
            metric metric;
            passive;
            priority number;
        }
        lsp-interval milliseconds;
        mesh-group (value | blocked);
        no-ipv4-multicast;
        no-unicast-topology;
        passive;
        point-to-point;
    }
    level (1 | 2) {
        disable;
        authentication-key key;
        authentication-type authentication;
        external-preference preference;
        no-csnp-authentication;
```

```
        no-hello-authentication;
        no-psnp-authentication;
        preference preference;
        prefix-export-limit number;
        wide-metrics-only;
      }
      loose-authentication-check;
      lsp-lifetime seconds;
      max-areas number;
      no-adjacency-holddown;
      no-authentication-check;
      no-ipv4-routing;
      overload {
        advertise-high-metrics;
        timeout seconds;
      }
      reference-bandwidth reference-bandwidth;
      rib-group {
        inet group-name;
      }
      topologies {
        ipv4-multicast;
      }
      traceoptions {
        file filename <files number> <size maximum-file-size> <world-readable |
          no-world-readable>;
        flag flag <flag-modifier> <disable>;
      }
      traffic-engineering {
        disable;
        family inet {
          shortcuts {
            multicast-rpf-routes:
          }
        }
      }
    }
    lldp {
      disable;
      advertisement-interval seconds;
      hold-multiplier number;
      interface (LLDP) (all | interface-name) {
        disable;
      }
      traceoptions {
        file filename <files number> <size size> <world-readable | no-world-readable> <match
          regex>;
        flag flag (detail | disable | receive | send);
      }
    }
    mstp {
      disable;
      bpdu-timeout-action;
      bridge-priority priority;
      configuration-name name;
      forward-delay seconds;
```

```
    hello-time seconds;
    interface (all | interface-name) {
      disable;
      bpdu-timeout-action {
        block;
        alarm;
      }
      cost  cost;
      edge;
      mode mode;
      no-root-port;
      priority priority;
    }
    max-age seconds;
    max-hops hops;
    msti msti-id {
      vlan (vlan-id | vlan-name);
      interface interface-name {
        disable;
        cost  cost;
        edge;
        mode mode;
        priority priority;
      }
    }
    revision-level revision-level;
    traceoptions {
      file filename <files number > <size size> <no-stamp | world-readable |
        no-world-readable>;
      flag flag;
    }
  }
  ospf {
    disable;
    area area-id {
      area-range ip-prefix</prefix-length> <exact> <override-metric metric> <restrict>;
      context-identifier identifier
      interface interface-name {
        disable;
        authentication {
          md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
          simple-password key-string;
        }
        bandwidth-based-metrics {
          bandwidth value metric number;
        }
        bfd-liveness-detection {
          authentication {
            algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
              meticulous-keyed-sha-1 | simple-password);
            key-chain key-chain-name;
            loose-check;
          }
          detection-time {
            threshold milliseconds;
          }
```

```
      full-neighbors-only;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (1 | automatic);
    }
    dead-interval seconds;
    dynamic-neighbors;
    flood-reduction;
    hello-interval seconds;
    interface-type (nbma | p2mp | p2p);
    metric metric;
    neighbor address <eligible>;
    no-eligible-backup;
    no-interface-state-traps;
    no-neighbor-down-notification;
    passive {
      traffic-engineering {
        remote-node-id address;
      }
    }
    poll-interval seconds;
    priority number;
    retransmit-interval seconds;
    secondary;
    te-metric metric;
    topology (name | default | ipv4-multicast) {
      disable;
      bandwidth-based-metrics {
        bandwidth value;
        metric number;
      }
      metric metric;
    }
    transit-delay seconds;
  }
  network-summary-export [ policy-names ];
  network-summary-import [ policy-names ];
  nssa {
    area-range ip-prefix</prefix-length> <exact> <override-metric metric> <restrict>;
    default-lsa {
      default-metric metric;
      metric-type type;
      type-7;
    }
    (summaries | no-summaries);
  }
  stub <default-metric metric> <summaries | no-summaries>;
  virtual-link neighbor-id router-id transit-area area-id {
    disable;
    authentication {
```

```
            md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
            simple-password key-string;
          }
          dead-interval seconds;
          demand-circuit;
          flood-reduction;
          hello-interval seconds;
          ipsec-sa sa-name;
          no-neighbor-down-notification;
          retransmit-interval seconds;
          topology (name | default | ipv4-multicast) {
            disable;
            metric metric;
          }
          transit-delay seconds;
        }
      }
      database-protection {
        ignore-count number;
        ignore-time seconds;
        maximum-lsa number;
        reset-time seconds;
        warning-only;
        warning-threshold percent;
      }
      export [ policy-names ];
      external-preference preference;
      graceful-restart {
        disable;
        helper-disable <both | restart-signaling | standard>;
        no-strict-lsa-checking;
        notify-duration seconds;
        restart-duration seconds;
      }
      import [ policy-names ];
      no-nssa-abr;
      no-rfc-1583;
      overload <timeout seconds>;
      preference preference;
      prefix-export-limit number;
      reference-bandwidth reference-bandwidth;
      rib-group group-name;
      topology (default | ipv4-multicast | name) {
        overload;
        prefix-export-limit number;
        topology-id number;
      }
      traceoptions {
        file filename <files number> <size maximum-file-size> <world-readable |
          no-world-readable>;
        flag flag <flag-modifier> <disable>;
      }
      traffic-engineering {
        advertise-unnumbered-interfaces;
        credibiliity-protocol-preference;
        ignore-lsp-metrics;
```

```
      multicast-rpf-routes;
      no-topology;
      shortcuts <lsp-metric-into-summary>;
    }
  }
  pim {
    disable;
    assert-timeout seconds;
    dense-groups {
      addresses;
    }
    dr-election-on-p2p;
    export;
    family (inet | inet6) {
      disable;
    }
    graceful-restart {
      disable;
      restart-duration seconds;
    }
    import [ policy-names ];
    interface interface-name {
      accept-remote-source;
      disable;
      family (inet | inet6) {
        disable;
      }
      hello-interval seconds;
      mode (dense | sparse | sparse-dense);
      neighbor-policy [ policy-names ];
      override-interval milliseconds;
      priority number;
      propagation-delay milliseconds;
      reset-tracking-bit;
      version version;
    }
    join-load-balance;
    join-prune-timeout;
    nonstop-routing;
    override-interval milliseconds;
    propagation-delay milliseconds;
    reset-tracking-bit;
    rib-group group-name;
    rp {
      auto-rp {
        (announce | discovery | mapping);
        (mapping-agent-election | no-mapping-agent-election);
      }
      bootstrap {
        family (inet | inet6) {
          export [ policy-names ];
          import [ policy-names ];
          priority number;
        }
      }
      bootstrap-import [ policy-names ];
```

```
    bootstrap-export [ policy-names ];
    bootstrap-priority number;
    dr-register-policy [ policy-names ];
    embedded-rp {
      group-ranges {
        destination-ip-prefix</prefix-length>;
      }
      maximum-rps limit;
    }
    local {
      family (inet | inet6) {
        address address;
        anycast-pim {
          disable;
            rp-set {
            address address <forward-msdp-sa>;
          }
          local-address address;
        }
        group-ranges {
          destination-ip-prefix</prefix-length>;
        }
        hold-time seconds;
        priority number;
      }
    }
    rp-register-policy [ policy-names ];
    spt-threshold {
      infinity [ policy-names ];
    }
    static {
      address address {
        group-ranges {
        version version;
        destination-ip-prefix</prefix-length>;
        }
      }
    }
  }
  rpf-selection {
    group group-address{
      source source-address{
        next-hop next-hop-address;
      }
      wildcard-source {
        next-hop next-hop-address;
      }
    }
    prefix-list prefix-list-addresses {
      source source-address {
        next-hop next-hop-address;
      }
      wildcard-source {
        next-hop next-hop-address;
      }
    }
```

```
    traceoptions {
      file filename <files number> <size size> <world-readable | no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    tunnel-devices [ mt-fpc/pic/port ];
  }
  rip {
    authentication-key password;
    authentication-type type;
    (check-zero | no-check-zero);
    group group-name {
      bfd-liveness-detection {
        authentication {
          algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
            meticulous-keyed-sha-1 | simple-password);
          key-chain key-chain-name;
          loose-check;
        }
        detection-time {
          threshold milliseconds;
        }
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        version (1 | automatic);
      }
      export [ policy-names ];
      import [ policy-names ];
      metric-out metric;
        neighbor neighbor-name {
          any-sender;
          authentication-key password;
          authentication-type type;
          bfd-liveness-detection {
            ... same statements as at the [edit protocols rip group group-name
              bfd-liveness-detection] hierarchy level ...
          }
          (check-zero | no-check-zero);
          import [ policy-names ];
          message-size number;
          metric-in metric;
          receive (both | none | version-1 | version-2);
          route-timeout seconds;
          send (broadcast | multicast | none | version-1);
          update-interval seconds;
        }
      preference preference;
      route-timeout seconds;
      update-interval seconds;
    }
    holddown seconds;
```

```
    import [ policy-names ];
    message-size number;
    metric-in metric;
    receive (both | none | version-1 | version-2);
    rib-group group-name;
    route-timeout seconds;
    send (broadcast | multicast | none | version-1);
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    update-interval seconds;
  }
  rstp {
    disable;
    bpdu-block-on-edge;
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
      disable;
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost  cost;
      edge;
      mode mode;
      no-root-port;
      priority priority;
    }
    max-age seconds;
    }
    traceoptions {
      file filename <files number > <size size> <no-stamp> <world-readable |
        no-world-readable>;
      flag flag;
    }
  }
  stp {
    disable;
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
      disable;
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost  cost;
      edge;
      mode mode;
      no-root-port;
      priority priority;
```

```
    }
    max-age seconds;
  }
    traceoptions {
      file filename <files number > <size size> <no-stamp | world-readable |
        no-world-readable>;
      flag flag;
    }
  uplink-failure-detection {
    group group-name {
      link-to-monitor interface-name;
      link-to-disable interface-name;
    }
  }
  vstp {
    bpdu-block-on-edge;
    disable (Spanning Trees);
    force-version stp;
    vlan vlan-id {
      bridge-priority (Spanning Trees) priority;
      forward-delay (Spanning Trees) seconds;
      hello-time seconds;
      interface (Spanning Trees) (all | interface-name) {
        bpdu-timeout-action (Spanning Trees) {
          block (Spanning Trees);
          log;
        }
        cost (Spanning Trees)  cost;
        disable (Spanning Trees);
        edge (Spanning Trees);
        mode mode;
        no-root;
        priority (Spanning Trees) priority;
      }
      max-age seconds;
      traceoptions {
        file filename <files number > <size size> <no-stamp | world-readable |
          no-world-readable>;
        flag flag;
      }
    }
  }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure protocols.

The remaining statements are explained separately.

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

Related Documentation
- *Junos OS Routing Protocols Configuration Guide*

ptopo-configuration-maximum-hold-time

Syntax ptopo-configuration-maximum-hold-time *seconds*;

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 9.6 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure how long to maintain the physical topology database entries. The physical topology identifies the devices on the network and their physical interconnections.

Options ***seconds***—Time to maintain physical topology database entries.

Default: 300

Range: 1 through 2147483647

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

Related Documentation
- show lldp on page 258
- *Understanding LLDP and LLDP-MED on EX Series Switches*
- Understanding LLDP on page 5

ptopo-configuration-trap-interval

Syntax ptopo-configuration-trap-interval *seconds*;

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 9.6 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify how often SNMP trap notifications are sent regarding changes in physical topology global statistics.

Default SNMP trap notifications of changes in physical topology global statistics are disabled.

Options ***seconds***—Interval between SNMP trap notifications about physical topology global statistics.

Range: 0 through 3600

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

radius

Syntax

```
radius {
  accounting-server [server-addresses];
  authentication-server [server-addresses];
}
```

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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

The statements are explained separately.

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

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

Related Documentation

- *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*
- *Configuring 802.1X RADIUS Accounting (CLI Procedure)*
- *Filtering 802.1X Supplicants by Using RADIUS Server Attributes*
- *Configuring RADIUS Accounting*

radius-options (edit system)

Syntax

```
radius-options {
  attributes {
    nas-ip-address ip-address;
  }
  enhanced-accounting;
  password-protocol mschap-v2;
}
```

Hierarchy Level [edit system]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2.
MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

NOTE: The **radius-options** statement is not available on QFabric systems.

enhanced-accounting statement introduced in Junos OS Release 14.1.

Description Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.

Options

enhanced-accounting—View the attribute values of a logged in user.

nas-ip-address *ip-address*—IP address of the network access server (NAS) that requests user authentication.

password-protocol *mschap-v2*—Protocol MS-CHAPv2, used for password authentication and password changing.

Required Privilege Level

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

Related Documentation

- *Configuring MS-CHAPv2 for Password-Change Support*
- Configuring RADIUS System Accounting on page 145
- *enhanced-accounting*

radius-server

Syntax

```
radius-server server-address {
  accounting-port port-number;
  port number;
  retry number;
  secret password;
  source-address source-address;
  timeout seconds;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure a RADIUS server for Point-to-Point Protocol (PPP).

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

Options ***server-address***—Address of the RADIUS authentication server.

The remaining statements are explained separately.

NOTE: **The accounting-port and source-address options are not available on QFabric systems.**

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

Related Documentation

- Configuring RADIUS Authentication (QFX Series or OCX Series) on page 127
- *accounting-port*
- port on page 201
- retry on page 224
- *secret*
- *source-address*
- *timeout*

rate-limit

Syntax rate-limit *limit*;

Hierarchy Level [edit system services finger],
[edit system services ftp],
[edit system services netconf ssh],
[edit system services ssh],
[edit system services telnet],
[edit system services tftp-server],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the maximum number of connections attempts per minute, per protocol (either IPv6 or IPv4) on an access service. For example, a rate limit of 10 allows 10 IPv6 telnet session connection attempts per minute and 10 IPv4 telnet session connection attempts per minute.

Default 150 connections

Options **rate-limit *limit***—(Optional) Maximum number of connection attempts allowed per minute, per IP protocol (either IPv4 or IPv6).

Range: 1 through 250

Default: 150

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

Related Documentation

- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*

remote-debug-permission

Syntax remote-debug-permission (qfabric-admin | qfabric-operator | qfabric-user);

Hierarchy Level [edit system login user *username* authentication]
[edit system root-authentication]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description (QFabric systems only) Configure authentication classes that permit or deny user access to individual components of the QFabric system.

Default qfabric-user

Options

qfabric-admin—Permits a user to log in to individual QFabric system components, view operations, and change component configurations.

qfabric-operator—Permits a user to log in to individual QFabric system components and view component operations.

qfabric-user—Prevents a user from logging in to individual QFabric system components.

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

Related Documentation

- *Example: Configuring QFabric System Login Classes*
- request component login on page 252
- *Understanding QFabric System Login Classes*

retry

Syntax retry *number*;

Hierarchy Level [edit system radius server *server-address*],
[edit system accounting destination radius server *server-address*]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Number of times the router or switch is allowed to try to contact a RADIUS authentication or accounting server.

Options ***number***—Number of retries allowed for contacting a RADIUS server.

Range: 1 through 10

Default: 3

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

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

Related Documentation

- Configuring RADIUS Authentication (QFX Series or OCX Series) on page 127
- *Configuring RADIUS Accounting*
- *timeout*

rising-threshold (Health Monitor)

Syntax rising-threshold *percentage*;

Hierarchy Level [edit snmp health-monitor]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Set the upper threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored object, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options ***percentage***—Upper threshold for the alarm entry.

Range: 1 through 100

Default: 80 percent of the maximum possible value

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

Related Documentation

- *Configuring Health Monitoring*
- falling-threshold on page 188

root-login

Syntax root-login (allow | deny | deny-password);

Hierarchy Level [edit system services ssh]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Control user access through SSH.

Default **root-login deny-password** is the default.

Options **allow**—Allow users to log in to the router or switch as root through SSH.

deny—Disable users from logging in to the router or switch as root through SSH.

deny-password—Allow users to log in to the router or switch as root through SSH when the authentication method (for example, RSA authentication) does not require a password.

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

Related Documentation

- *Configuring SSH Service for Remote Access to the Router or Switch*

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);
  }
}
}
```

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 SNMP.

The remaining statements are explained separately.

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

Related Documentation

- *Understanding the Implementation of SNMP*
- *Configuring SNMP*

ssh

Syntax

```
ssh {
  authentication-order [method 1 method2...];
  ciphers [ cipher-1 cipher-2 cipher-3 ...];
  client-alive-count-max seconds;
  client-alive-interval seconds;
  connection-limit limit;
  fingerprint-hash (md5 | sha2-256);
  hostkey-algorithm (algorithm | no-algorithm);
  key-exchange [algorithm1 algorithm2...];
  macs [algorithm1 algorithm2...];
  max-sessions-per-connection <number>;
  no-passwords;
  no-public-keys;
  no-tcp-forwarding;
  protocol-version [v1 v2];
  rate-limit limit;
  root-login (allow | deny | deny-password);
  }
tcp-forwarding (JDM)
```

Hierarchy Level [edit system services]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
client-alive-interval and **client-alive-max-count** statements introduced in Junos OS Release 12.2.
no-passwords statement introduced in Junos OS Release 13.3.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
no-public-keys statement introduced in Junos OS release 15.1.
tcp-forwarding statement introduced in Junos OS Release 15.1X53-D50 for the NFX250 Network Services Platform.
fingerprint-hash statement introduced in Junos OS Release 16.1.

Description Allow SSH requests from remote systems to access the local router or switch.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Configuring SSH Service for Remote Access to the Router or Switch*

system

Syntax

```
system {
  accounting {
    events [ login change-log interactive-commands ];
    destination {
      radius {
        {
          server server-address {
            accounting-port port-number;
            retry number;
            secret password;
            source-address address;
            timeout seconds;
          }
        }
      }
      tacplus {
        server {
          server server-address {
            port port-number;
            secret password;
            single-connection;
            timeout seconds;
          }
        }
      }
    }
  }
  archival {
    configuration {
      archive-sites {
        ftp://<username>:<password>@<host>:<port>/<url-path>;
        ftp://<username>:<password>@<host>:<port>/<url-path>;
      }
      transfer-interval interval;
      transfer-on-commit;
    }
  }
  arp {
    aging-timer minutes;
    interfaces;
  }
  authentication-order [ authentication-methods ];
  (compress-configuration-files | no-compress-configuration-files);
  default-address-selection;
  domain-name domain-name;
  domain-search [ domain-list ];
  host-name hostname;
  internet-options {
    icmpv4-rate-limitbucket-size bucket-size packet-rate packet-rate;
    source-port upper-limit <upper-limit>;
  }
  location {
```

```
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack number;
    vcoord vertical-coordinate;
  }
  login {
    announcementtext;
    class class-name {
      access-end;
      access-start;
      allow-configuration “regular-expression”;
      allowed-days “regular-expression”;
      deny-commands “regular-expression”;
      deny-configuration “regular-expression”;
      idle-timeout minutes;
      login-tip;
      permissions [ permissions ];
    }
    message text;
    password {
      change-type (set-transitions | character-set);
      format (md5 | sha1 | des);
      maximum-length length;
      minimum-changes number;
      minimum-length length;
    }
    retry-options {
      backoff-factor seconds;
      backoff-threshold number;
      minimum-time seconds;
      tries-before-disconnect number;
    }
    user username {
      authentication {
        (encrypted-password "password" | plain-text-password);
        load-key-file URL;
        remote-debug-permission (qfabric-admin | qfabric-operator |qfabric-user);
        ssh-rsa "public-key";
        ssh-dsa "public-key";
      }
      uid uid-value;
      class class-name;
      full-name complete-name;
    }
  }
  name-server {
    address;
  }
```

```
no-multicast-echo;
no-redirects;
no-ping-record-route;
no-ping-time-stamp;
ntp {
  authentication-key number type type value password;
  server address <key key-number> <version value> <prefer>;
}
ports {
  auxiliary {
    disable;
    insecure;
    type terminal-type;
  }
  console {
    disable;
    insecure;
    log-out-on-disconnect;
    type terminal-type;
  }
}
radius-server server-address {
  accounting-port port-number;
  port number;
  retry number;
  secret password;
  source-address source-address;
  timeout seconds;
  }
}
radius-options {
  password-protocol mschap-v2;
  }
  attributes {
    nas-ip-address ip-address;
root-authentication {
  (encrypted-password "password" | plain-text-password);
  ssh-rsa "public-key";
  ssh-dsa "public-key";
}
(saved-core-context | no-saved-core-context);
saved-core-files saved-core-files;
services {
  finger {
    connection-limit limit;
    rate-limit limit;
  }
  flow-tap-dtcp {
    ssh {
      connection-limit limit;
      rate-limit limit;
    }
  }
  ftp {
    connection-limit limit;
    rate-limit limit;
```

```
    }
    service-deployment {
      servers server-address {
        port port-number;
      }
      source-address source-address;
    }
    ssh {
      root-login (allow | deny | deny-password);
      protocol-version [v1 v2];
      connection-limit limit;
      rate-limit limit;
    }
    telnet {
      connection-limit limit;
      rate-limit limit;
    }
    web-management {
      http {
        interfaces [ interface-names ];
        port port;
      }
      https {
        interfaces [ interface-names ];
        local-certificate name;
        port port;
      }
      session {
        idle-timeout [ minutes ];
        session-limit [ session-limit ];
      }
    }
    xnm-clear-text {
      connection-limit limit;
      rate-limit limit;
    }
    xnm-ssl {
      connection-limit limit;
      local-certificate name;
      rate-limit limit;
    }
  }
  static-host-mapping {
    hostname {
      alias [ alias ];
      inet [ address ];
      sysid system-identifier;
    }
  }
  syslog {
    archive {
      files number;
      size maximum-file-size;
      start-time "YYYY-MM-DD.hh:mm";
      transfer-interval minutes;
      (world-readable | no-world-readable);
```

```
    }
    console {
      facility severity;
    }
    file filename {
      archive {
        files number;
        size maximum-file-size;
        start-time "YYYY-MM-DD.hh:mm";
        transfer-interval minutes;
        (world-readable | no-world-readable);
      }
      explicit-priority;
      facility severity;
      match "regular-expression";
      structured-data {
        brief;
      }
    }
    host (hostname | other-routing-engine | scc-master) {
      explicit-priority;
      facility-override facility;
      facility severity;
      log-prefix string;
      match "regular-expression";
    }
    source-address source-address;
    time-format (millisecond | year | year millisecond);
    user (username | *) {
      facility severity;
      match "regular-expression";
    }
  }
  tacplus-options {
    service-name service-name;
    (no-cmd-attribute-value | exclude-cmd-attribute);
  }
  tacplus-server server-address {
    port
    secret password;
    single-connection;
    source-address source-address;
    timeout seconds;
  }
  time-zone (GMThour-offset | time-zone);
  }
  tracing {
    destination-override {
    syslog host;
    }
  }
  use-imported-time-zones;
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure system management properties.

NOTE: The radius-server source-address and radius-options statements are not available on the QFabric system.

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

tacplus-options

Syntax

```
tacplus-options {
  (exclude-cmd-attribute | no-cmd-attribute-value);
  enhanced-accounting;
  service-name service-name;
  timestamp-and-timezone;
}
```

Hierarchy Level [edit system]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
no-cmd-attribute-value and **exclude-cmd-attribute** options introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 11.1 for QFX Series.
timestamp-and-timezone option introduced in Junos OS Release 12.2.
enhanced-accounting option introduced in Junos OS Release 14.1.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure TACACS+ options for authentication and accounting.

Options

enhanced-accounting—View the attribute values of a logged in user.

exclude-cmd-attribute—Exclude the **cmd** attribute value completely from start and stop accounting records to enable logging of accounting records in the correct log file on a TACACS+ server.

no-cmd-attribute-value—Set the **cmd** attribute value to an empty string in the TACACS+ accounting start and stop requests to enable logging of accounting records in the correct log file on a TACACS+ server.

service-name *service-name*—Name of the authentication service used when you configure multiple TACACS+ servers to use the same authentication service.

Default: junos-exec

timestamp-and-timezone—Include this statement if you want start time, stop time, and timezone attributes included in start/stop accounting records.

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

Related Documentation

- *Configuring TACACS+ Authentication*
- *Configuring TACACS+ System Accounting*
- Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 113
- *enhanced-accounting*

targets

Syntax

```
targets {
  address;
}
```

Hierarchy Level [edit snmp trap-group *group-name*]

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 one or more systems to receive SNMP traps.

Options ***address***—IPv4 or IPv6 address of the system to receive traps. You must specify an address, not a hostname.

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

Related Documentation

- *Configuring SNMP Trap Groups*

traceoptions (LLDP)

Syntax

```
traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable> <no-stamp>
    <replace>;
  flag flag <disable>;
}
```

Hierarchy Level [edit protocols lldp]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Define tracing operations for the Link Layer Discovery Protocol (LLDP). You can trace messages under LLDP for LLDP and PTOPO MIBs.

NOTE: The traceoptions statement is not supported on the QFX3000 QFabric system.

Default Tracing operations are disabled.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- **all**—All tracing operations.
- **configuration**—Trace configuration operations.
- **interface**—Trace interface update events.
- **netbios**—Trace NetBIOS events.
- **packet**—Trace packet events.
- **rtsock**—Trace routing socket operations.
- **snmp**—Trace SNMP configuration operations.

- **vlan**—Trace VLAN update events.

no-stamp—(Optional) Do not timestamp the trace file.

Default: If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

no-world-readable—(Optional) Restrict file access to the user who created the file.

replace—(Optional) Replace an existing trace file if there is one rather than appending output to it.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **files** option.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

Default: If you do not include this option, tracing output is appended to an existing trace file.

world-readable—(Optional) Enable unrestricted file access.

NOTE: The traceoptions statement is not supported on the QFX3000 QFabric system.

Required Privilege Level

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

Related Documentation

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

transfer-interval (Configuration)

Syntax transfer-interval *interval*;

Hierarchy Level [edit system archival configuration]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the router or switch to periodically transfer its currently active configuration to an archive site.

Options ***interval***—Interval at which to transfer the current configuration to an archive site.

Range: 15 through 2880 minutes

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

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

Related Documentation

- *Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site*
- *archive*
- configuration on page 185
- transfer-on-commit on page 244

transfer-on-commit

Syntax transfer-on-commit;

Hierarchy Level [edit system archival configuration]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Configure the 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.

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*
- *archive*
- configuration on page 185
- transfer-interval on page 243

trap-group

Syntax

```
trap-group group-name {
  categories {
    category;
  }
  destination-port port-number;
  routing-instance instance;
  targets {
    address;
  }
  version (all | v1 | v2);
}
```

Hierarchy Level [edit snmp]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Create a named group of hosts to receive the specified trap notifications. The name of the trap group is embedded in SNMP trap notification packets as one variable binding (varbind) known as the community name. At least one trap group must be configured for SNMP traps to be sent.

Options ***group-name***—Name of the trap group. If the name includes spaces, enclose it in quotation marks (" ").

The remaining statements are explained separately.

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

Related Documentation

- *Configuring SNMP Trap Groups*

trap-options

Syntax

```
trap-options {
  agent-address outgoing-interface;
  source-address address;
}
```

Hierarchy Level [edit snmp]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description 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.

The remaining statements are explained separately.

Default Disabled

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

Related Documentation

- *Configuring SNMP Trap Options*

user (Access)

Syntax

```
user username {
  authentication {
    (encrypted-password "password" | plain-text-password);
    load-key-file URL;
    remote-debug-permission (qfabric-admin | qfabric-operator |qfabric-user);
    ssh-dsa "public-key" <from hostname>;
    ssh-rsa "public-key" <from hostname>;
  }
  class class-name;
  full-name "complete-name";
  uid uid-value;
}
```

Hierarchy Level [edit system login]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure access permission for individual users.

Options The remaining statements are explained separately.

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

Related Documentation

- Configuring Junos OS User Accounts on page 106
- *class*

version

Syntax version (all | v1 | v2);

Hierarchy Level [edit snmp trap-group *group-name*]

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 Specify the version number of SNMP traps.

Default **all**—Send an SNMPv1 and SNMPv2 trap for every trap condition.

Options **all**—Send an SNMPv1 and SNMPv2 trap for every trap condition.

v1—Send SNMPv1 traps only.

v2—Send SNMPv2 traps only.

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

Related Documentation

- *Configuring SNMP Trap Groups*

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

Syntax clear lldp neighbors <interface *interface*>

Release Information Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description Clear the learned remote neighbor information on all or selected interfaces.

Options **none**—Clear the remote neighbor information on all interfaces.

interface *interface*—(Optional) Clear the remote neighbor information from the selected interface.

Required Privilege Level view

Related Documentation
- Understanding LLDP on page 5

List of Sample Output
clear lldp neighbors on page 250
clear lldp neighbors interface on page 250

Sample Output

clear lldp neighbors

```
user@switch> clear lldp neighbors
```

clear lldp neighbors interface

```
user@switch> clear lldp neighbors interface ge-0/1/1.0
```

clear lldp statistics

Syntax clear lldp statistics
<interface *interface*>

Release Information Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description Clear LLDP statistics on one or more interfaces.

Options **none**—Clears LLDP statistics on all interfaces.

interface *interface-names*—(Optional) Clear LLDP statistics on an interface.

Required Privilege Level view

Related Documentation
- Understanding LLDP on page 5

List of Sample Output
clear lldp statistics on page 251
clear lldp statistics interface on page 251

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

Syntax request component login *component-name*

Release Information Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description (QFabric systems only) Log in to a QFabric system component. To gain access to individual components by way of the **request component login** command, you must first provide the **qfabric-admin** or **qfabric-operator** class privilege to your user (for more information, see: remote-debug-permission).

Options ***component-name***—Specify the QFabric system component to which you wish to log in.

Required Privilege Level admin

Related Documentation
- remote-debug-permission on page 223

List of Sample Output

Sample Output

The three sample output displays show the results of attempts to log in to Node device EE3093. The results differ depending on the privilege level assigned to the user.

request component login (with qfabric-admin Privileges)

```
admin@qfabric> request component login EE3093
Warning: Permanently added 'qfabric-node-ee3093,192.0.2.0' (RSA) to the list of
known hosts.
--- JUNOS 11.3I built 2011-11-04 12:46:16 UTC
{master}
qfabric-admin@node-ee3093> ?
Possible completions:
  clear                Clear information in the system
  file                 Perform file operations
  help                 Provide help information
  load                 Load information from file
  monitor              Show real-time debugging information
  mtrace               Trace multicast path from source to receiver
  op                   Invoke an operation script
  ping                 Ping remote target
  quit                 Exit the management session
  request              Make system-level requests
  restart              Restart software process
  save                 Save information to file
  set                  Set CLI properties, date/time, craft interface message
  show                 Show system information
  ssh                  Start secure shell on another host
  start                Start shell
  telnet               Telnet to another host
  test                 Perform diagnostic debugging
```



```
  traceroute           Trace route to remote host{master}
qfabric-admin@node-ee3093>
```

request component login (with qfabric-operator Privileges)

```
operator@qfabric> request component login EE3093
Warning: Permanently added 'qfabric-node-EE3093,192.0.2.0' (RSA) to the list of
known hosts.
--- JUNOS 11.3I built 2011-11-04 12:46:16 UTC
{master}
qfabric-operator@node-EE3093> ?
Possible completions:
  file                 Perform file operations
  help                 Provide help information
  load                 Load information from file
  op                   Invoke an operation script
  quit                 Exit the management session
  request              Make system-level requests
  save                 Save information to file
  set                  Set CLI properties, date/time, craft interface message
  show                 Show system information
  start                Start shell
  test                 Perform diagnostic debugging
{master}
qfabric-operator@node-ee3093>
```

request component login (with qfabric-user Privileges)

```
user0@qfabric> request component login EE3093
error: User user0 does not have sufficient permissions to login to device ee3093
```

show ethernet-switching interfaces

Syntax
show ethernet-switching interfaces
<brief | detail | summary>
<interface *interface-name*>

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 information about switched Ethernet interfaces.

Options
none—(Optional) Display brief information for Ethernet-switching interfaces.

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

interface *interface-name*—(Optional) Display Ethernet-switching information for a specific interface.

Required Privilege Level
view

Related Documentation
- *Troubleshooting Ethernet SwitchingUnderstanding Bridging and VLANs*
- *Example: Setting Up Basic Bridging and a VLAN on the QFX Series*
- *Example: Setting Up Bridging with Multiple VLANs*
- *Understanding FCoE*
- *Interfaces Overview*

List of Sample Output
show ethernet-switching interfaces on page 255
show ethernet-switching interfaces summary on page 256
show ethernet-switching interfaces brief on page 256
show ethernet-switching interfaces detail on page 256
show ethernet-switching interfaces interface-name on page 257

Output Fields
Table 37 on page 254 lists the output fields for the **show ethernet-switching interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 37: show ethernet-switching interfaces Output Fields

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

Table 37: show ethernet-switching interfaces Output Fields *(continued)*

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

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 261
show lldp (EX4300 switches) on page 261
show lldp detail (EX4300 switches) on page 262

Output Fields

Table 38 on page 258 lists the output fields for the **show lldp** command. Output fields are listed in the approximate order in which they appear.

Table 38: show lldp Output Fields

Field Name	Field Description	Level of Output
LLDP	LLDP operating state. The state can be **enabled** or **disabled**. NOTE: If a VLAN that has been configured for untagged packets on an interface also has Layer 2 protocol tunneling (L2PT) enabled for LLDP, the LLDP operating state for that interface is displayed as **disabled**.	All levels

Table 38: show lldp Output Fields *(continued)*

Field Name	Field Description	Level of Output
Advertisement interval	Frequency, in seconds, at which LLDP advertisements are sent. This value is set by the advertisement-interval configuration statement.	All levels
Transmit delay	Seconds of delay before advertisements are sent to neighbors following a change to a TLV (type, length, or value) element in the LLDP protocol or to the state of the local system, such as a change in hostname or management address. You can set this value to reduce the delay in notifying neighbors of a change in the local system. This value is set by the *transmit-delay* configuration statement.	All levels
Hold timer	On EX4300 switches, the hold timer shows the length of time LLDP information is held before it is discarded. The hold timer value is equal to the advertisement interval multiplied by the hold multiplier. On all other switches, the hold timer shows the value of the hold multiplier. The hold multipler value is set by the hold-multiplier configuration statement.	All levels
Notification interval	How often LLDP trap notifications are generated as a result of LLDP database changes. If the interval value is 0, LLDP trap notifications on database changes are disabled. This value is set by the ***lldp-configuration-notification-interval*** configuration statement.	All levels
Config Trap Interval	How often LLDP trap notifications are generated as a result of changes in topology—for example, when an endpoint connects or disconnects. If the interval value is 0, LLDP trap notifications on topology changes are disabled. This value is set by the ptopo-configuration-trap-interval configuration statement.	All levels
Connection Hold timer	Amount of time the system maintains dynamic topology entries. This value is set by the ptopo-configuration-maximum-hold-time configuration statement.	All levels
LLDP-MED	LLDP-MED operating state. The state can be **Enabled** or **Disabled**.	All levels
MED fast start count	Number of advertisements sent from a switch to a device, such as a VoIP telephone, when the device is first detected by the switch. These increased advertisements are temporary. After a device and a switch exchange information and can communicate, advertisements are reduced to one per second. This value is set by using the ***fast-start*** configuration statement. NOTE: **fast-start**is not available on the QFX Series.	All levels
Interface	Name of the interface for which LLDP configuration information is being reported.	All levels
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs.	All levels

Table 38: show lldp Output Fields *(continued)*

Field Name	Field Description	Level of Output
LLDP	LLDP operating state. The state can be **Enabled** or **Disabled**.	All levels
Power Negotiation	LLDP power negotiation operating state. The state can be **Enabled** or **Disabled**.	All levels
Neighbor count	Total number of new LLDP neighbors detected since the last switch reboot.	**detail**
Interface	Name of the interface that is advertising VLAN information.	All levels
Vlan-id	VLAN tag associated with the interface sending LLDP frames. If the interface is not a member of a VLAN, the VLAN ID is advertised as 0.	**detail**
Vlan-name	VLAN name associated with the VLAN ID.	**detail**
LLDP basic TLVs supported	Basic TLVs supported on the switch: • **Chassis identifier**—TLV that advertises the MAC address associated with the local system. • **Port identifier**—TLV that advertises the port identification for the specified port in the local system. • **Port description**—Interface name for the port. • **System name**—TLV that advertises the user-configured name of the local system. • **System description**—TLV that advertises the system description containing information about the software and current image running on the system. This information is taken from the software and is not configurable. • **System capabilities**—TLV that advertises the primary functions performed by the system—for example, bridge or router. • **Management address**—TLV that advertises the IP management address of the local system.	**detail**
Supported LLDP 802 TLVs	802.3 TLVs supported on the switch: • **MAC/PHY configuration status**—TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information is based on the physical interface structure and is not configurable. • **Power via MDI**—TLV that advertises MDI power support, PSE power pair, and power class information. • **Link aggregation**—TLV that advertises if the interface is aggregated and its aggregated interface ID. • **Maximum frame size**—TLV that advertises the maximum transmission unit (MTU) of the interface sending LLDP frames. • **Port VLAN tag**—TLV that advertises the VLAN tag configured on the interface. • **Port VLAN name**—TLV that advertises the VLAN name configured on the interface.	**detail**

Table 38: show lldp Output Fields *(continued)*

Field Name	Field Description	Level of Output

Supported LLDP MED TLVs	LLDP-MED TLVs supported on the switch:
	• **LLDP MED capabilities**—TLV that advertises the primary function of the port. The capabilities values range from 0 through 15:
	  ◦ **0**—Capabilities
	  ◦ **1**—Network Policy
	  ◦ **2**—Location Identification
	  ◦ **3**—Extended Power via MDI-PSE
	  ◦ **4**—Inventory
	  ◦ **5–15**—Reserved
	• **Network policy**—TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types—such as voice or streaming video—802.1Q VLAN tagging, and 802.1p priority bits and DiffServ code points.
	• **Endpoint location**—TLV that advertises the physical location of the endpoint.
	• **Extended power Via MDI**—TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.
		detail

Sample Output

show lldp (EX3200 switches)

```
user@switch> show lldp
LLDP                      : Enabled
Advertisement interval    : 30 seconds
Transmit delay            : 2 seconds
Hold timer                : 4 seconds
Notification interval     : 0 Second(s)
Config Trap Interval      : 0 seconds
Connection Hold timer     : 300 seconds

LLDP MED                  : Disabled
MED fast start count      : 3 Packets


Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
all            -                   Enabled     Enabled      Enabled
```

show lldp (EX4300 switches)

```
user@switch> show lldp
LLDP                      : Enabled
Advertisement interval    : 30 seconds
Transmit delay            : 2 seconds
Hold timer                : 120 seconds
Notification interval     : 0 Second(s)
Config Trap Interval      : 0 seconds
Connection Hold timer     : 300 seconds

LLDP MED                  : Disabled
MED fast start count      : 3 Packets
```

```
Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
all            -                   Enabled     Enabled      Enabled
```

show lldp detail (EX4300 switches)

```
user@switch> show lldp detail
LLDP                     : Enabled
Advertisement interval   : 30 seconds
Transmit delay           : 2 seconds
Hold timer               : 120 seconds
Notification interval    : 0 Second(s)
Config Trap Interval     : 0 seconds
Connection Hold timer    : 300 seconds

LLDP MED                 : Disabled
MED fast start count     : 3 Packets


Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
  Neighbor count
all            -                   Enabled     Enabled      Enabled
  8

Interface      Parent Interface    Vlan-id     Vlan-name
xe-3/0/0.0     ae31.0              100         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

Syntax show lldp local-information

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description Display the information that the switch provides in Link Layer Discovery Protocol (LLDP) advertisements to its neighbors.

Required Privilege Level view

Related Documentation

- *Configuring LLDP (CLI Procedure)*
- *Understanding LLDP and LLDP-MED on EX Series Switches*
- management-address on page 197
- *Configuring LLDP*
- Understanding LLDP on page 5

List of Sample Output show lldp local-information (EX Series Switch) on page 264

Output Fields Table 39 on page 263 lists the output fields for the **show lldp local-information** command. Output fields are listed in the approximate order in which they appear.

Table 39: show lldp local-information Output Fields

Field Name	Field Description
LLDP Local Information details	Information about the local system (the switch): • **Chassis ID**—MAC address associated with the switch. • **System name**—User-configured name of the switch. • **System descr**—System description containing information about the switch model and the current software image running on the switch. This information is taken from the software and is not configurable.
System Capabilities	Capabilities (such as **bridge** or **router**) that are supported or enabled on the system.
Management Information	Details of the management information: **Port Name**, **Port Address** (such as **10.204.34.35**), **Address Type** (such as **ipv4** or **ipv6**), **Port ID** (SNMP interface index), **Port ID Subtype**, and **Port Subtype**. The **Port Subtype** displays: • **ifIndex(2)**— IP address of the switch's management Ethernet interface (**me0**) or virtual management Ethernet (**VME**) interface address (for a virtual chassis) is used to manage the switch. • **unknown(1)**—IP management address has been configured with set **protocols lldp management-address**.

Table 39: show lldp local-information Output Fields *(continued)*

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

Sample Output

show lldp local-information (EX Series Switch)

```
user@switch> show lldp local-information

LLDP Local Information details

Chassis ID   : 00:1d:b5:aa:b9:f0
System name  : switch
System descr : Juniper Networks, Inc. ex8208 , version 10.4I0 [builder] Build
               date: 2010-11-17 12:38:30 UTC

System Capabilities
    Supported       : Bridge Router
    Enabled         : Bridge Router

Management Information
    Port Name       : -
    Port Address    : 10.93.54.6
    Address Type    : IPv4
    Port ID         : 34
    Port ID Subtype : local(7)
    Port Subtype    : ifIndex(2)

Interface name Parent Interface  SNMP Index Interface description Status Tunneling
me0.0          -                 34         -                     Down   Disabled
xe-3/0/0.0     ae31.0            769        xe-3/0/0.0            Up     Disabled
xe-3/0/1.0     ae31.0            770        xe-3/0/1.0            Up     Disabled
xe-3/0/2.0     ae31.0            771        xe-3/0/2.0            Up     Disabled
xe-3/0/3.0     ae31.0            772        xe-3/0/3.0            Up     Disabled
xe-3/0/4.0     ae31.0            577        xe-3/0/4.0            Up     Disabled
xe-3/0/5.0     ae31.0            578        xe-3/0/5.0            Up     Disabled
xe-3/0/6.0     ae31.0            579        xe-3/0/6.0            Up     Disabled
xe-3/0/7.0     ae31.0            581        xe-3/0/7.0            Up     Disabled
```

show lldp neighbors

Syntax
<show lldp *neighbors*>
<interface *interface-ids*>

Release Information
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display learned information about Link Layer Discovery Protocol (LLDP) on all neighboring interfaces or on selected interfaces.

Options
none—Display learned LLDP information on all neighboring interfaces and devices.

interface *interface-ids*—(Optional) Display learned LLDP information on the selected interfaces or devices.

NOTE: When a port with DCBX enabled begins to exchange type, length, and value (TLV) entries, optional LLDP TLVs on that port are not advertised to neighbors in order to interoperate with a wider variety of converged network adapters (CNAs). As a result, information for those ports will not be listed in the output for this command.

Required Privilege Level
view

Related Documentation
- Understanding LLDP on page 5

List of Sample Output
show lldp neighbors on page 267
show lldp neighbors interface on page 268

Output Fields
Table 40 on page 265 lists the output fields for the **show lldp neighbors** command. Output fields are listed in the approximate order in which they appear.

Table 40: 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.
System name	List of system names gathered from neighbors.

Table 40: show lldp neighbors Output Fields *(continued)*

Field Name	Field Description
LLDP Neighbor Information	Information about both the local system (the switch) and a neighbor system on the interface (appears when the **interface** option is used).
Local Information	Information about the local system (appears when the **interface** option is used).
Index	Local interface index (appears when the **interface** option is used).
Time to live	Number of seconds for which this information is valid (appears when the **interface** option is used).
Time mark	Date and timestamp of information (appears when the **interface** option is used).
Local Interface	Name of the local physical interface (appears when the **interface** option is used).
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the **interface** option is used).
Local Port ID	Local interface SNMP index (appears when the interface option is used).
Ageout Count	Number of times the complete set of information advertised by the neighbor has been deleted from LLDP neighbor information maintained by the local system because the information timeliness interval has expired (appears when the **interface** option is used).
Neighbor Information	Information about a neighbor system on the interface (appears when the **interface** option is used).
Chassis type	Type of chassis identifier supplied, such as **MAC address** (appears when the **interface** option is used).
Chassis ID	Chassis identifier of the chassis type listed (appears when the **interface** option is used).
Port type	Type of port identifier supplied, such as **locally assigned** (appears when the **interface** option is used).
Port ID	Port identifier of the port type listed (appears when the **interface** option is used).
Port description	Port description (appears when the **interface** option is used).
System name	Name supplied by the system on the interface (appears when the **interface** option is used).
System Description	Description supplied by the system on the interface (appears when the **interface** option is used).

Table 40: show lldp neighbors Output Fields *(continued)*

Field Name	Field Description
System capabilities	Capabilities (such as **Bridge**, **Router**, and **Telephone**) that are supported or enabled by the system on the interface (appears when the **interface** option is used).
Management Info	Details of management information: **Type** (such as **ipv4** or **ipv6**), **Address** (such as **10.204.34.35**), **Port ID**, **Subtype**, **Interface Subtype**, and organization identifier (**OID**) (appears when the **interface** option is used). The **Interface Subtype** displays: • **ifIndex(2)**— IP address of the neighbor's management Ethernet interface (**me0**) or virtual management Ethernet (**VME**) interface address (for a virtual chassis) is used to manage the switch. • **unknown(1)**—Neighbor's IP management address has been configured with set **protocols lldp management-address**.
Media Info	Additional details about the endpoint device appear when a device that supports LLDP-MED is attached to the interface. The specific details depend upon the capabilities of the device. Details might include **Media endpoint class** (such as Class 3 for communication devices such as IP phones), **MED Hardware revision**, **MED Firmware revision**, **MED Software revision**, **MED Serial number**, **MED Manufacturer name**, or **MED Model name**.
Organization Info	One or more entries listing remote information by organizationally unique identifier (**OUI**), **Subtype**, **Index**, and **Info** (appears when the **interface** option is used).
Age	How long the neighbor has been identified (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).
Local Interface	Name of the local physical interface (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).
Chassis ID	Chassis identifier of the chassis type listed (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).
Port description	Port description (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).
System name	NetBIOS name of the host (appears when the **interface** option is used and NetBIOS snooping is enabled on the switch).

Sample Output

show lldp neighbors

```
user@switch> show lldp neighbors
```

```
Local Interface   Parent Interface   Chassis Id          Port info    System Name
xe-3/0/4.0        ae31.0             b0:c6:9a:63:80:40   xe-0/0/0.0   newyork31
xe-3/0/5.0        ae31.0             b0:c6:9a:63:80:40   xe-0/0/1.0   newyork31
xe-3/0/6.0        ae31.0             b0:c6:9a:63:80:40   xe-0/0/2.0   newyork31
xe-3/0/7.0        ae31.0             b0:c6:9a:63:80:40   xe-0/0/3.0   newyork31
xe-3/0/0.0        ae31.0             b0:c6:9a:63:80:40   xe-0/1/0.0   newyork31
xe-3/0/1.0        ae31.0             b0:c6:9a:63:80:40   xe-0/1/1.0   newyork31
xe-3/0/2.0        ae31.0             b0:c6:9a:63:80:40   xe-0/1/2.0   newyork31
xe-3/0/3.0        ae31.0             b0:c6:9a:63:80:40   xe-0/1/3.0   newyork31
```

show lldp neighbors interface

```
user@switch> show lldp neighbors interface ge-0/0/2

LLLDP Neighbor Information:
Local Information:
Index: 1 Time to live: 240 Time mark: Wed Dec  1 10:23:24 2010 Age: 29 secs
Local Interface    : ge-0/0/2.0
Parent Interface   : -
Local Port ID      : 507
Ageout Count       : 0

Neighbour Information:
Chassis type       : Mac address
Chassis ID         : 00:1f:12:38:7f:c0
Port type          : Locally assigned
Port ID            : 507
Port description   : ge-0/0/2.0
System name        : bng-l48p5-dev


System Description : Juniper Networks, Inc. ex4200-48p , version 10.4I0 Build
date: 2010-11-30 09:32:17 UTC

System capabilities
        Supported  : Bridge Router
        Enabled    : Bridge Router

Management Info
        Type              : IPv4
        Address           : 10.204.96.235
        Port ID           : 34
        Subtype           : 1
        Interface Subtype : ifIndex(2)
        OID               : 1.3.6.1.2.1.31.1.1.1.1.34
Media endpoint class: Network Connectivity

Organization Info
       OUI      : 0.12.f
       Subtype  : 1
       Index    : 1
       Info     : 22A8360000

Organization Info
       OUI      : 0.12.f
       Subtype  : 2
       Index    : 2
       Info     : 030100
```

show lldp statistics

Syntax show lldp statistics
<interface *interface-ids*>

Release Information Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Display LLDP statistics on all or selected interfaces.

Options **none**—Display LLDP statistics on all interfaces and devices.

interface *interface-ids*—(Optional) Display LLDP statistics on the selected devices.

Required Privilege Level view

Related Documentation
- Understanding LLDP on page 5

List of Sample Output show lldp statistics on page 269

Output Fields Table 41 on page 269 lists the output fields for the **show lldp statistics** command. Output fields are listed in the approximate order in which they appear.

Table 41: show lldp statistics Output Fields

Field Name	Field Description	Level of Output
Interface	Name of an interface.	All levels
Received	Total number of LLDP frames received on an interface.	All levels
Unknown-TLVs	Number of unrecognized LLDP TLVs received on an interface.	All levels
With Errors	Number of LLDP frames received that contain errors.	All levels
Discarded TLVs	Number of LLDP TLVs received and then discarded on an interface.	All levels
Transmitted	Total number of LLDP frames transmitted on an interface.	All levels
Untransmitted	Total number of LLDP frames not transmitted on an interface.	All levels

Sample Output

show lldp statistics

```
user@switch> show lldp statistics

Interface  Received  Unknown TLVs  With Errors  Discarded TLVs  Transmitted
Untransmitted
me0.0      0         0             0            0               8003         0
```

ge-0/0/0.0	8002	0	0	0	8003	0
ge-0/0/1.0	8002	0	0	0	8003	0

show route instance

Syntax
show route instance
<brief | detail | summary>
<*instance-name*>
<operational>

Release Information
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description
(QFabric systems only) Display routing instance information.

Options
none—(Same as **brief**) Display standard information about all routing instances.

brief | detail | summary—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to **brief**. (These options are not available with the **operational** keyword.)

instance-name—(Optional) Display information for a specified routing instance.

operational—(Optional) Display operational routing instances.

Required Privilege Level
view

List of Sample Output
show route instance on page 272
show route instance detail on page 272
show route instance operational on page 273
show route instance summary on page 273

Output Fields
Table 42 on page 271 lists the output fields for the **show route instance** command. Output fields are listed in the approximate order in which they appear.

Table 42: show route instance Output Fields

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

Table 42: show route instance Output Fields *(continued)*

Field Name	Field Description	Level of Output
Primary RIB	Primary table for this routing instance.	**brief** none **summary**
Active/holddown/hidden	Number of active, hold-down, and hidden routes.	All levels

Sample Output

show route instance

```
user@switch> show route instance
Instance             Type
         Primary RIB                                    Active/holddown/hidden
master               forwarding
         inet.0                                         4/0/1

__juniper_private1__ forwarding
         __juniper_private1__.inet.0                    1/0/3

__juniper_private2__ forwarding
         __juniper_private2__.inet.0                    0/0/1

__juniper_private3__ forwarding
         __juniper_private3__.inet.0                    1/0/2

__juniper_private4__ forwarding
         __juniper_private4__.inet.0                    4/0/2

__master.anon__      forwarding

r1                 virtual-router

r2                 virtual-router
```

show route instance detail

```
user@switch> show route instance detail
master:
  Router ID: 10.3.3.7
  Type: forwarding        State: Active
  Tables:
    inet.0                : 5 routes (4 active, 0 holddown, 1 hidden)

__juniper_private1__:
  Router ID: 0.0.0.0
  Type: forwarding        State: Active
  Interfaces:
    lo0.16385
    bme0.0
  Tables:
    __juniper_private1__.inet.0: 6 routes (1 active, 0 holddown, 3 hidden)

__juniper_private2__:
  Router ID: 0.0.0.0
  Type: forwarding        State: Active
  Interfaces:
    lo0.16384
```

```
  Tables:
    __juniper_private2__.inet.0: 1 routes (0 active, 0 holddown, 1 hidden)

__juniper_private3__:
  Router ID: 0.0.0.0
  Type: forwarding        State: Active
  Interfaces:
    bme0.1
  Tables:
    __juniper_private3__.inet.0: 4 routes (1 active, 0 holddown, 2 hidden)

__juniper_private4__:
  Router ID: 0.0.0.0
  Type: forwarding        State: Active
  Interfaces:
    bme0.2
  Tables:
    __juniper_private4__.inet.0: 8 routes (4 active, 0 holddown, 2 hidden)

__master.anon__:
  Router ID: 0.0.0.0
  Type: forwarding        State: Active

r1:
  Router ID: 0.0.0.0
  Type: virtual-router    State: Active
  Interfaces:
    xe-0/0/0.0

r2:
  Router ID: 0.0.0.0
  Type: virtual-router    State: Active
  Interfaces:
    xe-0/0/3.0
```

show route instance operational

```
user@switch> show route instance operational
Operational Routing Instances:

__juniper_private1__
__juniper_private2__
__juniper_private3__
__juniper_private4__
r1---qfabric
r2---qfabric
master
```

show route instance summary

```
user@switch> show route instance summary
Instance             Type
         Primary RIB                                    Active/holddown/hidden
master               forwarding
         inet.0                                         4/0/1

__juniper_private1__ forwarding
         __juniper_private1__.inet.0                    1/0/3

__juniper_private2__ forwarding
         __juniper_private2__.inet.0                    0/0/1
```

```
__juniper_private3__ forwarding
         __juniper_private3__.inet.0                    1/0/2

__juniper_private4__ forwarding
         __juniper_private4__.inet.0                    4/0/2

__master.anon__      forwarding

r1                 virtual-router
r2                 virtual-router
```

show snmp statistics

Syntax
show snmp statistics
<subagents>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Option **subagents** introduced in Junos OS Release 14.2.

Description
Display statistics about Simple Network Management Protocol (SNMP) packets sent and received by the router or switch.

Options
subagents—(Optional) Display the statistics of the protocol data unit (PDU), the number of SNMP requests and responses per subagent, and the SNMP statistics received from each subagent per logical system.

Required Privilege Level
view

Related Documentation
- *clear snmp statistics*

List of Sample Output
show snmp statistics on page 280
show snmp statistics subagents on page 280

Output Fields
Table 43 on page 276 describes the output fields for the **show snmp statistics** command. Output fields are listed in the approximate order in which they appear.

Table 43: show snmp statistics Output Fields

Field Name	Field Description
Input	Information about received packets: • **Packets(snmpInPkts)**—Total number of messages delivered to the SNMP entity from the transport service. • **Bad versions—(snmpInBadVersions**) Total number of messages delivered to the SNMP entity that were for an unsupported SNMP version. • **Bad community names—(snmpInBadCommunityNames)** Total number of messages delivered to the SNMP entity that used an SNMP community name not known to the entity. • **Bad community uses—(snmpInBadCommunityUses)** Total number of messages delivered to the SNMP entity that represented an SNMP operation that was not allowed by the SNMP community named in the message. • **ASN parse errors—(snmpInASNParseErrs)** Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages. • **Too bigs—(snmpInTooBigs)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **tooBig**. • **No such names—(snmpInNoSuchNames)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **noSuchName**. • **Bad values—(snmpInBadValues)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **badValue**. • **Read onlys—(snmpInReadOnlys)** Total number of valid SNMP PDUs delivered to the SNMP entity with an error status field of **readOnly**. Only incorrect implementations of SNMP generate this error.

Table 43: show snmp statistics Output Fields *(continued)*

Field Name	Field Description
Input (continued)	• **General errors—(snmpInGenErrs)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **genErr**. • **Total requests varbinds—(snmpInTotalReqVars)** Total number of MIB objects retrieved successfully by the SNMP entity as a result of receiving valid SNMP **GetRequest** and **GetNext** PDUs. • **Total set varbinds—(snmpInSetVars)** Total number of MIB objects modified successfully by the SNMP entity as a result of receiving valid SNMP **SetRequest** PDUs. • **Get requests—(snmpInGetRequests)** Total number of SNMP **GetRequest** PDUs that have been accepted and processed by the SNMP entity. • **Get nexts—(snmpInGetNexts)** Total number of SNMP **GetNext** PDUs that have been accepted and processed by the SNMP entity. • **Set requests—(snmpInSetRequests)** Total number of SNMP **SetRequest** PDUs that have been accepted and processed by the SNMP entity. • **Get responses—(snmpInGetResponses)** Total number of SNMP **GetResponse** PDUs that have been accepted and processed by the SNMP entity. • **Traps—(snmpInTraps)** Total number of SNMP traps generated by the SNMP entity. • **Silent drops—(snmpSilentDrops)** Total number of **GetRequest**, **GetNextRequest**, **GetBulkRequest**, **SetRequests**, and **InformRequest** PDUs delivered to the SNMP entity that were silently dropped because the size of a reply containing an alternate response PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the requests. • **Proxy drops—(snmpProxyDrops)** Total number of **GetRequest**, **GetNextRequest**, **GetBulkRequest**, **SetRequests**, and **InformRequest** PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in such a way (other than a timeout) that no response PDU could be returned. • **Commit pending drops**—Number of SNMP packets for **Set** requests dropped because of a previous pending SNMP **Set** request on the committed configuration. • **Throttle drops**—Number of SNMP packets for any requests dropped reaching the throttle limit.

Table 43: show snmp statistics Output Fields *(continued)*

Field Name	Field Description
V3 Input	Information about SNMP version 3 packets: • **Unknown security models—(snmpUnknownSecurityModels)** Total number of packets received by the SNMP engine that were dropped because they referenced a security model that was not known to or supported by the SNMP engine. • **Invalid messages—(snmpInvalidMsgs)** Number of packets received by the SNMP engine that were dropped because there were invalid or inconsistent components in the SNMP message. • **Unknown pdu handlers—(snmpUnknownPDUHandlers)** Number of packets received by the SNMP engine that were dropped because the PDU contained in the packet could not be passed to an application responsible for handling the PDU type. • **Unavailable contexts—(snmpUnavailableContexts)** Number of requests received for a context that is known to the SNMP engine, but is currently unavailable. • **Unknown contexts—(snmpUnknownContexts)** Total number of requests received for a context that is unknown to the SNMP engine. • **Unsupported security levels—(usmStatsUnsupportedSecLevels)** Total number of packets received by the SNMP engine that were dropped because they requested a security level unknown to the SNMP engine (or otherwise unavailable). • **Not in time windows—(usmStatsNotInTimeWindows)** Total number of packets received by the SNMP engine that were dropped because they appeared outside the authoritative SNMP engine's window. • **Unknown user names—(usmStatsUnknownUserNames)** Total number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine. • **Unknown engine ids—(usmStatsUnknownEngineIDs)** Total number of packets received by the SNMP engine that were dropped because they referenced an SNMP engine ID that was not known to the SNMP engine. • **Wrong digests—(usmStatsWrongDigests)** Total number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value. • **Decryption errors—(usmStatsDecryptionErrors)** Total number of packets received by the SNMP engine that were dropped because they could not be decrypted.

Table 43: show snmp statistics Output Fields *(continued)*

Field Name	Field Description
Output	Information about transmitted packets: • **Packets—(snmpOutPkts)** Total number of messages passed from the SNMP entity to the transport service. • **Too bigs—(snmpOutTooBigs)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **tooBig**. • **No such names—(snmpOutNoSuchNames)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **noSuchName**. • **Bad values—(snmpOutBadValues)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **badValue**. • **General errors—(snmpOutGenErrs)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **genErr**. • **Get requests—(snmpOutGetRequests)** Total number of SNMP **GetRequest** PDUs generated by the SNMP entity. • **Get nexts—(snmpOutGetNexts)** Total number of SNMP **GetNext** PDUs generated by the SNMP entity. • **Set requests—(snmpOutSetRequests)** Total number of SNMP **SetRequest** PDUs generated by the SNMP entity. • **Get responses—(snmpOutGetResponses)** Total number of SNMP **GetResponse** PDUs generated by the SNMP entity. • **Traps—(snmpOutTraps)** Total number of SNMP traps generated by the SNMP entity.

Table 44 on page 279 describes the output fields for the **show snmp statistics subagents** command. Output fields are listed in the approximate order in which they appear.

Table 44: show snmp statistics subagents Output Fields

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

Sample Output

show snmp statistics

```
user@host> show snmp statistics
SNMP statistics:
  Input:
    Packets: 246213, Bad versions: 12, Bad community names: 12,
    Bad community uses: 0, ASN parse errors: 96,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 227084, Total set varbinds: 67,
    Get requests: 44942, Get nexts: 190371, Set requests: 10712,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0,
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 1
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 44, Wrong digests: 23, Decryption errors: 0
  Output:
    Packets: 246093, Too bigs: 0, No such names: 31561,
    Bad values: 0, General errors: 2,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 246025, Traps: 0
```

show snmp statistics subagents

```
user@host> show snmp statistics subagents

  Subagent: /var/run/cosd-20
    Request PDUs: 0, Response PDUs: 0,
    Request Variables: 0, Response Variables: 0,
    Average Response Time(ms): 0.00,
    Maximum Response Time(ms): 0.00

  Subagent: /var/run/pfed-30
    Request PDUs: 0, Response PDUs: 0,
    Request Variables: 0, Response Variables: 0,
    Average Response Time(ms): 0.00,
    Maximum Response Time(ms): 0.00

  Subagent: /var/run/rmopd-15
    Request PDUs: 0, Response PDUs: 0,
    Request Variables: 0, Response Variables: 0,
    Average Response Time(ms): 0.00,
    Maximum Response Time(ms): 0.00

  Subagent: /var/run/chassisd-30
    Request PDUs: 33116, Response PDUs: 33116,
    Request Variables: 33116, Response Variables: 33116,
    Average Response Time(ms): 1.83,
    Maximum Response Time(ms): 203.48

  Subagent: /var/run/pkid-13
    Request PDUs: 0, Response PDUs: 0,
    Request Variables: 0, Response Variables: 0,
    Average Response Time(ms): 0.00,
    Maximum Response Time(ms): 0.00
```

```
Subagent: /var/run/apsd-13
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/dfcd-32
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/mib2d-33
  Request PDUs: 74211, Response PDUs: 74211,
  Request Variables: 74211, Response Variables: 74211,
  Average Response Time(ms): 2.30,
  Maximum Response Time(ms): 51.04

Subagent: /var/run/license-check-16
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/craftd-14
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/bfdd-19
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/smihelperd-24
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/cfmd-18
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/rpd_snmp
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/l2tpd-18
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00
```

ssh

List of Syntax
Syntax on page 283
Syntax (EX Series Switch and the QFX Series) on page 283

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 284

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
% ...
```

PART 5

Index

Index

Symbols

A

B

C

M

N

O

P

R

S

T