Junos® OS for EX Series Ethernet Switches

Access and User Management on EX Series Switches

Release
12.3

Modified: 2012-08-06

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

Junos® OS for EX Series Ethernet Switches Access and User Management on EX Series Switches
Release 12.3

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:

- EX Series

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

   ```
   system {
     scripts {
       commit {
         file ex-script.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 the *CLI User Guide*.

Documentation Conventions

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

Table 1: Notice Icons

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

Table 2 on page xiii 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

Software Overview

Understanding Software Infrastructure and Processes

Each switch runs the Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches on its general-purpose processors. Junos OS includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the chassis.

The 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.

With the J-Web interface and the command-line interface (CLI) to the Junos OS, you configure switching features and routing protocols and set the properties of network interfaces on your switch. After activating a software configuration, use either the J-Web or CLI user interface to monitor the switch, 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 fabric for the switch, providing route lookup, filtering, and switching on incoming data packets, then directing 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

The 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.
Ethernet switching process	eswd	Handles Layer 2 switching functionality such as MAC address learning, Spanning Tree protocol and access port security. The process is also responsible for managing Ethernet switching interfaces, VLANs, and VLAN interfaces. Manages Ethernet switching interfaces, VLANs, and VLAN interfaces.
Forwarding process	pfem	Defines how routing protocols operate on the switch. The overall performance of the switch 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.
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 switch. 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.
Routing protocol process	rpd	Defines how routing protocols such as RIP, OSPF, and BGP operate on the device, including selecting routes and maintaining forwarding tables.

Related Documentation

- For more information about processes, see *Junos OS Network Operations Guide*
- For more information about basic system parameters, supported protocols, and software processes, see *Junos OS System Basics Configuration Guide*

PART 2

Configuration

CHAPTER 2

Configuration Tasks

Configuring Management Access for the EX Series Switch (J-Web Procedure)

You can manage an EX Series switch remotely through the J-Web interface. To communicate with the switch, the J-Web interface uses Hypertext Transfer Protocol (HTTP). HTTP allows easy Web access but no encryption. The data that is transmitted between the Web browser and the switch by means of HTTP is vulnerable to interception and attack. To enable secure Web access the switch supports HTTP over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports as needed.

Navigate to the Secure Access Configuration page by selecting **Configure** > **System Properties** > **Management Access**. On this page, you can enable HTTP and HTTPS access on interfaces for managing the EX Series switch through the J-Web interface. You can also install SSL certificates and enable Junos XML management protocol over SSL with the Secure Access page.

1. Click **Edit** to modify the configuration. Enter information into the Management Access Configuration page as described in Table 4 on page 10.
2. To verify that Web access is enabled correctly, connect to the switch using the appropriate method:
   - For HTTP access—In your Web browser, type **http://*URL*** or **http://*IP address***.
   - For HTTPS access—In your Web browser, type **https://*URL*** or **https://*IP address***.
   - For SSL Junos XML management protocol access—To use this option, you must have a Junos XML management protocol client such as Junos Scope. For information about how to log into Junos Scope, see the *Junos Scope Software User Guide*.

NOTE: After you make changes to the configuration in this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

Table 4: Secure Management Access Configuration Summary

Field	Function	Your Action
Management Access tab		
Management Port IP/Management Port IPv6	Specifies the management port IP address. The software supports both IPv4 (displayed as IP) and IPv6 address. NOTE: IPv6 is not supported on EX2200 and EX 4500 switches.	To specify an IPv4 address: 1. Select the check box **IPv4 address**. 2. Type an IP address—for example: **10.10.10.10**. 3. Enter the subnet mask or address prefix. For example, 24 bits represents **255.255.255.0**. 4. Click **OK**. To specify an IPv6 address: 1. Select the check box **IPv6 address**. 2. Type an IP address—for example:**2001:ab8:85a3::8a2e:370:7334**. 3. Enter the subnet mask or address prefix. 4. Click **OK**.
Default Gateway	Defines a default gateway through which to direct packets addressed to networks that are not explicitly listed in the bridge table constructed by the switch.	For IPv4 address type a 32-bit IP address, in dotted decimal notation. Type a 128-bit IP address for IPv6 address type.
Loopback address	Specifies the IP address of the loopback interface.	Type an IP address.
Subnet Mask	Specifies the subnet mask for the loopback interface.	Enter the subnet mask or address prefix.
Services tab		
Services	Specifies services to be enabled: telnet and SSH.	Select to enable the required services.
Enable Junos XML management protocol over Clear Text	Enables clear text access to the Junos XML management protocol XML scripting API.	To enable clear text access, select the **Enable Junos XML management protocol over Clear Text** check box.
Enable Junos XML protocol over SSL	Enables secure SSL access to the Junos XML management protocol XML scripting API.	To enable SSL access, select the **Enable Junos XML management protocol over SSL** check box.

Table 4: Secure Management Access Configuration Summary *(continued)*

Field	Function	Your Action
Junos XML management protocol Certificate	Specifies SSL certificates to be used for encryption. This field is available only after you create at least one SSL certificate.	To enable an SSL certificate, select a certificate from the Junos XML management protocol SSL Certificate list—for example, **new**.
Enable HTTP	Enables HTTP access on interfaces.	To enable HTTP access, select the **Enable HTTP access** check box. Select and clear interfaces by clicking the direction arrows: • To enable HTTP access on an interface, add the interface to the HTTP Interfaces list. You can either select all interfaces or specific interfaces.
Enable HTTPS	Enables HTTPS access on interfaces.	To enable HTTPS access, select the **Enable HTTPS access** check box. Select and deselect interfaces by clicking the direction arrows: • To enable HTTPS access on an interface, add the interface to the HTTPS Interfaces list. You can either select all interfaces or specific interfaces. NOTE: Specify the certificate to be used for HTTPS access.
Certificates tab		
Certificates	Displays digital certificates required for SSL access to the switch. Allows you to add and delete SSL certificates.	To add a certificate: 1. Have a general SSL certificate available. See Generating SSL Certificates for more information. 2. Click **Add**. The Add a Local Certificate page opens. 3. Type a name in the Certificate Name box—for example, **new**. 4. Open the certificate file and copy its contents. 5. Paste the generated certificate and RSA private key in the Certificate box. To edit a certificate, select it and click **Edit**. To delete a certificate, select it and click **Delete**.

Related Documentation

- *Security Features for EX Series Switches Overview*

- *Understanding J-Web User Interface Sessions*
- *Enabling HTTPS Service on Switches Using Self-Signed Certificates (CLI Procedure)*

Generating SSL Certificates to Be Used for Secure Web Access

You can set up secure Web access for an EX Series switch. To enable secure Web access, you must generate a digital Secure Sockets Layer (SSL) certificate and then enable HTTPS access on the switch.

To generate an SSL certificate:

1. Enter the following **openssl** command in your SSH command-line interface on a BSD or Linux system on which **openssl** is installed. The **openssl** command generates a self-signed SSL certificate in the privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.

   % openssl req –x509 –nodes –newkey rsa:1024 –keyout *filename*.pem -out *filename*.pem

   where ***filename*** is the name of a file in which you want the SSL certificate to be written—for example, **my-certificate**.

2. When prompted, type the appropriate information in the identification form. For example, type **US** for the country name.

3. Display the contents of the file that you created.

   cat my-certificate.pem

You can use the J-Web Configuration page to install the SSL certificate on the switch. To do this, copy the file containing the certificate from the BSD or Linux system to the switch. Then open the file, copy its contents, and paste them into the Certificate box on the J-Web Secure Access Configuration page.

You can also use the following CLI statement to install the SSL certificate on the switch:

```
[edit]
user@switch# set security certificates local my-signed-cert load-key-file my-certificate.pem
```

Related Documentation

- Configuring Management Access for the EX Series Switch (J-Web Procedure) on page 9
- *Security Features for EX Series Switches Overview*

Configuring MS-CHAPv2 to Provide Password-Change Support (CLI Procedure)

Junos OS for EX Series switches enables you to configure the Microsoft Corporation implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the switch to provide password-change support. Configuring MS-CHAPv2 on the switch provides users accessing a switch the option of changing the password when the password expires, is reset, or is configured to be changed at next login.

See RFC 2433 at , Microsoft PPP CHAP Extensions, for information about MS-CHAP.

Before you configure MS-CHAPv2 to provide password-change support, ensure that you have:

- Configured RADIUS server authentication. Configure users on the authentication server and set the first-tried option in the authentication order to radius. See *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*.

To configure MS-CHAPv2, specify the following:

```
[edit system radius-options]
user@switch# set password-protocol mschap-v2
```

You must have the required access permission on the switch in order to change your password.

Related Documentation

- Managing Users (J-Web Procedure) on page 65
- For more about configuring user access, see the *Junos OS Access Privilege Configuration Guide*.

CHAPTER 3

Configuration Statements

[edit services] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the **[edit services]** hierarchy level on EX Series switches.

- *Supported* statements are those that you can use to configure some aspect of a software feature on the switch.
- *Unsupported* statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switches, see *EX Series Switch Software Features Overview*.

Supported Statements in the [edit services] Hierarchy Level

The following hierarchy shows the **[edit services]** configuration statements supported on EX Series switches:

```
services {
  captive-portal {
    authentication-profile-name authentication-profile-name;
    custom-options {
      banner-message string;
      footer-bgcolor color;
      footer-message string;
      footer-text-color color;
      form-header-bgcolor color;
      form-header-message string;
      footer-header-text-color color;
      form-reset-label label-name;
      form-submit-label label-name;
      header-bgcolor color;
      header-logo filename;
      header-message string;
      header-text-color color0;
      post-authentication-url url;
    }
    interface (all | interface-name) {
      quiet-period seconds;
      retries number-of-retries;
      server-timeout seconds;
      session-expiry seconds;
      supplicant (multiple | single | single-secure);
    }
    secure-authentication (http | https);
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <disable>;
    }
  }
  rpm {
    bgp {
      data-fill data;
      data-size size;
      destination-port port;
      history-size size;
      moving-average-size number-of-samples;
      probe-count count;
      probe-interval seconds;
      probe-type type;
      routing-instances {
        routing-instance-name;
      }
      test-interval seconds;
    }
    probe owner {
      test test-name {
```

```
            data-fill data;
            data-size size;
            destination-port port;
            dscp-code-point dscp-bits;
            hardware-timestamp;
            history-size size;
            moving-average-size number;
            one-way-hardware-timestamp;
            probe-count count;
            probe-interval seconds;
            probe-type type;
            routing-instance instance-name;
            source-address address;
            target (address address | url url);
            test-interval interval;
            thresholds {
              egress-time microseconds;
              ingress-time microseconds;
              jitter-egress microseconds;
              jitter-ingress microseconds;
              jitter-rtt microseconds;
              rtt microseconds;
              std-dev-egress microseconds;
              std-dev-ingress microseconds;
              std-dev-rtt microseconds;
              successive-loss count;
              total-loss count;
            }
            traps [ trap-names ];
          }
        }
        probe-limit number;
        probe-server {
          tcp {
            port port-number;
          }
          udp {
            port port-number;
          }
        }
      }
      unified-access-control {
        certificate-verification (optional | required | warning);
        infranet-controllerhostname {
          address ip-address;
          interface interface-name;
          password password;
          port port-number;
        }
        interval seconds;
        timeout seconds;
        timeout-action (close | no-change);
        traceoptions {
          file filename <files number> <size maximum-file-size> <world-readable |
            no-world-readable>;
          flag flag <disable>;
```

```
        }
    }
}
```

Unsupported Statements in the [edit services] Hierarchy Level

All statements in the **[edit services]** hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

Table 5: Unsupported [edit services] Configuration Statements on EX Series Switches

Statement	Hierarchy
NOTE: Variables, such as *interface-name*, are not shown in the statements or hierarchies.	
ca-profile	**[edit services unified-access-control infranet-controller]**
interface	**[edit services interface-pools]** **[edit services service-device-pools pool]**
pool	**[edit services interface-pools]** **[edit services service-device-pools]**
server-certificate-subject	**[edit services unified-access-control infranet-controller]**
service-device-pools	**[edit services]**
service-interface-pools	**[edit services]**

Related Documentation

- *Junos OS Configuration Statements and Commands*

allow-commands

Syntax allow-commands "*regular-expression*";

Hierarchy Level [edit system login class *class-name*]

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

Description Specify the operational mode commands that members of a login class can use.

Default If you omit this statement and the **deny-commands** statement, users can issue only those commands for which they have access privileges through the **permissions** statement.

Options ***regular-expression***—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

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

Related Documentation

- *Specifying Access Privileges for Junos OS Operational Mode Commands*
- deny-commands on page 28
- user on page 62

allow-configuration

Syntax allow-configuration "*regular-expression*";

Hierarchy Level [edit system login class *class-name*]

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

Description Explicitly allow configuration access to the specified levels in the hierarchy even if the permissions set with the **permissions** statement do not grant such access by default.

Default If you omit this statement and the **deny-configuration** statement, users can edit only those commands for which they have access privileges through the **permissions** statement.

Options ***regular-expression***—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

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

Related Documentation

- *Specifying Access Privileges Using allow/deny-configuration Statements*
- *Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies*
- deny-configuration on page 29
- user on page 62

announcement

Syntax announcement *text*;

Hierarchy Level [edit system login]

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

Description Configure a system login announcement. This announcement appears after a user logs in.

Options ***text***—Text of the announcement. If the text contains any spaces, enclose it in quotation marks.

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

Related Documentation
- *Configuring the Junos OS to Display a System Login Announcement*
- message on page 43

archive-sites

Syntax
```
archive-sites {
  site-name;
}
```

Hierarchy Level [edit accounting-options file *filename*]

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

Description Configure an archive site. If more than one site name is configured, an ordered list of archive sites for the accounting-data log files is created. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with a filename of the format ***router-name_log-filename_timestamp***.

Options ***site-name***—Any valid FTP URL to a destination. For information about specifying valid FTP URLs, see the *Junos System Basics Configuration Guide*.

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

Related Documentation
- *Configuring Archive Sites*

authentication (Login)

Syntax

```
authentication {
  (encrypted-password "password" | plain-text-password);
  load-key-file URL filename;
  ssh-dsa "public-key";
  ssh-ecdsa "public-key";
  ssh-rsa "public-key";
}
```

Hierarchy Level [edit system login user *username*]

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

Description Authentication methods that a user can use to log in to the router or switch. You can assign multiple authentication methods to a single user.

Options

encrypted-password "*password*"—Message Digest 5 (MD5) or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.

You cannot configure a blank password for **encrypted-password** using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

load-key-file *URL filename*—Load previously-generated RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys from a named file at a specified URL location. The file contains one or more SSH keys.

plain-text-password—When using this option, the command-line interface (CLI) prompts you for the password and then encrypts it.

ssh-dsa "*public-key*"—SSH version 2 authentication. Specify the DSA public key. You can specify one or more public keys for each user.

ssh-ecdsa "*public-key*"—SSH version 2 authentication. Specify the ECDSA public key. You can specify one or more public keys for each user.

ssh-rsa "*public-key*"—SSH version 1 and SSH version 2 authentication. Specify the RSA public key. You can specify one or more public keys for each user.

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

Related Documentation

- *Configuring Junos OS User Accounts*
- root-authentication on page 52

authentication-order

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

Hierarchy Level [edit system]

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

Description Configure the order in which the software tries different user authentication methods when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches.

Default If you do not include the **authentication-order** statement, users are verified based on their configured passwords.

Options ***authentication-methods***—One or more authentication methods, listed in the order in which they should be tried. The method can be one or more of the following:

- **password**—Use the password configured for the user with the **authentication** statement at the **[edit system login user]** hierarchy level.
- **radius**—Use RADIUS authentication services.
- **tacplus**—Use TACACS+ authentication services.

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

Related Documentation

- *Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication*
- authentication on page 23

change-type

Syntax change-type (character-sets | set-transitions);

Hierarchy Level [edit system login password]

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

Description Set requirements for using character sets in plain-text passwords. When you combine this statement with the **minimum-changes** statement, you can check for the total number of character sets included in the password or for the total number of character-set changes in the password. Newly created passwords must meet these requirements.

Options Specify one of the following:

- **character-sets**—The number of character sets in the password. Valid character sets include uppercase letters, lowercase letters, numbers, punctuation, and other special characters.
- **set-transitions**—The number of transitions between character sets.

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

Related Documentation
- *Special Requirements for Junos OS Plain-Text Passwords*
- minimum-changes on page 45

class (Assigning a Class to an Individual User)

Syntax class *class-name*;

Hierarchy Level [edit system login user *username*]

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

Description Configure a user's login class. You must configure one class for each user.

Options ***class-name***—One of the classes defined at the **[edit system login class]** hierarchy level.

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

Related Documentation
- *Configuring Junos OS User Accounts*

class (Defining Login Classes)

Syntax

```
class class-name {
  allow-commands "regular-expression";
  ( allow-configuration | allow-configuration-regexps) “regular expression 1” “regular
    expression 2”;
  configuration-breadcrumbs;
  deny-commands "regular-expression";
  ( deny-configuration | deny-configuration-regexps ) “regular expression 1” “regular expression
    2 ”;
  idle-timeout minutes;
  login-script filename;
  login-tip;
  permissions [ permissions ];
}
```

Hierarchy Level [edit system login]

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

Description Define a login class.

Options ***class-name***—A name you choose for the login class.

The remaining statements are explained separately.

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

Related Documentation

- *Defining Junos OS Login Classes*
- user on page 62

class-usage-profile

Syntax

```
class-usage-profile profile-name {
  file filename;
  interval minutes;
  source-classes {
    source-class-name;
  }
  destination-classes {
    destination-class-name;
  }
}
```

Hierarchy Level [edit accounting-options]

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

Description Create a class usage profile, which is used to log class usage statistics to a file in the **/var/log** directory. The class usage profile logs class usage statistics for the configured source classes on every interface that has **destination-class-usage** configured.

For information about configuring source classes, see the *Junos Routing Protocols Configuration Guide*. For information about configuring source class usage, see the *Junos Network Management Configuration Guide*.

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

The remaining statements are explained separately.

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

Related Documentation

- *Configuring Class Usage Profiles*

counters

Syntax

```
counters {
  counter-name;
}
```

Hierarchy Level [edit accounting-options filter-profile *profile-name*]

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

Description Names of counters for which filter profile statistics are collected. The packet and byte counts for the counters are logged to a file in the **/var/log** directory.

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

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

Related Documentation

- *Configuring the Counters*

deny-commands

Syntax deny-commands "*regular-expression*";

Hierarchy Level [edit system login class]

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

Description Specify the operational mode commands that the user is denied permission to issue even though the permissions set with the **permissions** statement would allow it.

Default If you omit this statement and the **allow-commands** statement, users can issue only those commands for which they have access privileges through the **permissions** statement.

Options ***regular-expression***—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

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

Related Documentation

- *Specifying Access Privileges for Junos OS Operational Mode Commands*
- allow-commands on page 20
- user on page 62

deny-configuration

Syntax deny-configuration "*regular-expression*";

Hierarchy Level [edit system login class]

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

Description Explicitly deny configuration access to the specified levels in the hierarchy even if the permissions set with the **permissions** statement grant such access by default.

Default If you omit this statement and the **allow-configuration** statement, users can edit those levels in the configuration hierarchy for which they have access privileges through the **permissions** statement.

Options ***regular-expression***—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

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

Related Documentation

- *Specifying Access Privileges Using allow/deny-configuration Statements*
- allow-configuration on page 21
- user on page 62

destination-classes

Syntax

```
destination-classes {
  destination-class-name;
}
```

Hierarchy Level [edit accounting-options class-usage-profile *profile-name*]

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

Description Specify the destination classes for which statistics are collected.

Options ***destination-class-name***—Name of the destination class to include in the source class usage profile.

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

Related Documentation

- *Configuring a Class Usage Profile*

fields (for Interface Profiles)

Syntax

```
fields {
  field-name;
}
```

Hierarchy Level [edit accounting-options interface-profile *profile-name*]

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

Description Statistics to collect in an accounting-data log file for an interface.

Options ***field-name***—Name of the field:

- **input-bytes**—Input bytes
- **input-errors**—Generic input error packets
- **input-multicast**—Input packets arriving by multicast
- **input-packets**—Input packets
- **input-unicast**—Input unicast packets
- **output-bytes**—Output bytes
- **output-errors**—Generic output error packets
- **output-multicast**—Output packets sent by multicast
- **output-packets**—Output packets
- **output-unicast**—Output unicast packets

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

Related Documentation

- *Configuring the Interface Profile*

file (Associating with a Profile)

Syntax file *filename*;

Hierarchy Level [edit accounting-options class-usage-profile *profile-name*],
[edit accounting-options filter-profile *profile-name*],
[edit accounting-options interface-profile *profile-name*],
[edit accounting-options mib-profile *profile-name*],
[edit accounting-options routing-engine-profile *profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
The **[edit accounting-options mib-profile *profile-name*]** hierarchy added in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series Switches.

Description Specify the accounting log file associated with the profile.

Options ***filename***—Name of the log file. You must specify a filename already configured in the **file** statement at the **[edit accounting-options]** hierarchy level.

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

Related Documentation

- *Configuring the Interface Profile*
- *Configuring the Filter Profile*
- *Configuring the MIB Profile*
- *Configuring the Routing Engine Profile*

file (Configuring a Log File)

Syntax

```
file filename {
  archive-sites {
    site-name;
  }
  files number;
  nonpersistent;
  size bytes;
  source-classes time;
  transfer-interval minutes;
}
```

Hierarchy Level [edit accounting-options]

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

Description Specify a log file to be used for accounting data.

Options ***filename***—Name of the file in which to write accounting data.

The remaining statements are explained separately.

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

Related Documentation

- *Configuring Accounting-Data Log Files*

files

Syntax files *number*;

Hierarchy Level [edit accounting-options file *filename*]

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

Description Specify the maximum number of log files to be used for accounting data.

Options ***number***—The maximum number of files. When a log file (for example, **profilelog**) reaches its maximum size, it is renamed **profilelog.0**, then **profilelog.1**, and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. The minimum value for ***number*** is 3 and the default value is 10.

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

Related Documentation

- *Configuring Accounting-Data Log Files*

filter-profile

Syntax

```
filter-profile profile-name {
  counters {
    counter-name;
  }
  file filename;
  interval minutes;
}
```

Hierarchy Level [edit accounting-options]

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

Description Create a profile to filter and collect packet and byte count statistics and write them to a file in the **/var/log** directory. To apply the profile to a firewall filter, you include the **accounting-profile** statement at the **[edit firewall filter *filter-name*]** hierarchy level. For more information about firewall filters, see the *Junos Network Management Configuration Guide*.

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

The remaining statements are explained separately.

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

Related Documentation

- *Configuring the Filter Profile*

format

Syntax format (md5 | sha1);

Hierarchy Level [edit system login password]

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

Description Configure the authentication algorithm for plain-text passwords.

Default For Junos OS, the default encryption format is **md5**. For Junos-FIPS software, the default encryption format is **sha1**.

Options The hash algorithm that authenticates the password can be one of these algorithms:

- **md5**—Produces a 128-bit digest.
- **sha1**—Produces a 160-bit digest.

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

Related Documentation
- *Special Requirements for Junos OS Plain-Text Passwords*

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.

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*
- user on page 62
- *user*

idle-timeout (System-Login)

Syntax idle-timeout *minutes*;

Hierarchy Level [edit system login class *class-name*]

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

Description For a login class, configure the maximum time that a session can be idle before the user is logged out of the router or switch. The session times out after remaining at the CLI operational mode prompt for the specified time.

Default If you omit this statement, a user is never forced off the system after extended idle times.

Options ***minutes***—Maximum idle time.

Range: 0 through 4294967295 minutes

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

Related Documentation

- *Configuring the Timeout Value for Idle Login Sessions*
- user on page 62

interface-profile

Syntax

```
interface-profile profile-name {
  fields {
    field-name;
  }
  file filename;
  interval minutes;
}
```

Hierarchy Level [edit accounting-options]

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

Description Create a profile to filter and collect error and packet statistics and write them to a file in the **/var/log** directory. You can specify an interface profile for either a physical or a logical interface.

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

The remaining statements are explained separately.

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

Related Documentation

- *Configuring the Interface Profile*

interval (Accounting Options)

Syntax interval *minutes*;

Hierarchy Level [edit accounting-options class-usage-profile *profile-name*],
[edit accounting-options filter-profile *profile-name*],
[edit accounting-options interface-profile *profile-name*],
[edit accounting-options mib-profile *profile-name*],
[edit accounting-options routing-engine-profile *profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
The **[edit accounting-options mib-profile *profile-name*]** hierarchy level added in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify how often statistics are collected for the accounting profile.

Options ***minutes***—Length of time between each collection of statistics.

Range: 1 through 2880 minutes

Default: 30 minutes

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

Related Documentation

- *Configuring the Interface Profile*
- *Configuring the Filter Profile*
- *Configuring the MIB Profile*
- *Configuring the Routing Engine Profile*

login

Syntax

```
login {
  announcement text;
  class class-name {
    allow-commands "regular-expression";
    allow-configuration-regexps "regular expression 1" "regular expression 2";
    configuration-breadcrumbs;
    deny-commands "regular-expression";
    ( deny-configuration | deny-configuration-regexps ) “regular expression 1” “regular
      expression 2 ”;
    idle-timeout minutes;
    login-script filename;
    login-tip;
    permissions [ permissions ];
  }
  message text;
  password {
    change-type (set-transitions | character-set);
    format (md5 | sha1 | des);
    maximum-length length;
    minimum-changes number;
    minimum-length length;
  }
  retry-options {
    backoff-threshold number;
    backoff-factor seconds;
    minimum-time seconds;
    tries-before-disconnect number;
  }
  user username {
    full-name complete-name;
    uid uid-value;
    class class-name;
    authentication authentication;
    (encrypted-password "password" | plain-text-password);
    ssh-rsa "public-key";
    ssh-dsa "public-key";
  }
}
```

Hierarchy Level [edit system]

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

Description Configure user access to the router or switch.

NOTE: 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
- *Defining Junos OS Login Classes*

login-alarms

Syntax
login-alarms;

Hierarchy Level
[edit system login class *class-name*]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Show system alarms automatically when an **admin** user logs in to the router or switch.

Options
class-name—Login class name.

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

Related Documentation
- *Configuring System Alarms to Appear Automatically Upon Login*

login-tip

Syntax
login-tip;

Hierarchy Level
[edit system login class *class-name*]

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

Description
Enable CLI tips at login.

Default
Disabled.

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

Related Documentation
- *Configuring CLI Tips*

maximum-length

Syntax maximum-length *length*;

Hierarchy Level [edit system login passwords]

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

Description Specify the maximum number of characters allowed in plain-text passwords. Newly created passwords must meet this requirement.

Default For Junos-FIPS software, the maximum number of characters for plain-text passwords is 20. For Junos OS, no maximum is set.

Options **length**—The maximum number of characters the password can include.

Range: 1 to 64 characters

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

Related Documentation

- *Special Requirements for Junos OS Plain-Text Passwords*
- *Example: Changing the Requirements for Junos OS Plain-Text Passwords*
- password (Login) on page 48

message

Syntax message *text*;

Hierarchy Level [edit system login]

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

Description Configure a system login message. This message appears before a user logs in.

You can format the message using the following special characters:

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

Options ***text***—Text of the message.

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

Related Documentation

- *Configuring the Junos OS to Display a System Login Message*
- announcement on page 22

mib-profile

Syntax

```
mib-profile profile-name {
  file filename;
  interval minutes;
  object-names {
    mib-object-name;
  }
  operation operation-name;
}
```

Hierarchy Level [edit accounting-options]

Release Information Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Create a MIB profile to collect selected MIB statistics and write them to a file in the **/var/log** directory.

NOTE: Do not configure MIB objects related to interface octets or packets for a MIB profile, because it can cause the SNMP walk or a CLI show command to time out.

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

The remaining statements are explained separately.

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

Related Documentation

- *Configuring the MIB Profile*

minimum-changes

Syntax minimum-changes *number*;

Hierarchy Level [edit system login passwords]

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

Description Specify the minimum number of character sets (or character set changes) required in plain-text passwords. Newly created passwords must meet this requirement.

This statement is used in combination with the **change-type** statement. If the change-type is **character-sets**, then the number of character sets included in the password is checked against the specified minimum. If change-type is **set-transitions**, then the number of character set changes in the password is checked against the specified minimum.

Default For Junos OS, the minimum number of changes is 1. For Junos-FIPS Software, the minimum number of changes is 3.

Options ***number***—The minimum number of character sets (or character set changes) required for the password.

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

Related Documentation

- *Special Requirements for Junos OS Plain-Text Passwords*
- change-type on page 25

minimum-length

Syntax minimum-length *length*;

Hierarchy Level [edit system login passwords]

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

Description Specify the minimum number of characters required in plain-text passwords. Newly created passwords must meet this requirement.

This statement can be used in combination with all of the other requirement options for plain-text passwords, such as **minimum-upper-cases**, **minimum-punctuations**, **minimum-lower-cases,** and so on.

Using several password minimum requirement options will cause the **minimum-length** to be reset if the total sum of the required minimums exceeds the **minimum-length** setting.

Default For Junos OS, the minimum number of characters for plain-text passwords is six. For Junos-FIPS software, the minimum number of characters for plain-text passwords is 10.

Options **length**—The minimum number of characters the password must include.

Range: 6 to 20 characters

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

Related Documentation

- *Special Requirements for Junos OS Plain-Text Passwords*
- *Example: Changing the Requirements for Junos OS Plain-Text Passwords*
- maximum-length on page 42

object-names

Syntax

```
object-names {
  mib-object-name;
}
```

Hierarchy Level [edit accounting-options mib-profile *profile-name*]

Release Information Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the name of each MIB object for which MIB statistics are collected for an accounting-data log file.

Options ***mib-object-name***—Name of a MIB object. You can specify more than one MIB object name.

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

Related Documentation

- *Configuring the MIB Profile*

operation

Syntax operation *operation-name*;

Hierarchy Level [edit accounting-options mib-profile *profile-name*]

Release Information Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the name of the operation used to collect MIB statistics for an accounting-data log file.

Options ***operation-name***—Name of the operation to use. You can specify a **get**, **get-next**, or **walk** operation.

Default: walk

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

Related Documentation

- *Configuring the MIB Profile*

password (Login)

Syntax

```
password {
  change-type (set-transitions | character-set);
  format (md5 | sha1);
  maximum-length length;
  minimum-changes number;
  minimum-length length;
  minimum-lower-cases number;
  minimum-numerics number;
  minimum-punctuations number;
  minimum-upper-cases number;
}
```

Hierarchy Level [edit system login]

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

Description Configure special requirements such as character length and encryption format for plain-text passwords. Newly created passwords must meet these requirements.

Using several password minimum requirement options will cause the **minimum-length** to be reset if the total sum of the required minimums exceeds the **minimum-length** setting.

The individual statements are explained separately.

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

Related Documentation

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

permissions

Syntax permissions [*permissions*];

Hierarchy Level [edit system login class]

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

Description Configure the login access privileges to be provided on the router or switch.

Options ***permissions***—Privilege type. For a list of permission flag types, see *Understanding Junos OS Access Privilege Levels*.

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

Related Documentation

- *Configuring Access Privilege Levels*
- user on page 62

radius-options (edit system)

Syntax

```
radius-options {
  attributes {
    nas-ip-address ip-address;
  }
  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.

NOTE: The **radius-options** statement is not available on QFabric systems.

Description Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.

Options

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 RADIUS Authentication*
- *Configuring RADIUS Authentication*

retry-options

Syntax

```
retry-options {
    backoff-factor seconds;
    backoff-threshold number;
    maximum-time seconds;
    minimum-time seconds;
    tries-before-disconnect number;
}
```

Hierarchy Level [edit system login]

Release Information

Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
maximum-time option introduced in Junos OS Release 9.6.
maximum-time option introduced in Junos OS Release 9.6 for EX Series switches.

Description Maximum number of times a user can attempt to enter a password while logging in through SSH or Telnet before being disconnected.

Required Privilege Level

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

Related Documentation

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

root-authentication

Syntax

```
root-authentication {
  (encrypted-password "password" | plain-text-password);
  ssh-dsa "public-key";
  ssh-ecdsa "public-key";
  ssh-rsa "public-key";
}
```

Hierarchy Level [edit system]

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

Description Configure the authentication methods for the root-level user, whose username is **root**.

Options

encrypted-password "*password*"— MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password.

You cannot configure a blank password for **encrypted-password** using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

plain-text-password—Plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password.

ssh-dsa "*public-key*"—SSH version 2 authentication. Specify the DSA (SSH version 2) public key. You can specify one or more public keys.

ssh-rsa "*public-key*"—SSH version 1 authentication. Specify the RSA (SSH version 1 and SSH version 2) public key. You can specify one or more public keys.

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

Related Documentation

- *Configuring the Root Password*
- authentication on page 23

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.

Description Control user access through SSH.

Default Allow user access through SSH.

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*

routing-engine-profile

Syntax

```
routing-engine-profile profile-name {
  fields {
    field-name;
  }
  file filename;
  interval minutes;
}
```

Hierarchy Level [edit accounting-options]

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

Description Create a Routing Engine profile to collect selected Routing Engine statistics and write them to a file in the **/var/log** directory.

Options ***profile-name***—Name of the Routing Engine statistics profile.

The remaining statements are explained separately.

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

Related Documentation

- *Configuring the Routing Engine Profile*

size

Syntax size *bytes*;

Hierarchy Level [edit accounting-options file *filename*]

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

Description Specify attributes of an accounting-data log file.

Options ***bytes***—Maximum size of each log file, in bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). When a log file (for example, **profilelog**) reaches its maximum size, it is renamed **profilelog.0**, then **profilelog.1**, and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. If you do not specify a size, the file is closed, archived, and renamed when the time specified for the transfer interval is exceeded.

Syntax: ***x*** to specify bytes, ***x***k to specify KB, ***x***m to specify MB, ***x***g to specify GB

Range: 256 KB through 1 GB

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

Related Documentation
- *Configuring the Maximum Size of the File*

source-classes

Syntax
```
source-classes {
  source-class-name;
}
```

Hierarchy Level [edit accounting-options class-usage-profile *profile-name*]

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

Description Specify the source classes for which statistics are collected.

Options ***source-class-name***—Name of the source class to include in the class usage profile.

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

Related Documentation
- *Configuring a Class Usage Profile*

start-time (Log File Transfer)

Syntax start-time *time*;

Hierarchy Level [edit accounting-options file *filename*]

Release Information Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the start time for transfer of an accounting-data log file.

Options ***time***—Start time for file transfer.

Syntax: *YYYY-MM-DD.hh:mm*

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

Related Documentation

- *Configuring the Start Time for File Transfer*

tacplus-options

Syntax

```
tacplus-options {
  (exclude-cmd-attribute | no-cmd-attribute-value);
  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.
Options for **no-cmd-attribute-value** and **exclude-cmd-attribute** introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 11.1 for QFX Series.
Option for **timestamp-and-timezone** introduced in Junos OS Release 12.2.

Description Configure TACACS+ options for authentication and accounting.

Options

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*
- *Configuring TACACS+ Authentication*
- *Configuring TACACS+ System Accounting*

tacplus-server

Syntax

```
tacplus-server server-address {
    secret password;
    single-connection;
    source-address source-address;
    timeout seconds;
}
```

Hierarchy Level [edit system]

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

Description Configure the TACACS+ server.

Options ***server-address***—Address of the TACACS+ authentication server.

The remaining statements are explained separately.

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

Related Documentation

- *Configuring TACACS+ Authentication*

traceoptions (Address-Assignment Pool)

Syntax

```
traceoptions {
  file filename {
    files number;
    size maximum-file-size;
    match regex;
    (world-readable | no-world-readable);
  }
  flag address-assignment;
  flag all;
  flag configuration;
  flag framework;
  flag ldap;
  flag local-authentication;
  flag radius;
}
```

Hierarchy Level [edit system processes general-authentication-service]

Release Information Flag for tracing address-assignment pool operations introduced in Junos OS Release 9.0.
option-name option introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure tracing options.

Options

file *filename*—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **address-assignment**—All address-assignment events
- **all**—All tracing operations
- **configuration**—Configuration events
- **framework**—Authentication framework events
- **ldap**—LDAP authentication events
- **local-authentication**—Local authentication events

- **radius**—RADIUS authentication events

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

no-world-readable—(Optional) Restrict access to the originator of the trace operation only.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and filename.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

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

Related Documentation
- *Configuring Address-Assignment Pools*

transfer-interval

Syntax
transfer-interval *minutes*;

Hierarchy Level
[edit accounting-options file *filename*]

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

Description
Specify the length of time the file remains open and receives new statistics before it is closed and transferred to an archive site.

Options
minutes—Time the file remains open and receives new statistics before it is closed and transferred to an archive site.

Range: 5 through 2880 minutes

Default: 30 minutes

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

Related Documentation
- *Configuring the Transfer Interval of the File*

uid

Syntax uid *uid-value*;

Hierarchy Level [edit system login user]

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

Description Numeric identifier associated with the user account name, either assigned by an administrator or assigned automatically when you commit the user configuration. It is used by applications that request numeric identifiers, such as some RADIUS queries or secure applications such as flow-tap monitoring.

Options ***uid-value***—Number associated with the login account. This value must be unique on the router or switch.

Range: 100 through 64000

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

Related Documentation

- *Configuring Junos OS User Accounts*

user (Access)

Syntax

```
user username {
  authentication {
  class class-name;
  (encrypted-password "password" | plain-text-password);
  full-name complete-name;
  load-key-file URL filename;
  ssh-dsa “public-key” <from hostname>;
  ssh-rsa “public-key” <from hostname>;
  uid uid-value;
  }
}
```

Hierarchy Level [edit system login]

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

Description Configure access permission for individual users.

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*
- class on page 25

PART 3

Administration

CHAPTER 4

Routine Monitoring

Managing Users (J-Web Procedure)

You can use the Users Configuration page for user information to add new users to an EX Series switch. For each account, you define a login name and password for the user and specify a login class for access privileges.

To configure users:

1. Select **Configure** > **System Properties** > **User Management**.

   The User Management page displays details of users, the authentication order, the RADIUS servers and TACACS servers present.

2. Click **Edit**.

3. Click any of the following options on the **Users** tab:

   - **Add**—Select this option to add a user. Enter details as described in Table 6 on page 66.
   - **Edit**—Select this option to edit an existing user's details. Enter details as described in Table 6 on page 66.
   - **Delete**—Select this option to delete a user.

4. Click an option on the **Authentication Methods and Order** tab:

   - Authentication Order—Drag and drop the authentication type from the Available Methods section to the Selected Methods. Click the up or down buttons to modify the authentication order.
   - RADIUS server—Click one:
     - **Add**—Select this option to add an authentication server. Enter details as described in Table 7 on page 67.
     - **Edit**—Select this option to modify the authentication server details. Enter details as described in Table 7 on page 67.
     - **Delete**—Select this option to delete an authentication server from the list.
   - TACACS server—Click one:

- **Add**—Select this option to add an authentication server. Enter details as described in Table 7 on page 67.
- **Edit**—Select this option to modify the authentication server details. Enter details as described in Table 7 on page 67.
- **Delete**—Select this option to delete an authentication server from the list.

NOTE: After you make changes to the configuration in this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

Table 6: User Management Configuration Page Summary

Field	Function	Your Action
User Information		
Username (required)	Specifies the name that identifies the user.	Type the username. It must be unique within the switching platform. Do not include spaces, colons, or commas in the username.
User Id	Specifies the user identification.	Type the user's ID.
Full Name	Specifies the user's full name.	Type the user's full name. If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.
Login Class (required)	Defines the user's access privilege.	Select the user's login class from the list: • **operator** • **read-only** • **super-user/superuser** • **unauthorized** This list also includes any user-defined login classes.
Password	Specifies the login password for this user.	Type the login password for this user. The login password must meet these criteria: • The password must be at least 6 characters long. • It can include alphabetic, numeric, and special characters, but not control characters. • It must contain at least one change of case or character class.
Confirm Password	Verifies the login password for this user.	Retype the login password for this user.

Table 7: Add an Authentication Server

Field	Function	Your Action
IP Address	Specifies the IP address of the server.	Type the server's 32-bit IP address, in dotted decimal notation.
Password	Specifies the password of the server.	Type the password of the server.
Confirm Password	Verifies that the password of the server is entered correctly.	Retype the password of the server.
Server Port	Specifies the port with which the server is associated.	Type the port number.
Source Address	Specifies the source address of the server.	Type the server's 32-bit IP address, in dotted decimal notation.
Retry Attempts	Specifies the number of login retries allowed after a login failure.	Type the number. NOTE: Only 1 retry is permitted for a TACACS server.
Time out	Specifies the time interval to wait before the connection to the server is closed.	Type the interval in seconds.

Related Documentation

- Configuring Management Access for the EX Series Switch (J-Web Procedure) on page 9

CHAPTER 5

Operational Commands

- request message
- show subscribers

request message

Syntax
request message all message "*text*"
request message message "*text*" (terminal *terminal-name* | user *user-name*)

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display a message on the screens of all users who are logged in to the router or switch or on specific screens.

Options
all—Display a message on the terminal of all users who are currently logged in.

message "*text*"—Message to display.

terminal *terminal-name*—Name of the terminal on which to display the message.

user *user-name*—Name of the user to whom to direct the message.

Required Privilege Level
maintenance

List of Sample Output
request message message on page 70

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

Sample Output

request message message

```
user@host> request message message "Maintenance window in 10 minutes" user maria
Message from user@host on ttyp0 at 20:27 ...
Maintenance window in 10 minutes
EOF
```

show subscribers

Syntax

show subscribers
<detail | extensive |terse>
<aci-interface-set-name *aci-interface-set-name*>
<address *address*>
<agent-circuit-identifier *agent-circuit-identifier-substring*>
<client-type *client-type*>
<count>
<interface *interface*>
<logical-system *logical-system*>
<mac-address *mac-address*>
<physical-interface *physical-interface-name*>
<profile-name *profile-name*>
<routing-instance *routing-instance*>
<stacked-vlan-id *stacked-vlan-id*>
<subscriber-state *subscriber-state*>
<user-name *user-name*>
<vlan-id *vlan-id*>

Release Information

Command introduced in Junos OS Release 9.3.
Command introduced in Junos OS Release 9.3 for EX Series switches.
client-type, **mac-address**, **subscriber-state**, and **extensive** options introduced in Junos OS Release 10.2.
count option usage with other options introduced in Junos OS Release 10.2.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Options **aci-interface-set-name** and **agent-circuit-identifier** introduced in Junos OS Release 12.2.
The **physical-interface** and **user-name** options introduced in Junos OS Release 12.3.

Description

Display information for active subscribers.

Options

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

aci-interface-set-name—(Optional) Display all dynamic subscriber sessions that use the specified agent circuit identifier (ACI) interface set. Use the ACI interface set name generated by the router, such as aci-1003-ge-1/0/0.4001, and not the actual ACI value found in the DHCP or PPPoE control packets.

address—(Optional) Display subscribers whose IP address matches the specified address. You must specify the IPv4 or IPv6 address prefix without a netmask (for example, 192.168.17.1). If you specify the IP address as a prefix with a netmask (for example, 192.168.17.1/32), the router displays a message that the IP address is invalid, and rejects the command.

agent-circuit-identifier-substring—(Optional) Display all dynamic subscriber sessions whose ACI value matches the specified substring.

client-type—(Optional) Display subscribers whose client type matches the specified client type (DHCP, L2TP, PPP, PPPOE, VLAN, or static).

count—(Optional) Display the count of total subscribers and active subscribers for any specified option. You can use the **count** option alone or with the **address**, **client-type**, **interface**, **logical-system**, **mac-address**, **profile-name**, **routing-instance**, **stacked-vlan-id**, **subscriber-state**, or **vlan-id** options.

id—(Optional) Display a specific subscriber session whose session id matches the specified subscriber ID. You can display subscriber IDs by using the **show subscribers extensive** or the **show subscribers interface extensive** commands.

interface—(Optional) Display subscribers whose interface matches the specified interface.

logical-system—(Optional) Display subscribers whose logical system matches the specified logical system.

mac-address—(Optional) Display subscribers whose MAC address matches the specified MAC address.

physical-interface-name—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose physical interface matches the specified physical interface.

profile-name—(Optional) Display subscribers whose dynamic profile matches the specified profile name.

routing-instance—(Optional) Display subscribers whose routing instance matches the specified routing instance.

subscriber-state—(Optional) Display subscribers whose subscriber state matches the specified subscriber state (ACTIVE, CONFIGURED, INIT, TERMINATED, or TERMINATING).

user-name—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose username matches the specified subscriber name.

vlan-id—(Optional) Display subscribers whose VLAN ID matches the specified VLAN ID.

stacked-vlan-id—(Optional) Display subscribers whose stacked VLAN ID matches the specified stacked VLAN ID.

NOTE: Due to display limitations, logical system and routing instance output values are truncated when necessary.

Required Privilege Level view

Related Documentation
- *show subscribers summary*
- *Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration*

List of Sample Output
show subscribers (IPv4) on page 76
show subscribers (IPv6) on page 76

Output Fields Table 8 on page 73 lists the output fields for the **show subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 8: show subscribers Output Fields

Field Name	Field Description
User Name	Name of subscriber.
Type	Subscriber client type (DHCP, L2TP, PPP, PPPoE, STATIC-INTERFACE, VLAN).
IP Address	Subscriber IPv4 address.
IP Netmask	Subscriber IP netmask.
Primary DNS Address	IP address of primary DNS server.

Table 8: show subscribers Output Fields *(continued)*

Field Name	Field Description
Secondary DNS Address	IP address of secondary DNS server.
Primary WINS Address	IP address of primary WINS server.
Secondary WINS Address	IP address of secondary WINS server.
IPv6 Address	Subscriber IPv6 address, or multiple addresses.
IPv6 Prefix	Subscriber IPv6 prefix. If you are using DHCPv6 prefix delegation, this is the delegated prefix.
IPv6 User Prefix	IPv6 prefix obtained through ND/RA.
IPv6 Address Pool	Subscriber IPv6 address pool. The IPv6 address pool is used to allocate IPv6 prefixes to the DHCPv6 clients.
IPv6 Network Prefix Length	Length of the network portion of the IPv6 address.
IPv6 Prefix Length	Length of the subscriber IPv6 prefix.
Logical System	Logical system associated with the subscriber.
Routing Instance	Routing instance associated with the subscriber.
Interface	Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface. The * character indicates a continuation of addresses for the same session.
Interface Type	Whether the subscriber interface is **Static** or **Dynamic**.
Interface Set	Internally generated name of the dynamic ACI interface set used by the subscriber session.
Interface Set Type	Interface type of the ACI interface set: **Dynamic**. This is the only ACI interface set type currently supported.
Interface Set Session ID	Identifier of the dynamic ACI interface set entry in the session database.
Underlying Interface	Name of the underlying interface for the subscriber session.
Dynamic Profile Name	Dynamic profile used for the subscriber.
Dynamic Profile Version	Version number of the dynamic profile used for the subscriber.
MAC Address	MAC address associated with the subscriber.
State	Current state of the subscriber session (**Init**, **Configured**, **Active**, **Terminating**, **Tunneled**).

Table 8: show subscribers Output Fields *(continued)*

Field Name	Field Description
VLAN Id	VLAN ID associated with the subscriber in the form *tpid.vlan-id*.
Stacked VLAN Id	Stacked VLAN ID associated with the subscriber in the form *tpid.vlan-id*.
RADIUS Accounting ID	RADIUS accounting ID associated with the subscriber.
Agent Circuit ID	Option 82 agent circuit ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.
Agent Remote ID	Option 82 agent remote ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.
DHCP Relay IP Address	IP address used by the DHCP relay agent.
Login Time	Date and time at which the subscriber logged in.
IPv4 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to IPv4 packets that fail the RPF check.
IPv6 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to IPv6 packets that fail the RPF check.
DHCP Options	**len** = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCP options, as defined in RFC 2132.
Session ID	ID number for a subscriber service session.
Underlying Session ID	For DHCPv6 subscribers on a PPPoE network, displays the session ID of the underlying PPPoE interface.
Service Sessions	Number of service sessions (that is, a service activated using RADIUS CoA) associated with the subscribers.
Service Session Name	Service session profile name.
Session Timeout (seconds)	Number of seconds of access provided to the subscriber before the session is automatically terminated.
Idle Timeout (seconds)	Number of seconds subscriber can be idle before the session is automatically terminated.
IPv6 Delegated Address Pool	Name of the pool used for DHCPv6 prefix delegation.
IPv6 Delegated Network Prefix Length	Length of the prefix configured for the IPv6 delegated address pool.
IPv6 Interface Address	Address assigned by the Framed-Ipv6-Prefix AAA attribute.

Table 8: show subscribers Output Fields *(continued)*

Field Name	Field Description
IPv6 Framed Interface Id	Interface ID assigned by the Framed-Interface-Id AAA attribute.
ADF IPv4 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv4 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
IPv4 Input Filter Name	Name assigned to the IPv4 input filter (client or service session).
IPv4 Output Filter Name	Name assigned to the IPv4 output filter (client or service session).
IPv6 Input Filter Name	Name assigned to the IPv6 input filter (client or service session).
IPv6 Output Filter Name	Name assigned to the IPv6 output filter (client or service session).
IFL Input Filter Name	Name assigned to the logical interface input filter (client or service session).
IFL Output Filter Name	Name assigned to the logical interface output filter (client or service session).

Sample Output

show subscribers (IPv4)

```
user@host> show subscribers
Interface               IP Address/VLAN ID   User Name         LS:RI
ge-1/3/0.1073741824     100                                    default:default
demux0.1073741824       10.0.0.10          WHOLESALER-CLIENT default:default
demux0.1073741825       11.0.0.3           RETAILER1-CLIENT  test1:retailer1
demux0.1073741826       12.0.0.3           RETAILER2-CLIENT  test1:retailer2
```

show subscribers (IPv6)

```
user@host> show subscribers
Interface          IP Address/VLAN ID   User Name           LS:RI
ge-1/0/0.0         2001:db8:c0:0:0:0/74    WHOLESALER-CLIENT   default:default
     *             2001:db8:1/128          subscriber-25       default:default
```

show subscribers (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers
Interface           IP Address/VLAN ID         User Name
LS:RI
demux0.1073741834   0x8100.1002 0x8100.1
default:default
demux0.1073741835   0x8100.1001 0x8100.1
default:default
pp0.1073741836      61.1.1.1                dualstackuser1@EXAMPLE1.com
default:ASP-1
*                   2041:1:1::/48
*                   2061:1:1:1::/64
pp0.1073741837      23.1.1.3                dualstackuser2@EXAMPLE1.com
default:ASP-1
*                   2001:db81:2:5::/64
```

show subscribers (LNS on MX Series Routers)

```
user@host> show subscribers
Interface           IP Address/VLAN ID   User Name         LS:RI
si-4/0/0.1          192.168.4.1          xyz@example.com   default:default
```

show subscribers client-type dhcp detail

```
user@host> show subscribers client-type dhcp detail
Type: DHCP
IP Address: 10.20.9.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Login Time: 2009-08-25 14:43:52 PDT

Type: DHCP
IP Address: 10.20.10.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744383
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:94:00:01:f3
State: Active
Radius Accounting ID: jnpr :2560
Login Time: 2009-08-25 14:43:56 PDT
```

show subscribers count

```
user@host> show subscribers count
Total Subscribers: 188, Active Subscribers: 188
```

show subscribers address detail (IPv6)

```
user@host> show subscribers address 10.16.12.137 detail
```

```
Type: PPPoE
User Name: pppoeTerV6User1Svc
IP Address: 10.16.12.137
IP Netmask: 255.0.0.0
IPv6 User Prefix: 1016:0:0:c88::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073745151
Interface type: Dynamic
Underlying Interface: demux0.8201
Dynamic Profile Name: pppoe-client-profile
MAC Address: 00:0d:02:01:00:01
Session Timeout (seconds): 31622400
Idle Timeout (seconds): 86400
State: Active
Radius Accounting ID: jnpr demux0.8201:6544
Session ID: 6544
Agent Circuit ID: ifl3720
Agent Remote ID: ifl3720
Login Time: 2012-05-21 13:37:27 PDT
Service Sessions: 1
```

show subscribers detail (IPv4)

```
user@host> show subscribers detail
Type: DHCP
IP Address: 10.20.9.7
IP Netmask: 255.255.0.0
Primary DNS Address: 192.168.17.1
Secondary DNS Address: 192.168.17.2
Primary WINS Address: 192.168.22.1
Secondary WINS Address: 192.168.22.2
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Session Timeout (seconds): 3600
Idle Timeout (seconds): 600
Login Time: 2009-08-25 14:43:52 PDT
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
33 2d 37 2d 30 37 05 01 06 0f 21 2c
Service Sessions: 2
```

show subscribers detail (IPv6)

```
user@host> show subscribers detail
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2001:db8db2:ffff:1::/64
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:51:ff:ff:00:03
State: Active
```

```
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

show subscribers detail (IPv6 Static Demux Interface)

```
user@host> show subscribers detail
Type: STATIC-INTERFACE
User Name: demux0.1@example.net
IPv6 Prefix: 1:2:3:4:5:6:7:aa/128
Logical System: default
Routing Instance: default
Interface: demux0.1
Interface type: Static
Dynamic Profile Name: junos-default-profile
State: Active
Radius Accounting ID: 185
Login Time: 2010-05-18 14:33:56 EDT
```

show subscribers detail (L2TP LNS Subscribers on MX Series Routers)

```
user@host> show subscribers detail
Type: L2TP
User Name: user1@example.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
```

show subscribers detail (Tunneled Subscriber)

```
user@host> show subscribers detail
Type: PPPoE
User Name: user1@example.com
Logical System: default
Routing Instance: default
Interface: pp0.1
State: Active, Tunneled
Radius Accounting ID: 512
```

show subscribers detail (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
```

```
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@EXAMPLE1.com
IP Address: 61.1.1.1
IPv6 Prefix: 2041:1:1::/48
IPv6 User Prefix: 2061:1:1:1::/64
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST

Type: DHCP
IPv6 Prefix: 2041:1:1::/48
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: jnpr :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

show subscribers detail (ACI Interface Set Session)

```
user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0
Interface Set: aci-1001-ge-1/0/0.2800
Interface Set Session ID: 0
Underlying Interface: ge-1/0/0.2800
Dynamic Profile Name: aci-vlan-set-profile-2
Dynamic Profile Version: 1
State: Active
Session ID: 1
Agent Circuit ID: aci-ppp-dhcp-20
Login Time: 2012-05-26 01:54:08 PDT
```

show subscribers detail (PPPoE Subscriber Session with ACI Interface Set)

```
user@host> show subscribers detail
Type: PPPoE
User Name: ppphint2
```

```
IP Address: 10.10.1.5
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Interface Set: aci-1001-demux0.1073741824
Interface Set Type: Dynamic
Interface Set Session ID: 2
Underlying Interface: demux0.1073741824
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:64:39:01:02
State: Active
Radius Accounting ID: 3
Session ID: 3
Agent Circuit ID: aci-ppp-dhcp-dvlan-50
Login Time: 2012-03-07 13:46:53 PST
```

show subscribers extensive

```
user@host> show subscribers extensive
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2001:db8db2:ffff:1::/64
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:51:ff:ff:00:03
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Address Pool: pd_pool
IPv6 Network Prefix Length: 48
```

show subscribers extensive (RPF Check Fail Filter)

```
user@host> show subscribers extensive
...
Type: VLAN
  Logical System: default
  Routing Instance: default
  Interface: ae0.1073741824
  Interface type: Dynamic
  Dynamic Profile Name: vlan-prof
  State: Active
  Session ID: 9
  VLAN Id: 100
  Login Time: 2011-08-26 08:17:00 PDT
  IPv4 rpf-check Fail Filter Name: rpf-allow-dhcp
  IPv6 rpf-check Fail Filter Name: rpf-allow-dhcpv6
...
```

show subscribers extensive (L2TP LNS Subscribers on MX Series Routers)

```
user@host> show subscribers extensive
```

```
Type: L2TP
User Name: user1@example.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
IPv4 Input Filter Name: classify-si-5/2/0.1073749824-in
IPv4 Output Filter Name: classify-si-5/2/0.1073749824-out
```

show subscribers extensive (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@EXAMPLE1.com
IP Address: 61.1.1.1
IPv6 Prefix: 2041:1:1::/48
IPv6 User Prefix: 2061:1:1:1::/64
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST
IPv6 Delegated Network Prefix Length: 48
IPv6 Interface Address: 2061:1:1:1::1/64
IPv6 Framed Interface Id: 1:1:2:2
IPv4 Input Filter Name: FILTER-IN-pp0.1073741825-in
IPv4 Output Filter Name: FILTER-OUT-pp0.1073741825-out
IPv6 Input Filter Name: FILTER-IN6-pp0.1073741825-in
IPv6 Output Filter Name: FILTER-OUT6-pp0.1073741825-out

Type: DHCP
IPv6 Prefix: 2041:1:1::/48
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
```

```
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: jnpr :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Delegated Network Prefix Length: 48
```

show subscribers aci-interface-set-name detail (Subscriber Sessions Using Specified ACI Interface Set)

```
user@host> show subscribers aci-interface-set-name aci-1003-ge-1/0/0.4001 detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:65:26:01:02
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT
```

show subscribers agent-circuit-identifier detail (Subscriber Sessions Using Specified ACI Substring)

```
user@host> show subscribers agent-circuit-identifier aci-ppp-vlan detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
```

```
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:65:26:01:02
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT
```

show subscribers interface extensive

```
user@host> show subscribers interface demux0.1073741826 extensive
Type: VLAN
User Name: test1@test.com
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Dynamic
Dynamic Profile Name: profile-vdemux-relay-23qos
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 12
Session ID: 12
Stacked VLAN Id: 0x8100.1500
VLAN Id: 0x8100.2902
Login Time: 2011-10-20 16:21:59 EST

Type: DHCP
User Name: test1@test.com
IP Address: 172.16.200.6
IP Netmask: 255.255.255.0
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Static
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 21
Session ID: 21
Login Time: 2011-10-20 16:24:33 EST
Service Sessions: 2

Service Session ID: 25
Service Session Name: SUB-QOS
State: Active

Service Session ID: 26
Service Session Name: service-cb-content
```

```
State: Active
IPv4 Input Filter Name: content-cb-in-demux0.1073741826-in
IPv4 Output Filter Name: content-cb-out-demux0.1073741826-out
```

show subscribers logical-system terse

```
user@host> show subscribers logical-system test1 terse
Interface           IP Address/VLAN ID   User Name         LS:RI
demux0.1073741825     11.0.0.3            RETAILER1-CLIENT  test1:retailer1
demux0.1073741826     12.0.0.3            RETAILER2-CLIENT  test1:retailer2
```

show subscribers physical-interface count

```
user@host> show subscribers physical-interface ge-1/0/0 count
Total subscribers: 3998, Active Subscribers: 3998
```

show subscribers routing-instance inst1 count

```
user@host> show subscribers routing-instance inst1 count
Total Subscribers: 188, Active Subscribers: 183
```

show subscribers stacked-vlan-id detail

```
user@host> show subscribers stacked-vlan-id 101 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id detail (Combined Output)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id interface detail (Combined Output for a Specific Interface)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 interface ge-1/2/0.* detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers user-name detail

```
user@host> show subscribers user-name larry1 detail
Type: DHCP
User Name: larry1
```

```
IP Address: 100.0.0.37
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.1
Interface type: Static
Dynamic Profile Name: foo
MAC Address: 00:10:94:00:00:01
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-11-07 08:25:59 PST
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 01 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 32 2f
37 2d 30 2d 30 37 05 01 06 0f 21 2c
```

show subscribers vlan-id

```
user@host> show subscribers vlan-id 100
Interface           IP Address                              User Name
ge-1/0/0.1073741824
ge-1/2/0.1073741825
```

show subscribers vlan-id detail

```
user@host> show subscribers vlan-id 100 detail
Type: VLAN
Interface: ge-1/0/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT

Type: VLAN
Interface: ge-1/2/0.1073741825
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT
```

PART 4

Troubleshooting

CHAPTER 6

Troubleshooting Procedures

Troubleshooting Loss of the Root Password

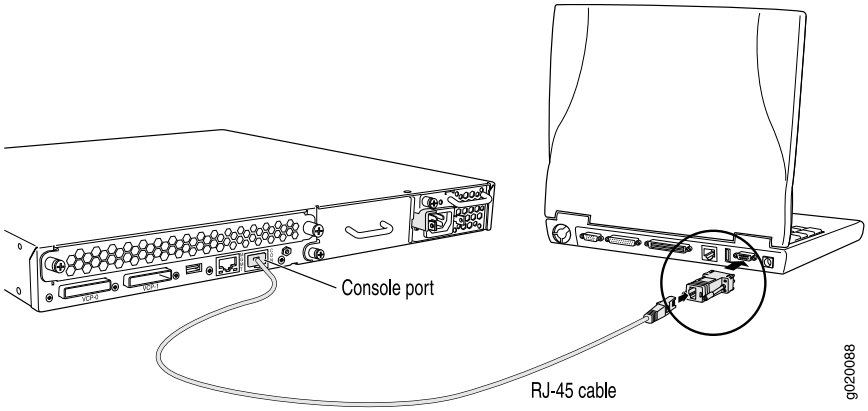
Problem **Description:** If you forget the root password for the switch, you can use the password recovery procedure to reset the root password.

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

Solution To recover the root password:

1. Power off your switch by unplugging the power cord or turning off the power at the wall switch.
2. Insert one end of the Ethernet cable into the serial port on the management device and connect the other end to the console port on the back of the switch. See Figure 1 on page 89

Figure 1: Connecting to the Console Port on the EX Series Switch



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

4. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
5. Power on your switch by plugging in the power cord or turning on the power at the wall switch.
6. When the following prompt appears, press the Spacebar to access the switch's bootstrap loader command prompt:

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

7. At the following prompt, type **boot -s** to start up the system in single-user mode:
   loader> boot -s
8. At the following prompt, type **recovery** to start the root password recovery procedure:
   Enter full path name of shell or 'recovery' for root password recovery or RETURN for /bin/sh: recovery

   A series of messages describe consistency checks, mounting of filesystems, and initialization and checkout of management services. Then the CLI prompt appears.
9. Enter configuration mode in the CLI:
   user@switch> configure
10. Set the root password. For example:
    user@switch# set system root-authentication plain-text-password
11. At the following prompt, enter the new root password. For example:
    New password: juniper1

    ```
    Retype new password:
    ```

12. At the second prompt, reenter the new root password.
13. If you are finished configuring the network, commit the configuration.
    root@switch# commit

    ```
    commit complete
    ```

14. Exit configuration mode in the CLI.
    root@switch# exit
15. Exit operational mode in the CLI.
    root@switch> exit
16. At the prompt, enter **y** to reboot the switch.
    Reboot the system? [y/n] y

Related Documentation

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

- *Connecting and Configuring an EX Series Switch (J-Web Procedure)*
- For information about configuring an encrypted root password, configuring SSH keys to authenticate root logins, and configuring special requirements for plain-text passwords, see the *Junos OS System Basics Configuration Guide*.