



User and Access Management Feature Guide for the QFX Series

Release
14.1X53



Modified: 2015-09-14

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

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

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

User and Access Management Feature Guide for the QFX Series
14.1X53
Copyright © 2015, Juniper Networks, Inc.
All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

	About the Documentation	xv
	Documentation and Release Notes	xv
	Supported Platforms	xv
	Using the Examples in This Manual	xv
	Merging a Full Example	xvi
	Merging a Snippet	xvi
	Documentation Conventions	xvii
	Documentation Feedback	xix
	Requesting Technical Support	xix
	Self-Help Online Tools and Resources	xix
	Opening a Case with JTAC	xx
Part 1	User and Access Management Overview	
Chapter 1	Understanding the Software	3
	Understanding Software Infrastructure and Processes	3
	Routing Engine and Packet Forwarding Engine	3
	Junos OS Processes	4
	Understanding LLDP	5
	Monitoring SNMP	6
Chapter 2	Understanding Access and Authentication Methods	9
	Understanding Junos OS Access Privilege Levels	9
	Junos OS Login Class Permission Flags	9
	Allowing or Denying Individual Commands for Junos OS Login Classes	13
	Junos OS User Authentication Methods	14
	Understanding Login Authentication	15
	MAC RADIUS Authentication	15
Part 2	Configuring Access	
Chapter 3	Configuring 802.1X Authentication to Control Network Access	19
	802.1X for Switches Overview	20
	How 802.1X Authentication Works	20
	802.1X Features Overview	21
	Configuring 802.1X Interface Settings (CLI Procedure)	22
	Specifying RADIUS Server Connections on Switches (CLI Procedure)	24
	Example: Connecting a RADIUS Server for 802.1X to a Switch	25

	Configuring Server Fail Fallback (CLI Procedure)	30
	Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch	31
	Understanding 802.1X and VSAs on Switches	37
	VSA Match Conditions and Actions	38
	Filtering 802.1X Supplicants By Using RADIUS Server Attributes	40
	Configuring Match Statements on the RADIUS Server	40
	Applying a Port Firewall Filter from the RADIUS Server	42
	Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on a Switch	43
	Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication	49
	Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to a Switch	54
	Understanding Guest VLANs for 802.1X on Switches	60
	Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch	61
	Understanding 802.1X and RADIUS Accounting on Switches	66
	Configuring 802.1X RADIUS Accounting (CLI Procedure)	67
	Understanding Dynamic VLANs for 802.1X on Switches	68
	Example: Configuring Fallback Options on Switches for EAP-TTLS Authentication and Odyssey Access Clients	69
	Controlling Authentication Session Timeouts (CLI Procedure)	74
	Verifying 802.1X Authentication	74
Chapter 4	Configuring MAC RADIUS Authentication to Control Network Access	77
	Configuring MAC RADIUS Authentication (CLI Procedure)	77
	Specifying RADIUS Server Connections on Switches (CLI Procedure)	79
	Configuring Server Fail Fallback (CLI Procedure)	81
	Example: Configuring MAC RADIUS Authentication on a Switch	82
	Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication	88
	Controlling Authentication Session Timeouts (CLI Procedure)	93
Chapter 5	Bypassing 802.1X and MAC RADIUS Authentication to Allow Trusted Hosts to Access the Network	95
	Configuring Static MAC Bypass of Authentication (CLI Procedure)	95
	Example: Configuring Static MAC Bypass of Authentication on a Switch	95
Chapter 6	Configuring Device Discovery Using LLDP and LLDP-MED	101
	Understanding 802.1X and LLDP and LLDP-MED	101
	Configuring LLDP (CLI Procedure)	104
	Enabling LLDP on Interfaces	104
	Adjusting LLDP Advertisement Settings	105
	Adjusting SNMP Notification Settings of LLDP Changes	105
	Specifying a Management Address for the LLDP Management TLV	106
	Configuring LLDP Power Negotiation	106
	Configuring LLDP-MED (CLI Procedure)	107
	Enabling LLDP-MED on Interfaces	107
	Configuring Location Information Advertised by the Switch	108

	Configuring for Fast Start	108
Chapter 7	Configuring VoIP	109
	Understanding 802.1X and VoIP	109
	Example: Setting Up VoIP with 802.1X and LLDP-MED on a Switch	111
	Example: Configuring VoIP on a Switch Without Including 802.1X Authentication	120
Chapter 8	Configuring and Managing Root Users	127
	Configuring Management Access	127
	Configuring Access Privilege Levels	127
	Configuring Login Tips	128
	Recovering the Root Password	128
	Example: Configuring a Plain-Text Password for Root Logins	130
	Example: Configuring SSH Authentication for Root Logins	132
	Understanding Troubleshooting Resources	132
	Troubleshooting Overview	134
	Recovering the Root Password	136
Chapter 9	Configuring and Managing User Accounts	139
	Junos OS User Accounts Overview	139
	Junos OS Login Classes Overview	141
	Special Requirements for Junos OS Plain-Text Passwords	142
	Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies	144
	Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands	145
	Defining Access Privileges Using allow or deny configuration Statements	146
	Example: Configuring User Accounts	147
	Example: Configuring Access Privilege Levels	148
	Example: Configuring Access Privileges for Operational Mode Commands	149
	Example: Changing the Requirements for Junos OS Plain-Text Passwords	149
	Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions	151
	Understanding Troubleshooting Resources	152
	Troubleshooting Overview	154
	Recovering the Root Password	156
Part 3	Configuring Authentication	
Chapter 10	Configuring and Managing Local Password Authentication	161
	Junos OS User Accounts Overview	161
	Junos OS User Authentication Methods	163
	Junos OS Login Classes Overview	164
	Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies	165
	Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands	166

	Special Requirements for Junos OS Plain-Text Passwords	167
	Configuring Junos OS User Accounts	169
	Example: Configuring User Login Accounts	169
	Example: Creating Login Classes with Specific Privileges	170
	Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication	171
	Example: Changing the Requirements for Junos OS Plain-Text Passwords	173
Chapter 11	Configuring and Managing TACACS+ Authentication	175
	Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication	175
	Using RADIUS or TACACS+ Authentication	175
	Using Local Password Authentication	176
	Order of Authentication Attempts	176
	Configuring TACACS+ Authentication (QFX Series)	180
	Configuring TACACS+ Server Details	180
	Specifying a Source Address for the Junos OS to Access External TACACS+ Servers	181
	Configuring the Same Authentication Service for Multiple TACACS+ Servers	181
	Configuring Juniper Networks Vendor-Specific TACACS+ Attributes	182
	Juniper Networks Vendor-Specific TACACS+ Attributes	182
	Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication	184
Chapter 12	Configuring and Managing RADIUS Authentication	187
	Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication	187
	Using RADIUS or TACACS+ Authentication	187
	Using Local Password Authentication	188
	Order of Authentication Attempts	188
	Configuring RADIUS Authentication (QFX Series or OCX Series)	192
	Configuring RADIUS Server Details	192
	Configuring MS-CHAPv2 for Password-Change Support	193
	Specifying a Source Address for the Junos OS to Access External RADIUS Servers	194
	Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands	194
	Example: Configuring RADIUS Authentication	196
	Example: Configuring RADIUS Template Accounts	197
	Example: Configuring User Login Accounts	197
	Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication	198
Chapter 13	Configuring and Managing RADIUS Accounting	201
	Understanding RADIUS Accounting	201
	Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication	202
	Using RADIUS or TACACS+ Authentication	202
	Using Local Password Authentication	203

	Order of Authentication Attempts	203
	Juniper Networks Vendor-Specific RADIUS Attributes	207
	Configuring RADIUS System Accounting	209
	Configuring Auditing of User Events on a RADIUS Server	209
	Specifying RADIUS Server Accounting and Auditing Events	209
	Configuring RADIUS Server Accounting	210
	Configuring RADIUS Authentication (QFX Series or OCX Series)	211
	Configuring RADIUS Server Details	211
	Configuring MS-CHAPv2 for Password-Change Support	212
	Specifying a Source Address for the Junos OS to Access External RADIUS Servers	213
	Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands	214
	Example: Configuring RADIUS System Accounting	215
Chapter 14	Configuring and Managing RADIUS Template Accounts	217
	Overview of Template Accounts for RADIUS and TACACS+ Authentication	217
	Example: Configuring RADIUS Template Accounts	217
Chapter 15	Configuring and Managing VSAs for RADIUS and TACACS+	219
	Understanding VSAs	219
	VSA Match Conditions and Actions	220
	Juniper Networks Vendor-Specific TACACS+ Attributes	222
Part 4	Configuration Statements and Operational Commands	
Chapter 16	Configuration Statements	227
	access	230
	accounting (Access Profile)	231
	accounting-options	232
	accounting-server	234
	accounting-stop-on-access-deny	235
	accounting-stop-on-failure	236
	advertisement-interval	237
	agent-address	238
	archival	239
	archive-sites (Configuration File)	240
	authentication-order	241
	authentication-server	242
	authenticator	243
	authorization	244
	block-interval	245
	categories	245
	client-list	246
	client-list-name	246
	clients	247
	commit-delay	247
	community (SNMP)	248
	configuration	249
	connection-limit	250

contact	251
disable (802.1X)	251
disable (LLDP)	252
dot1x	253
eapol-block	254
falling-threshold (Health Monitor)	255
filter-duplicates	255
full-name	256
guest-vlan	256
health-monitor	257
hold-multiplier	258
idle-timeout (Access)	259
interface (802.1X)	260
interface (LLDP)	262
interface (Static MAC Bypass)	263
interval (Health Monitor)	264
lldp	265
lldp-med (Ethernet Switching)	267
lldp-med-bypass	268
lldp-configuration-notification-interval	268
location	269
mac-radius	270
management-address	271
maximum-requests	272
name	272
nas-ip-address	273
no-mac-table-binding (802.1X)	273
nonvolatile	274
no-reauthentication	274
oid	275
order	276
port (RADIUS Server)	277
profile	278
protocols	279
protocol-version	292
ptopo-configuration-maximum-hold-time	293
ptopo-configuration-trap-interval	293
quiet-period	294
radius	295
radius-options (edit system)	296
radius-options (Protocols 802.1X)	297
radius-server	298
rate-limit	299
reauthentication	300
remote-debug-permission	301
retries	302
retry	303
rising-threshold (Health Monitor)	304
root-login	305

	server-fail	306
	server-timeout	307
	services (Switches)	308
	snmp	309
	ssh	313
	static (Protocols 802.1X)	314
	supplicant	315
	supplicant-timeout	316
	system	317
	tacplus-options	323
	targets	324
	transmit-period	324
	traceoptions (LLDP)	325
	transfer-interval (Configuration)	327
	transfer-on-commit	328
	trap-group	329
	trap-options	330
	user (Access)	331
	version	332
	vlan-assignment	333
	voip	334
Chapter 17	Operational Commands	335
	clear dot1x	336
	clear lldp neighbors	338
	clear lldp statistics	339
	show dot1x	340
	show dot1x authentication-failed-users	345
	show dot1x firewall	346
	show dot1x static-mac-address	347
	show ethernet-switching interfaces	349
	show lldp	353
	show lldp local-information	358
	show lldp neighbors	360
	show lldp statistics	364
	show network-access aaa statistics accounting	366
	show network-access aaa statistics authentication	367
	show network-access aaa statistics dynamic-requests	369
	show route instance	370
	show snmp statistics	374
	ssh	378

List of Figures

Part 2	Configuring Access	
Chapter 3	Configuring 802.1X Authentication to Control Network Access	19
	Figure 1: Topology for Configuration	27
	Figure 2: Topology for Configuring Supplicant Modes	33
	Figure 3: Topology for Firewall Filter and RADIUS Server Attributes Configuration	45
	Figure 4: Conceptual Model: Dynamic Filter Updated for Each New User	51
	Figure 5: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server	52
	Figure 6: Topology for Configuration	56
	Figure 7: Topology for Guest VLAN Example	63
	Figure 8: EX Series Switch Connecting OAC to RADIUS Server Using EAP-TTLS Authentication	71
Chapter 4	Configuring MAC RADIUS Authentication to Control Network Access	77
	Figure 9: Topology for MAC RADIUS Authentication Configuration	84
	Figure 10: Conceptual Model: Dynamic Filter Updated for Each New User	90
	Figure 11: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server	91
Chapter 5	Bypassing 802.1X and MAC RADIUS Authentication to Allow Trusted Hosts to Access the Network	95
	Figure 12: Topology for Static MAC Authentication Configuration	97
Chapter 7	Configuring VoIP	109
	Figure 13: VoIP Multiple Supplicant Topology	110
	Figure 14: VoIP Single Supplicant Topology	111
	Figure 15: VoIP Topology	114

List of Tables

	About the Documentation	xv
	Table 1: Notice Icons	xvii
	Table 2: Text and Syntax Conventions	xvii
Part 1	User and Access Management Overview	
Chapter 1	Understanding the Software	3
	Table 3: Junos OS Processes	4
Chapter 2	Understanding Access and Authentication Methods	9
	Table 4: Login Class Permission Flags	10
Part 2	Configuring Access	
Chapter 3	Configuring 802.1X Authentication to Control Network Access	19
	Table 5: Components of the Topology	27
	Table 6: Components of the Supplicant Mode Configuration Topology	34
	Table 7: Match Conditions	38
	Table 8: Actions for VSAs	39
	Table 9: Components of the Firewall Filter and RADIUS Server Attributes Topology	45
	Table 10: Components of the Topology	57
	Table 11: Components of the Guest VLAN Topology	63
	Table 12: Components of the OAC Deployment	71
Chapter 4	Configuring MAC RADIUS Authentication to Control Network Access	77
	Table 13: Components of the MAC RADIUS Authentication Configuration Topology	85
Chapter 5	Bypassing 802.1X and MAC RADIUS Authentication to Allow Trusted Hosts to Access the Network	95
	Table 14: Components of the Static MAC Authentication Configuration Topology	97
Chapter 7	Configuring VoIP	109
	Table 15: Components of the VoIP Configuration Topology	114
Chapter 8	Configuring and Managing Root Users	127
	Table 16: Troubleshooting Resources on the QFX and OCX Series	132
	Table 17: Troubleshooting on the QFX Series	134
Chapter 9	Configuring and Managing User Accounts	139
	Table 18: Predefined System Login Classes	141

	Table 19: Special Requirements for Plain-Text Passwords	142
	Table 20: Configuration Mode Hierarchies—Common Regular Expression Operators	145
	Table 21: Common Regular Expression Operators to Allow or Deny Operational Mode Commands	146
	Table 22: Troubleshooting Resources on the QFX and OCX Series	152
	Table 23: Troubleshooting on the QFX Series	154
Part 3	Configuring Authentication	
Chapter 10	Configuring and Managing Local Password Authentication	161
	Table 24: Predefined System Login Classes	164
	Table 25: Configuration Mode Hierarchies—Common Regular Expression Operators	165
	Table 26: Common Regular Expression Operators to Allow or Deny Operational Mode Commands	166
	Table 27: Special Requirements for Plain-Text Passwords	167
Chapter 11	Configuring and Managing TACACS+ Authentication	175
	Table 28: Order of Authentication Attempts	177
	Table 29: Juniper Networks Vendor-Specific TACACS+ Attributes	183
Chapter 12	Configuring and Managing RADIUS Authentication	187
	Table 30: Order of Authentication Attempts	189
Chapter 13	Configuring and Managing RADIUS Accounting	201
	Table 31: Order of Authentication Attempts	204
	Table 32: Juniper Networks Vendor-Specific RADIUS Attributes	207
Chapter 15	Configuring and Managing VSAs for RADIUS and TACACS+	219
	Table 33: Match Conditions	220
	Table 34: Actions for VSAs	221
	Table 35: Juniper Networks Vendor-Specific TACACS+ Attributes	222
Part 4	Configuration Statements and Operational Commands	
Chapter 17	Operational Commands	335
	Table 36: show dot1x Output Fields	340
	Table 37: show dot1x authentication-failed-users Output Fields	345
	Table 38: show dot1x static-mac-address Output Fields	347
	Table 39: show ethernet-switching interfaces Output Fields	349
	Table 40: show lldp Output Fields	353
	Table 41: show lldp local-information Output Fields	358
	Table 42: show lldp neighbors Output Fields	360
	Table 43: show lldp statistics Output Fields	364
	Table 44: show network-access aaa statistics accounting Output Fields	366
	Table 45: show network-access aaa statistics authentication Output Fields	367
	Table 46: show network-access aaa statistics dynamic-requests Output Fields	369
	Table 47: show route instance Output Fields	370
	Table 48: show snmp statistics Output Fields	374

About the Documentation

- [Documentation and Release Notes on page xv](#)
- [Supported Platforms on page xv](#)
- [Using the Examples in This Manual on page xv](#)
- [Documentation Conventions on page xvii](#)
- [Documentation Feedback on page xix](#)
- [Requesting Technical Support on page xix](#)

Documentation and Release Notes

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

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

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

Supported Platforms

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

- [QFX Series standalone switches](#)

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

Table 1 on page xvii 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 xvii 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.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric metric>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (string1 string2 string3)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.

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 at the Juniper Networks Technical Documentation 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

User and Access Management Overview

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

CHAPTER 1

Understanding the Software

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

Understanding Software Infrastructure and Processes

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

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

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

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

Routing Engine and Packet Forwarding Engine

A switch has two primary software processing components:

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

Junos OS Processes

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

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

[Table 3 on page 4](#) describes the primary Junos OS processes.

Table 3: Junos OS Processes

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

Table 3: Junos OS Processes (*continued*)

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

Related Documentation

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

Understanding LLDP

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

LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include specifics, such as chassis and port

identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in Junos OS.

The device supports the following basic TLVs:

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

The device supports the following 802.3 TLVs:

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

**Related
Documentation**

- *Configuring LLDP*

Monitoring SNMP

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
user@switch> show snmp statistics

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

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

- Related Documentation**
- [health-monitor on page 257](#)
 - *show snmp mib*
 - [show snmp statistics on page 374](#)

CHAPTER 2

Understanding Access and Authentication Methods

- [Understanding Junos OS Access Privilege Levels on page 9](#)
- [Junos OS User Authentication Methods on page 14](#)
- [Understanding Login Authentication on page 15](#)

Understanding Junos OS Access Privilege Levels

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

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

The following sections provide additional information about permissions:

- [Junos OS Login Class Permission Flags on page 9](#)
- [Allowing or Denying Individual Commands for Junos OS Login Classes on page 13](#)

Junos OS Login Class Permission Flags

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

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

Table 4 on page 10 lists the Junos[®] operating system (Junos OS) login class permission flags that you can configure by including the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level.

Table 4: Login Class Permission Flags

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

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

Permission Flag	Description
flow-tap-operation	Can make flow-tap requests to the router or switch. For example, a Dynamic Tasking Control Protocol (DTCP) client must have flow-tap-operation permission to authenticate itself to the Junos OS as an administrative user. NOTE: The flow-tap-operation option is not included in the all-control permissions flag.
idp-profiler-operation	Can view profiler data.
interface	Can view the interface configuration in configuration mode and with the show configuration operational mode command.
interface-control	Can view chassis, class of service (CoS), groups, forwarding options, and interfaces configuration information. Can edit configuration at the following hierarchy levels: <ul style="list-style-type: none"> • [edit chassis] • [edit class-of-service] • [edit groups] • [edit forwarding-options] • [edit interfaces]
maintenance	Can perform system maintenance, including starting a local shell on the router and becoming the superuser in the shell by using the su root command, and can halt and reboot the router by using the request system commands.
network	Can access the network by using the ping , ssh , telnet , and traceroute commands.
pgcp-session-mirroring	Can view the pgcp session mirroring configuration.
pgcp-session-mirroring-control	Can modify the pgcp session mirroring configuration.
reset	Can restart software processes by using the restart command and can configure whether software processes are enabled or disabled at the [edit system processes] hierarchy level.
rollback	Can use the rollback command to return to a previously committed configuration other than the most recently committed one.
routing	Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.

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

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

Allowing or Denying Individual Commands for Junos OS Login Classes

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

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

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

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

- Related Documentation**
- [Configuring Access Privilege Levels on page 127](#)
 - [Access Privilege User Permission Flags Overview](#)

Junos OS User Authentication Methods

The Junos OS supports three methods of user authentication: local password authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+).

With local password authentication, you configure a password for each user allowed to log in to the router or switch.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the router or switch using telnet. They are both distributed client-server systems—the RADIUS and TACACS+ clients run on the router or switch, and the server runs on a remote network system.

You can configure the router or switch to be both a RADIUS and TACACS+ client, and you can also configure authentication passwords in the Junos OS configuration file. You can prioritize the methods to configure the order in which the software tries the different authentication methods when verifying user access.

- Related Documentation**
- [Configuring RADIUS Authentication](#)
 - [Configuring TACACS+ Authentication](#)
 - [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 175](#)
 - [Configuring RADIUS Authentication \(QFX Series or OCX Series\) on page 192](#)
 - [Configuring TACACS+ Authentication \(QFX Series\) on page 180](#)

Understanding Login Authentication

You can control access to your network using several different authentication methods—media access control (MAC) RADIUS, for example. Authentication prevents unauthorized devices and users from gaining access to your LAN. For MAC RADIUS authentication, end devices must be authenticated before they receive an IP address from a DHCP server.

You can enable end devices to access the network without authenticating on the RADIUS server by configuring the MAC address of the end device in the static MAC bypass list by configuring the MAC address using the **authentication-whitelist** statement.

You can configure one or more authentication methods on a single interface and thereby enable fallback to the next method if the first or second method is unsuccessful.

On a single interface you can configure one or a combination of several authentication methods.

This topic covers:

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

MAC RADIUS Authentication

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

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

When you configure the **mac-radius restrict** option, the switch immediately attempts a MAC- RADIUS authentication by sending a request to the RADIUS server for authentication of the MAC address of the end device. If MAC address of the end device is configured for RADIUS authentication, LAN access between the two switches is created.

Related Documentation

- [Configuring RADIUS Authentication \(QFX Series or OCX Series\) on page 192](#)

PART 2

Configuring Access

- [Configuring 802.1X Authentication to Control Network Access on page 19](#)
- [Configuring MAC RADIUS Authentication to Control Network Access on page 77](#)
- [Bypassing 802.1X and MAC RADIUS Authentication to Allow Trusted Hosts to Access the Network on page 95](#)
- [Configuring Device Discovery Using LLDP and LLDP-MED on page 101](#)
- [Configuring VoIP on page 109](#)
- [Configuring and Managing Root Users on page 127](#)
- [Configuring and Managing User Accounts on page 139](#)

CHAPTER 3

Configuring 802.1X Authentication to Control Network Access

- [802.1X for Switches Overview on page 20](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 22](#)
- [Specifying RADIUS Server Connections on Switches \(CLI Procedure\) on page 24](#)
- [Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25](#)
- [Configuring Server Fail Fallback \(CLI Procedure\) on page 30](#)
- [Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31](#)
- [Understanding 802.1X and VSAs on Switches on page 37](#)
- [VSA Match Conditions and Actions on page 38](#)
- [Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 40](#)
- [Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on a Switch on page 43](#)
- [Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on page 49](#)
- [Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to a Switch on page 54](#)
- [Understanding Guest VLANs for 802.1X on Switches on page 60](#)
- [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 61](#)
- [Understanding 802.1X and RADIUS Accounting on Switches on page 66](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 67](#)
- [Understanding Dynamic VLANs for 802.1X on Switches on page 68](#)
- [Example: Configuring Fallback Options on Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 69](#)
- [Controlling Authentication Session Timeouts \(CLI Procedure\) on page 74](#)
- [Verifying 802.1X Authentication on page 74](#)

802.1X for Switches Overview

How 802.1X Authentication Works

IEEE 802.1X provides network edge security, protecting Ethernet LANs from unauthorized user access. 802.1X authentication works by using an *authenticator port access entity* (the switch) to block all traffic to and from a supplicant (end device) at the port until the supplicant's credentials are presented and matched on the *Authentication server* (a RADIUS server). When the end device (supplicant) is authenticated, the switch stops blocking traffic and opens the port to the supplicant.

The end device is authenticated in either *single* mode, *single-secure* mode, or *multiple* mode:

- **single**—Authenticates only the first end device. All other end devices that connect later to the port are allowed full access without any further authentication. They effectively *piggyback* on the first end device's authentication.
- **single-secure**—Allows only one end device to connect to the port. No other end device is allowed to connect until the first logs out.
- **multiple**—Allows multiple end devices to connect to the port. Each end device will be authenticated individually.

Network access can be further defined using VLANs and firewall filters, which both act as filters to separate and match groups of end devices to the areas of the LAN they require. For example, you can configure VLANs to handle different categories of authentication failures depending upon:

- Whether or not the end device is 802.1X-enabled.
- Whether or not MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected.
- Whether the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message. See [“Configuring Server Fail Fallback \(CLI Procedure\)”](#) on [page 30](#).

802.1X Features Overview



NOTE: EX4600 switches support 802.1X authentication only when these switches operate in a mixed Virtual Chassis with EX4300 switches, and only on EX4300 interfaces.

The following 802.1X features are supported on Juniper Networks Ethernet Switches:

- **Guest VLAN**—Provides limited access to a LAN, typically just to the Internet, for nonresponsive end devices that are not 802.1X-enabled when MAC RADIUS authentication has not been configured on the switch interfaces to which the hosts are connected. Also, a guest VLAN can be used to provide limited access to a LAN for guest users. Typically, the guest VLAN provides access just to the Internet and to other guests' end devices.
- **Server-reject VLAN**—Provides limited access to a LAN, typically just to the Internet, for responsive end devices that have sent the wrong credentials.
- **Server-fail VLAN**—Provides limited access to a LAN, typically just to the Internet, for end devices during a RADIUS server timeout.
- **Dynamic VLAN**—Enables an end device, after authentication, to be a member of a VLAN dynamically.
- **Private VLAN**—Enables configuration of 802.1X authentication on interfaces that are members of private VLANs (PVLANS).
- **Dynamic changes to a user session**—Allows the switch administrator to terminate an already authenticated session. This feature is based on support of the RADIUS Disconnect Message defined in RFC 3576.
- **Support for VoIP**—If an IP phone is 802.1X-enabled, it is authenticated like any other supplicant. If the phone is not 802.1X-enabled, but has another 802.1X-compatible device connected to its data port, that device is authenticated, and then VoIP traffic can flow to and from the phone (provided that the interface is configured in single mode and not in single-secure mode).



NOTE: Configuring a VoIP VLAN on private VLAN (PVLAN) interfaces is not supported.

- **RADIUS accounting**—Sends accounting information to the RADIUS accounting server. Accounting information is sent to the server whenever a subscriber logs in or logs out and whenever a subscriber activates or deactivates a subscription.
- **Vendor Specific Attributes (VSAs)**—Supports the **Juniper-Switching-Filter** attribute on the RADIUS authentication server that can be used further define a supplicant's access during the 802.1X authentication process. Centrally configuring VSAs on the authentication server does away with the need to configure these same attributes in the form of firewall filters on every switch in the LAN to which the supplicant may connect to the LAN.

The following features are supported to authenticate devices that are not 802.1X-enabled:

- Static MAC bypass—Provides a bypass mechanism to authenticate devices that are not 802.1X-enabled (such as printers). Static MAC bypass connects these devices to 802.1X-enabled ports, bypassing 802.1X authentication.
- MAC RADIUS authentication—Provides a means to enable or disable MAC authentication independently of whether 802.1X authentication is enabled.

**Related
Documentation**

- [Understanding Authentication on Switches](#)
- [Understanding 802.1X and VoIP on page 109](#)
- [Understanding 802.1X and LLDP and LLDP-MED on page 101](#)
- [Understanding 802.1X and RADIUS Accounting on Switches on page 66](#)
- [Understanding Guest VLANs for 802.1X on Switches on page 60](#)
- [Understanding 802.1X and VSAs on Switches on page 37](#)
- [Understanding Server Fail Fallback and Authentication on Switches](#)

Configuring 802.1X Interface Settings (CLI Procedure)

IEEE 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the *authentication server* (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.



NOTE:

- You can also specify an 802.1X exclusion list to specify supplicants that can bypass authentication and be automatically connected to the LAN. See [“Configuring Static MAC Bypass of Authentication \(CLI Procedure\)” on page 95](#).
- You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.
- You cannot configure 802.1X user authentication on redundant trunk groups (RTGs). For more information on RTGs, see [Understanding Redundant Trunk Links](#).

Before you begin, specify the RADIUS server or servers to be used as the authentication server. See [“Specifying RADIUS Server Connections on Switches \(CLI Procedure\)” on page 24](#).

To configure 802.1X on an interface:

1. Configure the supplicant mode as **single** (authenticates the first supplicant), **single-secure** (authenticates only one supplicant), or **multiple** (authenticates multiple supplicants):

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name supplicant multiple
```

2. Enable reauthentication and specify the reauthentication interval:

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name reauthentication interval seconds
```

3. Configure the interface timeout value for the response from the supplicant:

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name supplicant-timeout seconds
```

4. Configure the timeout for the interface before it resends an authentication request to the RADIUS server:

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name server-timeout seconds
```

5. Configure how long, in seconds, the interface waits before retransmitting the initial EAPOL PDUs to the supplicant:

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name transmit-period seconds
```

6. Configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out:

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name maximum-requests number
```

7. Configure the number of times the switch attempts to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt.

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name retries number
```



NOTE: This setting specifies the number of tries before the switch puts the interface in a HELD state.

Related Documentation

- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
- [Monitoring 802.1X Authentication](#)
- [Verifying 802.1X Authentication on page 74](#)
- [Configuring LLDP \(CLI Procedure\) on page 104](#)
- [Understanding Authentication on Switches](#)

Specifying RADIUS Server Connections on Switches (CLI Procedure)

IEEE 802.1X and MAC RADIUS authentication both provide network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from devices at the interface until the supplicant's credentials or MAC address are presented and matched on the *authentication server* (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

To use 802.1X or MAC RADIUS authentication, you must specify the connections on the switch for each RADIUS server to which you will connect.

To configure a RADIUS server on the switch:

1. Define the IP address of the RADIUS server, the RADIUS server authentication port number, and the secret password. You can define more than one RADIUS server. The secret password on the switch must match the secret password on the server:

```
[edit access]
user@switch# set radius-server 10.0.0.100 port 1812 secret abc
```



NOTE: Specifying the authentication port is optional, and port 1812 is the default. However, we recommend that you configure it in order to avoid confusion as some RADIUS servers might refer to an older default.

2. (Optional) Specify the IP address by which the switch is identified by the RADIUS server. If you do not specify this, the RADIUS server uses the address of the interface sending the RADIUS request. We recommend that you specify this IP address because if the request gets diverted on an alternate route to the RADIUS server, the interface relaying the request might not be an interface on the switch.

```
[edit access]
user@switch# set access radius-server source-address 10.93.14.100
```

3. Configure the authentication order, making **radius** the first method of authentication:

```
[edit access]
user@switch# set profile profile1 authentication-order radius
```

4. Create a profile and specify the list of RADIUS servers to be associated with the profile. For example, you might choose to group your RADIUS servers geographically by city. This feature enables easy modification whenever you want to change to a different set of authentication servers.

```
[edit access profile]
user@switch# set atlanta radius authentication-server 10.0.0.100 10.2.14.200
```

5. Specify the group of servers to be used for 802.1X or MAC RADIUS authentication by identifying the profile name:

```
[edit access profile]
user@switch# set protocols dot1x authenticator authentication-profile-name denver
```

6. Configure the IP address of the switch in the list of clients on the RADIUS server. For specifics on configuring the RADIUS server, consult the documentation for your server.

- Related Documentation**
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 22](#)
 - [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
 - [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 77](#)
 - [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 67](#)

Example: Connecting a RADIUS Server for 802.1X to a Switch

802.1X is the IEEE standard for Port-Based Network Access Control (PNAC). You use 802.1X to control network access. Only users and devices providing credentials that have been verified against a user database are allowed access to the network. You can use a RADIUS server as the user database for 802.1X authentication, as well as for MAC RADIUS authentication.

This example describes how to connect a RADIUS server to a switch, and configure it for 802.1X:

- [Requirements on page 25](#)
- [Overview and Topology on page 26](#)
- [Configuration on page 28](#)
- [Verification on page 29](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch* or *Example: Setting Up Basic Bridging and a VLAN on the QFX Series*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.



NOTE: For more about ELS, see: *Getting Started with Enhanced Layer 2 Software*

- Configured users on the RADIUS authentication server.

Overview and Topology

The EX Series switch acts as an authenticator Port Access Entity (PAE). It blocks all traffic and acts as a control gate until the supplicant (client) is authenticated by the server. All other users and devices are denied access.

Figure 1 on page 27 shows one EX4200 switch that is connected to the devices listed in Table 5 on page 27.



NOTE: This figure also applies to QFX5100 switches.

Figure 1: Topology for Configuration

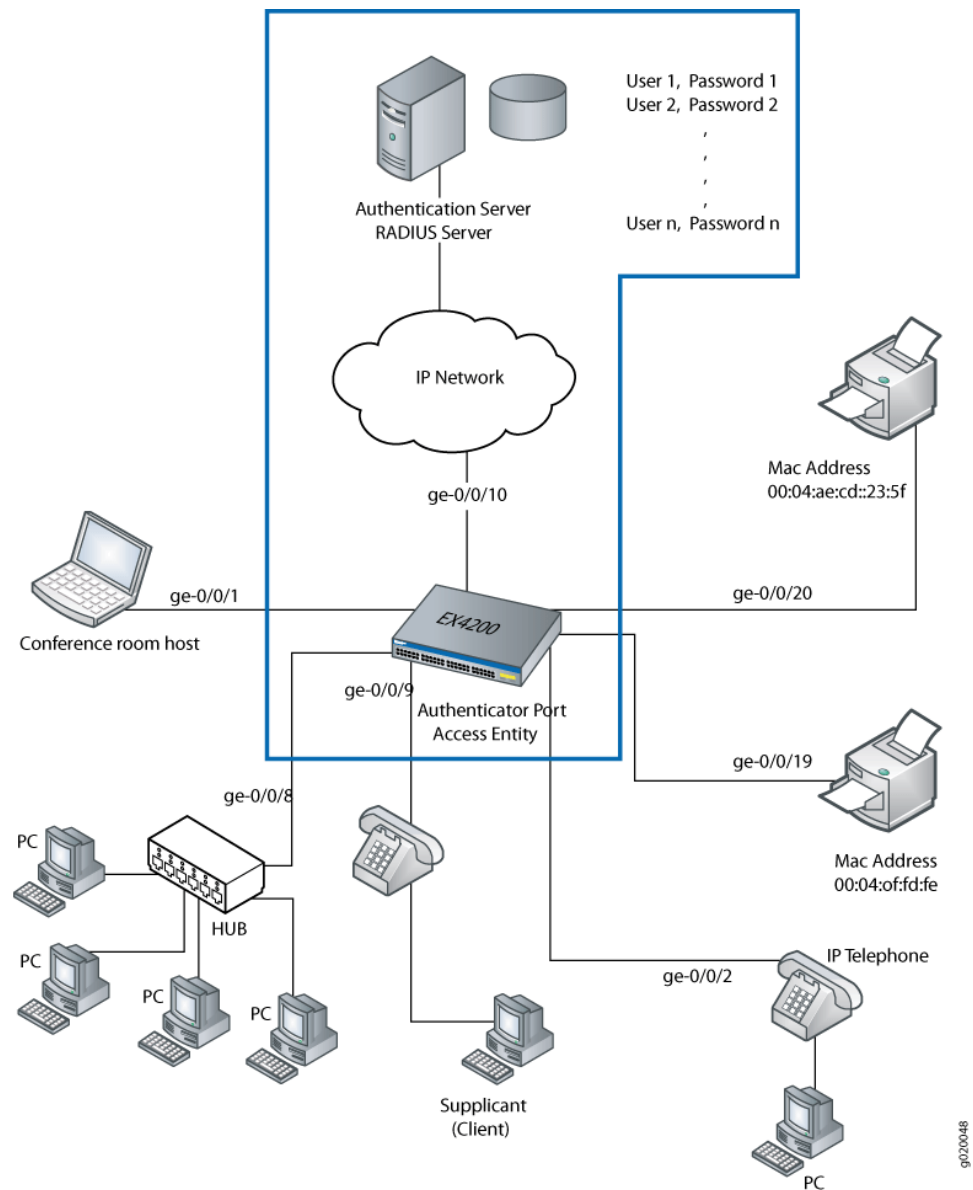


Table 5: Components of the Topology

Property	Settings
Switch hardware	EX4200 access switch, 24 Gigabit Ethernet ports: 8 PoE ports (ge-0/0/0 through ge-0/0/7) and 16 non-PoE ports (ge-0/0/8 through ge-0/0/23)
VLAN name	default
One RADIUS server	Backend database with an address 10.0.0.100 connected to the switch at port ge-0/0/10

In this example, connect the RADIUS server to access port ge-0/0/10 on the EX4200 switch. The switch acts as the authenticator and forwards credentials from the supplicant to the user database on the RADIUS server. You must configure connectivity between the EX4200 and the RADIUS server by specifying the address of the server and configuring the secret password. This information is configured in an access profile on the switch.



NOTE: For more information about authentication, authorization, and accounting (AAA) services, see the [Junos OS System Basics Configuration Guide](#).

Configuration

CLI Quick Configuration

To quickly connect the RADIUS server to the switch, copy the following commands and paste them into the switch terminal window:

```
[edit]
set access radius-server 10.0.0.100 secret juniper
set access radius-server 10.0.0.200 secret juniper
set access profile profile1 authentication-order radius
set access profile profile1 radius authentication-server [10.0.0.100 10.0.0.200]
```

Step-by-Step Procedure

To connect the RADIUS server to the switch:

1. Define the address of the servers, and configure the secret password. The secret password on the switch must match the secret password on the server:


```
[edit]
user@switch# set access radius-server 10.0.0.100 secret juniper
user@switch# set access radius-server 10.0.0.200 secret juniper
```
2. Configure the authentication order, making **radius** the first method of authentication:


```
[edit]
user@switch# set access profile profile1 authentication-order radius
```
3. Configure a list of server IP addresses to be tried in sequential order to authenticate the supplicant:


```
[edit]
user@switch# set access profile profile1 radius authentication-server [10.0.0.100 10.0.0.200]
```

Results Display the results of the configuration:

```
user@switch> show configuration access
radius-server {
  10.0.0.100
  port 1812;
  secret "$9$qPT3ApBSrv69rvWLVb.P5"; ## SECRET-DATA
}
}
profile profile1{
  authentication-order radius;
  radius {
    authentication-server 10.0.0.100 10.0.0.200;
  }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verify That the Switch and RADIUS Server are Properly Connected on page 29](#)

Verify That the Switch and RADIUS Server are Properly Connected

Purpose	Verify that the RADIUS server is connected to the switch on the specified port.
Action	<p>Ping the RADIUS server to verify the connection between the switch and the server:</p> <pre>user@switch> ping 10.0.0.100 PING 10.0.0.100 (10.0.0.100): 56 data bytes 64 bytes from 10.93.15.218: icmp_seq=0 ttl=64 time=9.734 ms 64 bytes from 10.93.15.218: icmp_seq=1 ttl=64 time=0.228 ms</pre>
Meaning	ICMP echo request packets are sent from the switch to the target server at 10.0.0.100 to test whether the server is reachable across the IP network. ICMP echo responses are being returned from the server, verifying that the switch and the server are connected.
Related Documentation	<ul style="list-style-type: none">• Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31• Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 61• Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch• Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 67• Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 40

Configuring Server Fail Fallback (CLI Procedure)

You can use the server fail fallback feature to specify how end devices connected to the switch are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

802.1X and MAC RADIUS authentication work by using an *authenticator port access entity* (the switch) to block all traffic to and from an end device at the interface until the end device's credentials are presented and matched on the *authentication server* (a RADIUS server). When the end device has been authenticated, the switch stops blocking and opens the interface to the end device.

When you set up 802.1X or MAC RADIUS authentication on the switch, you specify a primary authentication server and one or more backup authentication servers. If the primary authentication server cannot be reached by the switch and the secondary authentication servers are also unreachable, a RADIUS server timeout occurs. Because the authentication server grants or denies access to the end devices awaiting authentication, the switch does not receive access instructions for end devices attempting access to the LAN and normal authentication cannot be completed. With server fail fallback, you can configure authentication alternatives that permit the switch to take appropriate actions toward end devices awaiting authentication or reauthentication.



NOTE: The authentication fallback method called *server-reject VLAN* provides limited access to a LAN, typically only to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials. If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is not allowed.

To configure basic server fail fallback options by using the CLI:

- Configure an interface to allow traffic to flow from a supplicant to the LAN if a RADIUS server timeout occurs (as if the end device had been successfully authenticated by a RADIUS server):

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name server-fail permit
```

- Configure an interface to prevent traffic flow from an end device to the LAN (as if the end device had failed authentication and had been rejected by the RADIUS server):

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name server-fail deny
```

- Configure an interface to move an end device to a specified VLAN if a RADIUS server timeout occurs:

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name server-fail vlan-name
```

- Configure an interface to recognize already connected end devices as reauthenticated if there is a RADIUS timeout during reauthentication (new users will be denied access):

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name server-fail use-cache
```

- Configure an interface that receives a RADIUS access-reject message from the authentication server to move end devices attempting LAN access on the interface to a specified VLAN already configured on the switch (in this case, the VLAN name is *vlan-sf*):

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name server-reject-vlan vlan-sf
```



NOTE: If an IP phone is authenticated in the server-reject VLAN, voice traffic is not allowed.

Related Documentation

- [Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to a Switch on page 54](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 22](#)
- [Monitoring 802.1X Authentication](#)
- [Understanding Server Fail Fallback and Authentication on Switches](#)

Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch

802.1x port-based network access control (PNAC) authentication on a switch provides three types of authentication to meet the access needs of your enterprise LAN:

- Authenticate the first end device (supplicant) on an authenticator port, and allow all other end devices also connecting to have access to the LAN.
- Authenticate only one end device on an authenticator port at one time.
- Authenticate multiple end devices on an authenticator port. Multiple supplicant mode is used in VoIP configurations.

This example configures a switch to use IEEE 802.1X to authenticate end devices that use three different administrative modes.

- [Requirements on page 32](#)
- [Overview and Topology on page 33](#)
- [Configuration of 802.1X to Support Multiple Supplicant Modes on page 34](#)
- [Verification on page 35](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from end devices until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for end devices (supplicants) that have permission to connect to the network.

Before you configure the ports for 802.1X authentication, be sure you have:

- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch* or *Example: Setting Up Basic Bridging and a VLAN on the QFX Series*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.



NOTE: For more about ELS, see: *Getting Started with Enhanced Layer 2 Software*

- Configured users on the authentication server.

Overview and Topology

As shown in [Figure 2 on page 33](#), the topology contains an EX4200 access switch connected to the authentication server on port ge-0/0/10. Interfaces ge-0/0/8, ge-0/0/9, and ge-0/0/11 will be configured for three different administrative modes.



NOTE: This figure also applies to QFX5100 switches.

Figure 2: Topology for Configuring Supplicant Modes

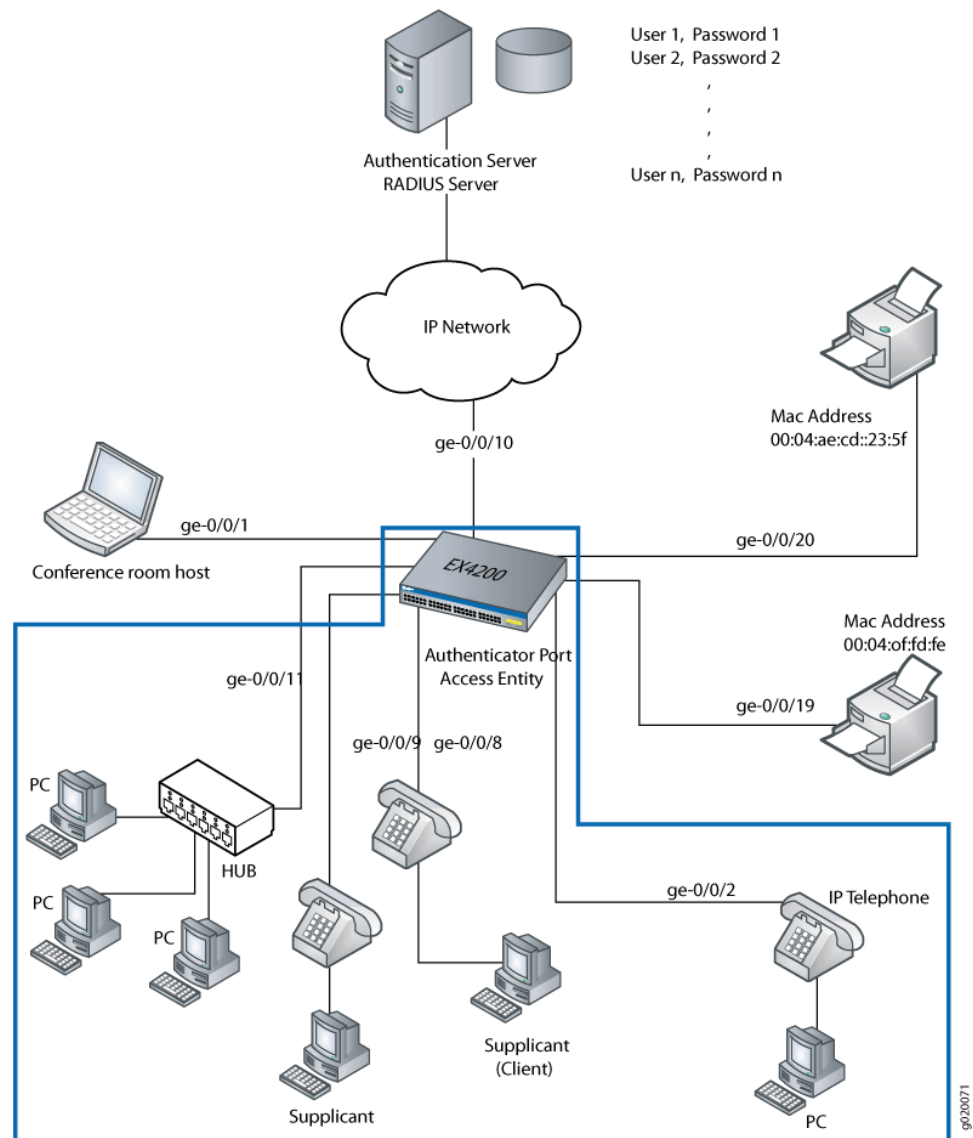


Table 6: Components of the Supplicant Mode Configuration Topology

Property	Settings
Switch hardware	EX4200 switch, 24 Gigabit Ethernet ports: 8 PoE ports (ge-0/0/0 through ge-0/0/7) and 16 non-PoE ports (ge-0/0/8 through ge-0/0/23)
Connections to Avaya phones—with integrated hub, to connect phone and desktop PC to a single port; (requires PoE)	ge-0/0/8, ge-0/0/9, and ge-0/0/11

To configure the administrative modes to support supplicants in different areas of the Enterprise network:

- Configure access port ge-0/0/8 for single supplicant mode authentication.
- Configure access port ge-0/0/9 for single secure supplicant mode authentication.
- Configure access port ge-0/0/11 for multiple supplicant mode authentication.

Single supplicant mode authenticates only the first end device that connects to an authenticator port. All other end devices connecting to the authenticator port after the first has connected successfully, whether they are 802.1X-enabled or not, are permitted access to the port without further authentication. If the first authenticated end device logs out, all other end devices are locked out until an end device authenticates.

Single-secure supplicant mode authenticates only one end device to connect to an authenticator port. No other end device can connect to the authenticator port until the first logs out.

Multiple supplicant mode authenticates multiple end devices individually on one authenticator port. If you configure a maximum number of devices that can be connected to a port through port security, the lesser of the configured values is used to determine the maximum number of end devices allowed per port.

Configuration of 802.1X to Support Multiple Supplicant Modes

CLI Quick Configuration To quickly configure the ports with different 802.1X authentication modes, copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator interface ge-0/0/8 supplicant single
set protocols dot1x authenticator interface ge-0/0/9 supplicant single-secure
set protocols dot1x authenticator interface ge-0/0/11 supplicant multiple
```

Step-by-Step Procedure Configure the administrative mode on the interfaces:

1. Configure the supplicant mode as single on interface ge-0/0/8:

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/8 supplicant single
```
2. Configure the supplicant mode as single secure on interface ge-0/0/9:

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/9 supplicant single-secure
```
3. Configure multiple supplicant mode on interface ge-0/0/11:

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/11 supplicant multiple
```

Results

Check the results of the configuration:

```
[edit]
user@access-switch> show configuration
protocols {
  dot1x {
    authenticator {
      interface {
        ge-0/0/8.0 {
          supplicant single;
        }
        ge-0/0/9.0 {
          supplicant single-secure;
        }
        ge-0/0/11.0 {
          supplicant multiple;
        }
      }
    }
  }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying the 802.1X Configuration on page 35](#)

Verifying the 802.1X Configuration

Purpose Verify the 802.1X configuration on interfaces ge-0/0/8, ge-0/0/9, and ge-0/0/5.

Action Verify the 802.1X configuration by issuing the operational mode command **show dot1x interface**:

```
user@switch> show dot1x interface ge-0/0/8.0 detail
ge-0/0/8.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
```

```
user@switch> show dot1x interface ge-0/0/9.0 detail
ge-0/0/9.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single-Secure
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 0
```

```
user@switch> show dot1x interface ge-0/0/11.0 detail
ge-0/0/11.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 0
```

Meaning The **Supplicant mode** output field displays the configured administrative mode for each interface. Interface ge-0/0/8.0 displays **Single** supplicant mode. Interface ge-0/0/9.0

displays **Single Secure** supplicant mode. Interface ge-0/0/11.0 displays **Multiple** supplicant mode.

Related Documentation

- [Controlling Authentication Session Timeouts \(CLI Procedure\) on page 74](#)
- [Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25](#)
- [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 61](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 67](#)
- [Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 40](#)
- [Understanding Authentication on Switches](#)

Understanding 802.1X and VSAs on Switches

Juniper Networks Ethernet Switches support the configuration of RADIUS server attributes specific to Juniper Networks. These attributes are known as vendor-specific attributes (VSAs) and are described in RFC 2138, *Remote Authentication Dial In User Service* (RADIUS). Through VSAs, you can configure port-filtering attributes on the RADIUS server. VSAs are clear text fields sent from the RADIUS server to the switch as a result of the success or failure of 802.1X authentication. The 802.1X authentication prevents unauthorized user access by blocking a supplicant at the port until the supplicant is authenticated by the RADIUS server. The VSA attributes are interpreted by the switch during authentication, after which the switch takes appropriate actions. Implementing port-filtering attributes with 802.1X authentication on the RADIUS server provides a central location for controlling LAN access for supplicants.

These port-filtering attributes specific to Juniper Networks are encapsulated in a RADIUS server VSA with the vendor ID set to the Juniper Networks ID number, 2636.

Besides configuring port-filtering attributes through VSAs, you can apply a port firewall filter that has already been configured on the switch directly to the RADIUS server. Like port-filtering attributes, the filter is applied during the 802.1X authentication process, and its actions are applied at the switch port. Adding a port firewall filter to a RADIUS server eliminates the need to add the filter to multiple ports and switches. For more information, see [“Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on a Switch” on page 43](#).

VSAs are only supported for 802.1X single-supplicant configurations and multiple-supplicant configurations.

Related Documentation

- [Understanding Authentication on Switches](#)
- [Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31](#)
- [Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 40](#)

- [Configuring Firewall Filters \(CLI Procedure\)](#)
- [VSA Match Conditions and Actions on page 38](#)

VSA Match Conditions and Actions

Devices support the configuration of RADIUS server attributes specific to Juniper Networks. These attributes are known as vendor-specific attributes (VSAs). They are configured on RADIUS servers and work in combination with 802.1X authentication. Using VSAs, you can apply port firewall filter attributes as a subset of match conditions and actions sent from the RADIUS server to the switch as a result of successful 802.1X authentication.

Each term in a VSA configured through the RADIUS server consists of *match conditions* and an *action*. Match conditions are the values or fields that the packet must contain. You can define single, multiple, or no match conditions. If no match conditions are specified for the term, the packet is accepted by default. The action is the action that the switch takes if a packet matches the match conditions for the specific term. Allowed actions are to accept a packet or to discard a packet.

The following guidelines apply when you specify match conditions and actions for VSAs:

- Both **match** and **action** statements are mandatory.
- Any or all options (separated by commas) may be included in each **match** and **action** statement.
- Fields separated by commas will be ANDed if they are of a different type. The same types cannot be repeated.
- For OR cases (for example, match 10.1.1.0/24 OR 11.1.1.0/24), apply multiple VSAs to the 802.1X supplicant.
- In order for the **forwarding-class** option to be applied, the forwarding class must be configured on the switch. If it is not configured on the switch, this option is ignored.

[Table 7 on page 38](#) describes the match conditions you can specify when configuring a VSA using the **match** command on the RADIUS server. The string that defines a match condition is called a *match statement*.

Table 7: Match Conditions

Option	Description
<code>destination-mac mac-address</code>	Destination media access control (MAC) address of the packet.
<code>source-vlan source-vlan</code>	Name of the source VLAN.
<code>source-dot1q-tag tag</code>	Tag value in the 802.1Q header, in the range 0 through 4095.
<code>destination-ip ip-address</code>	Address of the final destination node.

Table 7: Match Conditions (*continued*)

Option	Description
ip-protocol <i>protocol-id</i>	<p>IPv4 protocol value. In place of the numeric value, you can specify one of the following text synonyms:</p> <p>ah, egp (8), esp (50), gre (47), icmp (1), igmp (2), ipip (4), ipv6 (41), ospf (89), pim (103), rsvp (46), tcp (6), or udp (17)</p>
source-port <i>port</i>	<p>TCP or User Datagram Protocol (UDP) source port field. Normally, you specify this match statement in conjunction with the ip-protocol match statement to determine which protocol is being used on the port. In place of the numeric field, you can specify one of the text options listed under destination-port.</p>
destination-port <i>port</i>	<p>TCP or UDP destination port field. Normally, you specify this match in conjunction with the ip-protocol match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify one of the following text synonyms (the port numbers are also listed):</p> <p>afs (1483), bgp (179), biff (512), bootpc (68), bootps (67), cvspserver (2401), cmd (514), dhcp (67), domain (53), eklogin (2105), ekshell (2106), exec (512), finger (79), ftp (21), ftp-data (20), http (80), https (443), ident (113), imap (143), kerberos-sec (88), klogin (543), kpasswd (761), krb-prop (754), krbupdate (760), kshell (544), ldap (389), login (513), mobileip-agent (434), mobileip-mn (435), msdp (639), netbios-dgm (138), netbios-ns (137), netbios-ssn (139), nfsd (2049), nntp (119), ntalk (518), ntp (123), pop3 (110), pptp (1723), printer (515), radacct (1813), radius (1812), rip (520), rkinit (2108), smtp (25), snmp (161), snmptrap (162), snpp (444), socks (1080), ssh (22), sunrpc (111), syslog (514), telnet (23), tacacs-ds (65), talk (517), tftp (69), timed (525), who (513), xmcp (177), zephyr-clt (2103), zephyr-hm (2104)</p>

When you define one or more terms that specify the filtering criteria, you also define the action to take if the packet matches all criteria. [Table 8 on page 39](#) shows the actions that you can specify in a term.

Table 8: Actions for VSAs

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

Related Documentation • [Filtering 802.1X Suplicants By Using RADIUS Server Attributes on page 40](#)

- [Understanding 802.1X and VSAs on Switches on page 37](#)
- [Understanding VSAs on page 219](#)

Filtering 802.1X Supplicants By Using RADIUS Server Attributes

There are two ways to configure the RADIUS server with port firewall filters:

- Include a match statement and corresponding action in the **Juniper-Firewall-Filter** attribute. The **Juniper-Firewall-Filter** attribute is a vendor-specific attribute (VSA) in the Juniper dictionary on the RADIUS server. Use this attribute to configure simple filter conditions for authenticated users. Nothing needs to be configured on the switch; all of the configuration is on the RADIUS server.
- Apply a local firewall filter to users authenticated through the RADIUS server. Use this method for more complex filters. The firewall filter must be configured on each switch.



NOTE: If the firewall filter configuration is modified after users are authenticated using the 802.1X authentication, then the established 802.1X authentication session must be terminated and re-established for the firewall filter configuration changes to take effect.

This topic describes using FreeRADIUS software to configure VSAs. For specifics on configuring your server, consult the AAA documentation that was included with your server.

This topic includes the following tasks:

1. [Configuring Match Statements on the RADIUS Server on page 40](#)
2. [Applying a Port Firewall Filter from the RADIUS Server on page 42](#)

Configuring Match Statements on the RADIUS Server

You can configure simple filter conditions by using the **Juniper-Switching-Filter** attribute in the Juniper dictionary on the RADIUS server. These filters are then sent to a switch whenever a new user is authenticated successfully. The filters are created and applied on all switches that authenticate users through that RADIUS server without the need to configure anything on each individual switch.

To configure the **Juniper-Switching-Filter** attribute, enter one or more match conditions and a resulting action using the CLI for the RADIUS server. Enter the match statement plus an action statement enclosed within quotation marks (" ") using the following syntax:

```
match <destination-mac mac-address> <source-vlan vlan-name> <source-dot1q-tag
tag> <destination-ip ip-address> <ip-protocol protocol-id> <source-port port>
<destination-port port>
}
action [allow | deny] <forwarding-class class-of-service> <loss-priority (low | medium |
high)>
}
```

See [“VSA Match Conditions and Actions” on page 38](#) for definitions of match statement options.

To configure match conditions on the RADIUS server:

1. Verify that the Juniper dictionary is loaded on your RADIUS server and includes the filtering attribute **Juniper-Switching-Filter**, attribute ID 48:

```
[root@freeradius]# cat /usr/local/share/freeradius/dictionary.juniper

# dictionary.juniper
#
# Version:      $Id: dictionary.juniper,v 1.2.6.1 2005/11/30 22:17:25 a1and
Exp
$
#  VENDOR      Juniper      2636
BEGIN-VENDOR   Juniper
ATTRIBUTE      Juniper-Local-User-Name      1      string
ATTRIBUTE      Juniper-Allow-Commands       2      string
ATTRIBUTE      Juniper-Deny-Commands        3      string
ATTRIBUTE      Juniper-Allow-Configuration  4      string
ATTRIBUTE      Juniper-Deny-Configuration   5      string
ATTRIBUTE      Juniper-Switching-Filter      48     string
<-
```

2. Enter the match conditions and actions. For example:

- To deny authentication based on the 802.1Q tag (here, the 802.1Q tag is **10**):

```
[root@freeradius]#
cd /usr/local/etc/raddb
vi users
```

For each relevant user, add the **Juniper-Switching-Filter** attribute:

```
Juniper-Switching-Filter = "Match Source-dot1q-tag 10 Action deny"
```

- To deny access based on a destination IP address:

```
[root@freeradius]# cd /usr/local/etc/raddb
vi users
```

For each relevant user, add the **Juniper-Switching-Filter** attribute:

```
Juniper-Switching-Filter = "Match Destination-ip 192.168.1.0/31 Action deny"
```

- To set the packet loss priority (PLP) to **high** based on a destination MAC address and the IP protocol:

```
[root@freeradius]# cd /usr/local/etc/raddb
vi users
```

For each relevant user, add the **Juniper-Switching-Filter** attribute:

```
Juniper-Switching-Filter = "Match Destination-mac 00:04:0f:fd:ac:fe, Ip-protocol 2,
forwarding-class high, Action loss-priority high"
```



NOTE: For the **forwarding-class** option to be applied, the forwarding class must be configured on the switch. If it is not configured on the switch, this option is ignored. You must specify both the forwarding class and the packet loss priority.

3. Stop and restart the RADIUS process to activate the configuration.

Applying a Port Firewall Filter from the RADIUS Server

You can apply a firewall filter to user policies on the RADIUS server. The RADIUS server can then specify the firewall filters that are to be applied to each user that requests to authenticate. Use this method when the firewall filter has more extensive conditions or you want to use different conditions for the same filter on different switches. The firewall filters must be configured on each switch.

For more information about firewall filters, see *Firewall Filters for EX Series Switches Overview* or *Overview of Firewall Filters*.

To apply a port firewall filter centrally from the RADIUS server:



NOTE: If port firewall filters are also configured locally for the interface, then VSAs take precedence if they conflict with the filters. If the VSAs and the local port firewall filters do not conflict, they are merged.

1. Create the firewall filter on the local switch. In this example, the filter is called **filter1**.
2. Open the **users** file on the RADIUS server:

```
[root@freeradius]#  
cd /usr/local/pool/raddb  
vi users
```

3. For each relevant user, add the filter (here, the filter ID is **filter1**):

```
Filter-Id = "filter1"
```



NOTE: Multiple filters are not supported on a single interface. However, you can support multiple filters for multiple users that are connected to the switch on the same interface by configuring a single filter with policies for each of those users.

4. Stop and restart the RADIUS process to activate the configuration.

Related Documentation

- [Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on a Switch on page 43](#)
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 22](#)
- [Understanding 802.1X and VSAs on Switches on page 37](#)

Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on a Switch

You can use RADIUS server attributes and a port firewall filter to centrally apply terms to multiple supplicants (end devices) connected to a switch in your enterprise. Terms are applied after a device is successfully authenticated through 802.1X. If the firewall filter configuration is modified after end devices are authenticated using the 802.1X authentication, then the established 802.1X authentication session must be terminated and re-established for the firewall filter changes to take effect.

Switches support port firewall filters. Port firewall filters are configured on a single switch, but in order for them to operate throughout an enterprise, they have to be configured on multiple switches. To reduce the need to configure the same port firewall filter on multiple switches, you can instead apply the filter centrally on the RADIUS server using RADIUS server attributes.

The following example uses FreeRADIUS to apply a port firewall filter on a RADIUS server. For specifics on configuring your server, consult the documentation that was included with your RADIUS server.

This example describes how to configure a port firewall filter with terms, create counters to count packets for the supplicants, apply the filter to user profiles on the RADIUS server, and display the counters to verify the configuration:

- [Requirements on page 43](#)
- [Overview and Topology on page 44](#)
- [Configuring the Port Firewall Filter and Counters on page 46](#)
- [Applying the Port Firewall Filter to the Supplicant User Profiles on the RADIUS Server on page 48](#)
- [Verification on page 48](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.3 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Set up a connection between the switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to a Switch” on page 25](#).
- Configured 802.1X authentication on the switch, with the authentication mode for interface `ge-0/0/2` set to **multiple**. See [“Configuring 802.1X Interface Settings \(CLI Procedure\)” on page 22](#) and [“Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch” on page 31](#).
- Configured users on the RADIUS authentication server (in this example, the user profiles for Supplicant 1 and Supplicant 2 in the topology are modified on the RADIUS server).

Overview and Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, you can apply a single port firewall filter configured through the Junos OS CLI on the switch to any number of end devices (supplicants) on one interface by adding the filter centrally to the RADIUS server. Only a single filter can be applied to an interface; however, the filter can contain multiple terms for separate end devices.

For more information about firewall filters, see *Firewall Filters for EX Series Switches Overview* or *Overview of Firewall Filters*.

RADIUS server attributes are applied to end devices after the devices are successfully authenticated using 802.1X. To authenticate an end device, the switch forwards the end device's credentials to the RADIUS server. The RADIUS server matches the credentials against preconfigured information about the supplicant located in the supplicant's user profile on the RADIUS server. If a match is found, the RADIUS server instructs the switch to open an interface to the end device. Traffic then flows from and to the end device on the LAN. Further instructions configured in the port firewall filter and added to the end device's user profile using a RADIUS server attribute further define the access that the end device is granted. Filtering terms configured in the port firewall filter are applied to the end device after 802.1X authentication is complete.



NOTE: If you modify the port firewall filter after an end device is successfully authenticated using 802.1X, you must terminate and re-establish the 802.1X authentication session for the firewall filter configuration changes to be effective.

[Figure 3 on page 45](#) shows the topology used for this example. The RADIUS server is connected to an EX4200 switch on access port `ge-0/0/10`. Two end devices (supplicants) are accessing the LAN on interface `ge-0/0/2`. Supplicant 1 has the MAC address `00:50:8b:6f:60:3a`. Supplicant 2 has the MAC address `00:50:8b:6f:60:3b`.



NOTE: This figure also applies to QFX5100 switches.

Figure 3: Topology for Firewall Filter and RADIUS Server Attributes Configuration

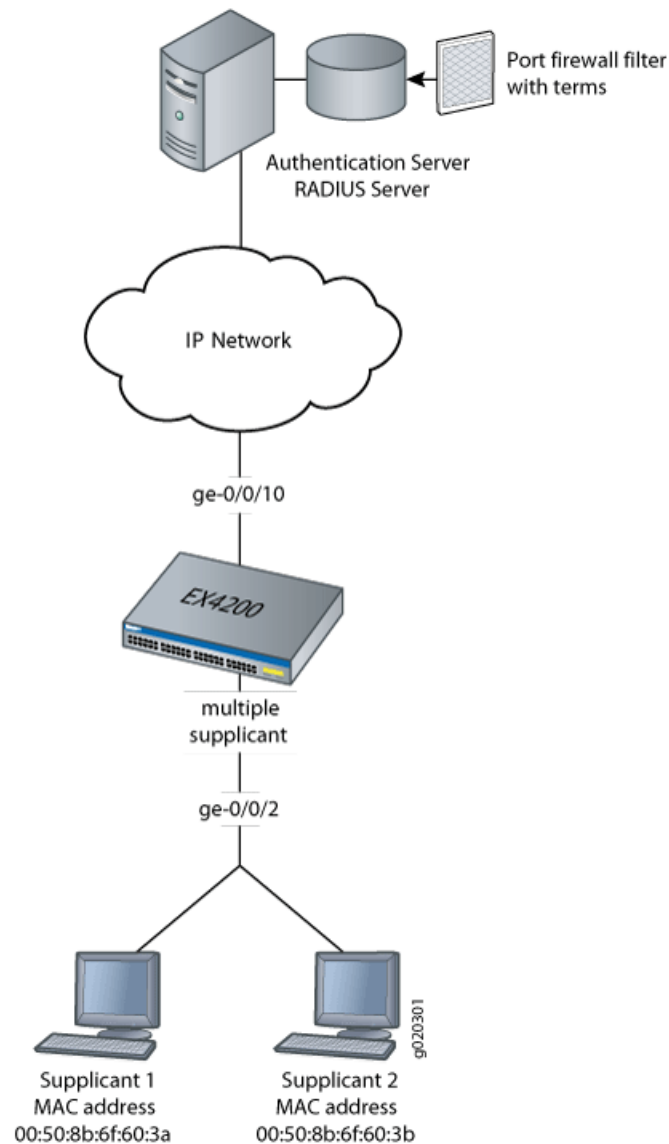


Table 9 on page 45 describes the components in this topology.

Table 9: Components of the Firewall Filter and RADIUS Server Attributes Topology

Property	Settings
Switch hardware	EX4200 access switch, 24 Gigabit Ethernet ports, 8 PoE ports.
One RADIUS server	Backend database with the address 10.0.0.100 connected to the switch at port ge-0/0/10.
802.1X supplicants connected to the switch on interface ge-0/0/2	<ul style="list-style-type: none"> • Supplicant 1 has MAC address 00:50:8b:6f:60:3a. • Supplicant 2 has MAC address 00:50:8b:6f:60:3b.

Table 9: Components of the Firewall Filter and RADIUS Server Attributes Topology (*continued*)

Property	Settings
Port firewall filter to be applied on the RADIUS server	filter1
Counters	counter1 counts packets from Supplicant 1, and counter2 counts packets from Supplicant 2.
Policer	policer p1
User profiles on the RADIUS server	<ul style="list-style-type: none"> Supplicant 1 has the user profile supplicant1. Supplicant 2 has the user profile supplicant2.

In this example, you configure a port firewall filter named **filter1**. The filter contains terms that will be applied to the end devices based on the MAC addresses of the end devices. When you configure the filter, you also configure the counters **counter1** and **counter2**. Packets from each end device are counted, which helps you verify that the configuration is working. Policer **policer p1** limits the traffic rate based on the values for **exceeding** and **discard** parameters. Then, you check to see that the RADIUS server attribute is available on the RADIUS server and apply the filter to the user profiles of each end device on the RADIUS server. Finally, you verify the configuration by displaying output for the two counters.



NOTE: For more information about authentication, authorization, and accounting (AAA) services, see the [Junos OS System Basics Configuration Guide](#).

Configuring the Port Firewall Filter and Counters

CLI Quick Configuration To quickly configure a port firewall filter with terms for Supplicant 1 and Supplicant 2 and create parallel counters for each supplicant, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter filter1 term supplicant1 from source-mac-address 00:50:8b:6f:60:3a
set firewall family ethernet-switching filter filter1 term supplicant2 from source-mac-address 00:50:8b:6f:60:3b
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall policer p1 then discard
set firewall family ethernet-switching filter filter1 term supplicant1 then count counter1
set firewall family ethernet-switching filter filter1 term supplicant1 then policer p1
set firewall family ethernet-switching filter filter1 term supplicant2 then count counter2
```

Step-by-Step Procedure To configure a port firewall filter and counters on the switch:

1. Configure a port firewall filter (here, **filter1**) with terms for each end device based on the MAC address of each end device:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term supplicant1 from source-mac-address 00:50:8b:6f:60:3a
user@switch# set filter filter1 term supplicant2 from source-mac-address 00:50:8b:6f:60:3b
```

2. Set policer definition:

```
user@switch# show policer p1 |display set
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall policer p1 then discard
```

3. Create two counters that will count packets for each end device and a policer that limits the traffic rate:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term supplicant1 then count counter1
user@switch# set filter filter1 term supplicant1 then policer p1
user@switch# set filter filter1 term supplicant2 then count counter2
```

Results Display the results of the configuration:

```
user@switch> show configuration
firewall {
  family ethernet-switching {
    filter filter1 {
      term supplicant1 {
        from {
          source-mac-address {
            00:50:8b:6f:60:3a;
          }
        }
        then count counter1;
        then policer p1;
      }
      term supplicant2 {
        from {
          source-mac-address {
            00:50:8b:6f:60:3b;
          }
        }
        then count counter2;
      }
    }
  }
}
policer p1 {
  if-exceeding {
    bandwidth-limit 1m;
    burst-size-limit 1k;
  }
  then discard;
}
```

Applying the Port Firewall Filter to the Supplicant User Profiles on the RADIUS Server

Step-by-Step Procedure To verify that the RADIUS server attribute **Filter-ID** is on the RADIUS server and to apply the filter to the user profiles:

1. Display the dictionary **dictionary.rfc2865** on the RADIUS server, and verify that the attribute **Filter-ID** is in the dictionary:

```
[root@freeradius]# cd usr/share/freeradius/dictionary.rfc2865
```

2. Close the dictionary file.

3. Display the local user profiles of the end devices to which you want to apply the filter (here, the user profiles are called **supplicant1** and **supplicant2**):

```
[root@freeradius]# cat /usr/local/etc/raddb/users
```

The output shows:

```
supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
    Tunnel-Type = VLAN,
    Tunnel-Medium-Type = IEEE-802,
    Tunnel-Private-Group-Id = "1005"
```

```
supplicant2 Auth-Type := EAP, User-Password == "supplicant2"
    Tunnel-Type = VLAN,
    Tunnel-Medium-Type = IEEE-802,
    Tunnel-Private-Group-Id = "1005"
```

4. Apply the filter to both user profiles by adding the line **Filter-Id = "filter1"** to each profile, and then close the file:

```
[root@freeradius]# cat /usr/local/etc/raddb/users
```

After you paste the line into the files, the files look like this:

```
supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
    Tunnel-Type = VLAN,
    Tunnel-Medium-Type = IEEE-802,
    Tunnel-Private-Group-Id = "1005",
    Filter-Id = "filter1"
```

```
supplicant2 Auth-Type := EAP, User-Password == "supplicant2"
    Tunnel-Type = VLAN,
    Tunnel-Medium-Type = IEEE-802,
    Tunnel-Private-Group-Id = "1005",
    Filter-Id = "filter1"
```

Verification

Verifying That the Filter Has Been Applied to the Supplicants

Purpose After the end devices are authenticated, verify that the filter has been configured on the switch and added to each end device's user profile on the RADIUS server:

Action Display information about firewall filter **filter1**:

```
user@switch> show firewall filter filter1
Filter: filter1
Counters:
Name                               Bytes      Packets
counter1                           128         2
counter2                            64         1
```

Meaning The output of the command **show firewall filter filter1** displays **counter1** and **counter2**. Packets from Supplicant 1 are counted using **counter1**, and packets from Supplicant 2 are counted using **counter2**. The output displays packets incrementing for both counters. The filter has been applied to both end devices.

- Related Documentation**
- [Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31](#)
 - [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches](#)
 - [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 67](#)
 - [Understanding Authentication on Switches](#)
 - [Understanding 802.1X and VSAs on Switches on page 37](#)

Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication



NOTE: This example uses Junos OS for EX Series and QFX5100 switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

Firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server. The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.

This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

- [Requirements on page 50](#)
- [Overview and Topology on page 50](#)
- [Configuration on page 52](#)
- [Verification on page 54](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 13.2 or later for EX Series switches
- One EX4300 switch
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

- Set up a connection between the switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to a Switch” on page 25](#).
- Configured 802.1X authentication on the switch, with the authentication mode for the interface ge-0/0/2 set to **multiple**. See [“Configuring 802.1X Interface Settings \(CLI Procedure\)” on page 22](#) and [“Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch” on page 31](#).
- Configured users on the RADIUS authentication server.

Overview and Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines the interface firewall filter with the user policies sent to the switch from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

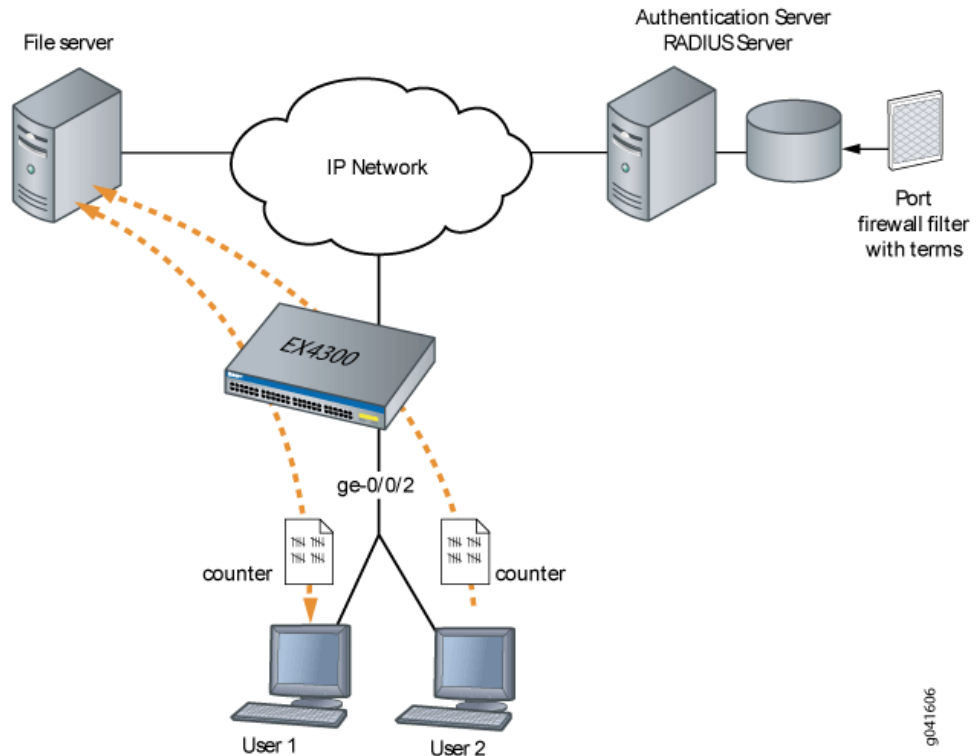
When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in [Figure 4 on page 51](#), when User 1 is authenticated by

the EX Series switch, the system adds a term to the firewall filter **dynamic-filter-example**. When User 2 is authenticated, another term is added to the firewall filter, and so on.



NOTE: This figure also applies to QFX5100 switches.

Figure 4: Conceptual Model: Dynamic Filter Updated for Each New User



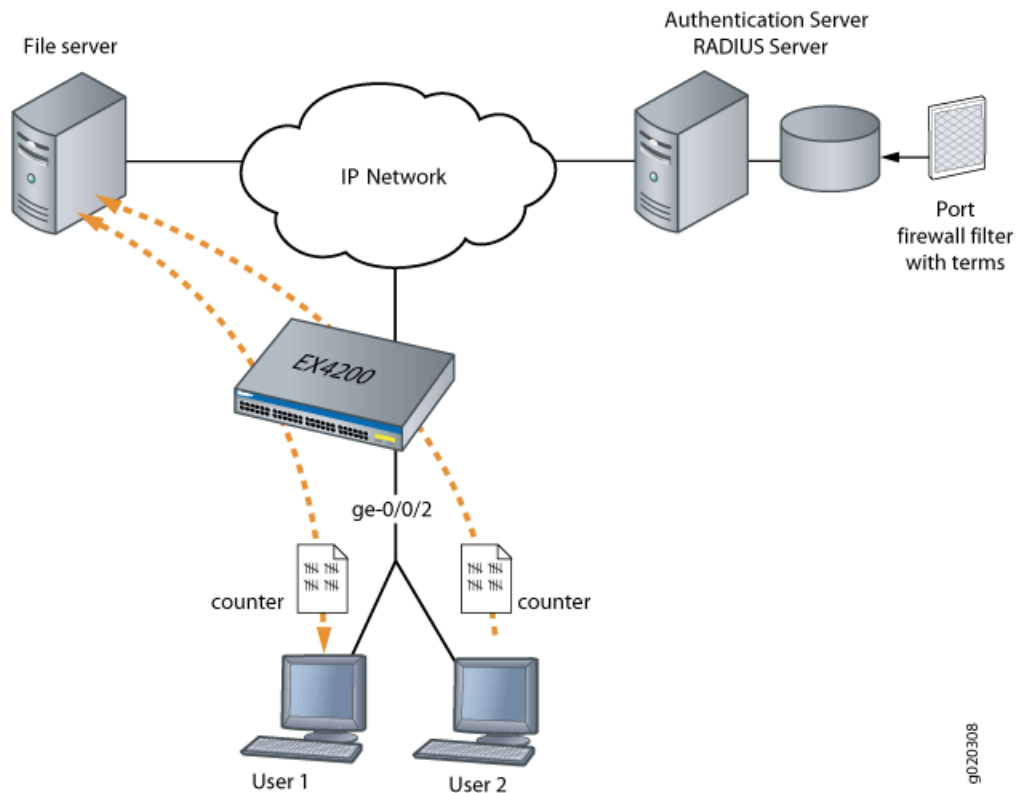
This is a conceptual model of the internal process—you cannot access or view the dynamic filter.



NOTE: If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface ge-0/0/2 to the file server, which is located on subnet 192.0.2.16/28, and set policer definitions to rate-limit the traffic. [Figure 5 on page 52](#) shows the network topology for this example.

Figure 5: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server



Configuration

Configuring Firewall Filters on Interfaces with Multiple Supplicants

CLI Quick Configuration

To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter filter1 term term1 from ip-destination-address 192.0.2.16/28
set firewall family ethernet-switching filter filter1 term term2 from ip-destination-address 192.0.2.16/28
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1500
set firewall policer p1 then discard
set firewall family ethernet-switching filter filter1 term term1 then count counter1
set firewall family ethernet-switching filter filter1 term term2 then policer p1
```

Step-by-Step Procedure

To configure firewall filters on an interface enabled for multiple supplicants:

1. Set the policer definition:

```
user@switch# show policer p1 |display set
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1500
set firewall policer p1 then discard
```

2. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term term1 from ip-destination-address 192.0.2.16/28
user@switch# set filter filter1 term term2 from ip-destination-address 192.0.2.16/28
user@switch# set filter filter1 term term1 then count counter1
user@switch# set filter filter1 term term2 then policer p1
```

Results Check the results of the configuration:

```
user@switch> show configuration
```

```
firewall {
  family ethernet-switching {
    filter filter1 {
      term term1 {
        from {
          ip-destination-address {
            192.0.2.16/28;
          }
        }
        then count counter1;
      }
      term term2 {
        from {
          ip-destination-address {
            192.0.2.16/28;
          }
        }
        then policer p1;
      }
    }
  }
  policer p1 {
    if-exceeding {
      bandwidth-limit 1m;
      burst-size-limit 1500;
    }
    then discard;
  }
}
protocols {
  dot1x {
    authenticator
    interface ge-0/0/2 {
      supplicant multiple;
    }
  }
}
```

Verification

Verifying Firewall Filters on Interfaces with Multiple Supplicants

Purpose	Verify that firewall filters are functioning on the interface with multiple supplicants.
Action	<ol style="list-style-type: none">1. Check the results with one user authenticated on the interface. In this case, User 1 is authenticated on ge-0/0/2: <pre>user@switch> show dot1x firewall Filter: dot1x_ge-0/0/2 Counters counter1_dot1x_ge-0/0/2_user1 100</pre>2. When a second user, User 2, is authenticated on the same interface, ge-0/0/2, you can verify that the filter includes the results for both of the users authenticated on the interface: <pre>user@switch> show dot1x firewall Filter: dot1x-filter-ge-0/0/0 Counters counter1_dot1x_ge-0/0/2_user1 100 counter1_dot1x_ge-0/0/2_user2 400</pre>
Meaning	The results displayed by the show dot1x firewall command output reflect the dynamic filter created with the authentication of each new user. User 1 accessed the file server located at the specified destination address 100 times, while User 2 accessed the same file server 400 times.
Related Documentation	<ul style="list-style-type: none">• Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on a Switch on page 43• Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches• Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 40

Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to a Switch

Server fail fallback allows you to specify how 802.1X supplicants connected to the switch are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

You use 802.1X to control network access. Only users and devices (supplicants) providing credentials that have been verified against a user database are allowed access to the network. You use a RADIUS server as the user database.

This example describes how to configure an interface to move a supplicant to a VLAN in the event of a RADIUS server timeout:

- [Requirements on page 55](#)
- [Overview and Topology on page 55](#)
- [Configuration on page 57](#)
- [Verification on page 58](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.3 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch* or *Example: Setting Up Basic Bridging and a VLAN on the QFX Series*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.



NOTE: For more about ELS, see: *Getting Started with Enhanced Layer 2 Software*

- Set up a connection between the switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to a Switch” on page 25](#).
- Disable firewall filters on the interface. Firewall filters interfere with server fail fallback operation.
- Configured users on the authentication server.

Overview and Topology

A RADIUS server timeout occurs if no authentication RADIUS servers are reachable when a supplicant logs in and attempts to access the LAN. Using server fail fallback, configure alternative options for supplicants attempting LAN access. You can configure the switch

to accept or deny access to supplicants or to maintain the access already granted towards supplicants before the RADIUS server timeout. Additionally, you can configure the switch to move supplicants to a specific VLAN if a RADIUS timeout occurs or if the RADIUS server sends an EAP Access-Reject message.

Figure 6 on page 56 shows the topology used for this example. The RADIUS server is connected to the EX4200 switch on access port **ge-0/0/10**. The switch acts as the authenticator port access entity (PAE) and forwards credentials from the supplicant to the user database on the RADIUS server. The switch blocks all traffic and acts as a control gate until the supplicant is authenticated by the authentication server. A supplicant is connected to the switch through interface **ge-0/0/1**.



NOTE: This figure also applies to QFX5100 switches.

Figure 6: Topology for Configuration

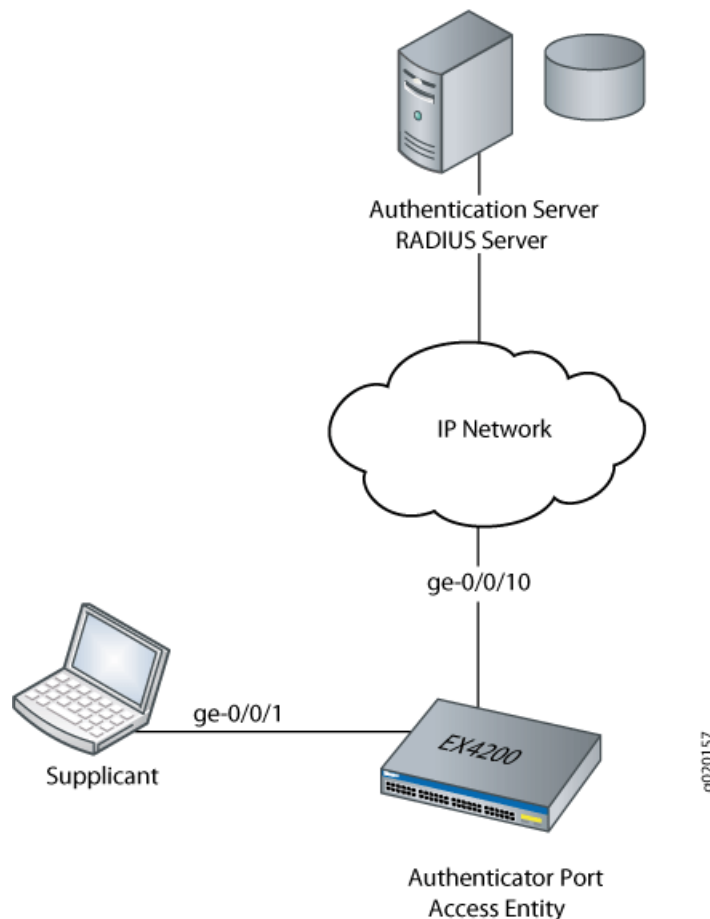


Table 10 on page 57 describes the components in this topology.

Table 10: Components of the Topology

Property	Settings
Switch hardware	EX4200 access switch, 24 Gigabit Ethernet ports: 8 PoE ports.
VLAN names	default VLAN vlan-sf VLAN
Supplicant	Supplicant attempting access on interface ge-0/0/1
One RADIUS server	Backend database with an address of 10.0.0.100 connected to the switch at port ge-0/0/10

In this example, configure interface **ge-0/0/1** to move a supplicant attempting access to the LAN during a RADIUS timeout to another VLAN. A RADIUS timeout prevents the normal exchange of EAP messages that carry information from the RADIUS server to the switch and permit the authentication of a supplicant. The **default** VLAN is configured on interface **ge-0/0/1**. When a RADIUS timeout occurs, supplicants on the interface will be moved from the **default** VLAN to the VLAN named **vlan-sf**.



NOTE: For more information about authentication, authorization, and accounting (AAA) services, see [Junos OS System Basics Configuration Guide](#).

Configuration

CLI Quick Configuration To quickly configure server fail fallback on the switch, copy the following commands and paste them into the switch terminal window:

```
[edit protocols dot1x authenticator]
set interface ge-0/0/1 server-fail vlan-name vlan-sf
```

Step-by-Step Procedure To configure an interface to divert supplicants to a specific VLAN when a RADIUS timeout occurs (here, the VLAN is **vlan-sf**):

1. Define the VLAN to which supplicants are diverted:

```
[edit protocols dot1x authenticator]
user@switch# set interface ge-0/0/1 server-fail vlan-name vlan-sf
```

Results Display the results of the configuration:

```
user@switch> show configuration
interfaces {
  ge-0/0/1 {
    unit 0 {
      family ethernet-switching {
        vlan {
          members default;
        }
      }
    }
  }
}
```

```
protocols {
  dot1x {
    authenticator {
      authentication-profile-name profile52;
    }
    interface {
      ge-0/0/1.0 {
        server-fail vlan-name vlan-sf;
      }
    }
  }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying That the Supplicants Are Moved to an Alternative VLAN During a RADIUS Timeout](#) on page 58

Verifying That the Supplicants Are Moved to an Alternative VLAN During a RADIUS Timeout

Purpose Verify that the interface moves supplicants to an alternative VLAN during a RADIUS timeout.



NOTE: On switches running Junos OS for EX Series with support for ELS, the output for the `show vlans` command will contain additional information. If your switch runs software that supports ELS, see `show vlans`. For ELS details, see *Getting Started with Enhanced Layer 2 Software*

Action Display the VLANs configured on the switch; the interface **ge-0/0/1.0** is a member of the **default** VLAN:

```
user@switch> show vlans
Name      Tag      Interfaces
default
          ge-0/0/0.0, ge-0/0/1.0*, ge-0/0/5.0*, ge-0/0/10.0,
          ge-0/0/12.0*, ge-0/0/14.0*, ge-0/0/15.0, ge-0/0/20.0
v2         77
          None
vlan-sf    50
          None
mgmt
          me0.0*
```

Display 802.1X protocol information on the switch to view supplicants that are authenticated on interface **ge-0/0/1.0**:

```
user@switch> show dot1x interface brief
802.1X Information:
Interface  Role      State      MAC address  User
ge-0/0/1.0  Authenticator  Authenticated  00:00:00:00:00:01  abc
ge-0/0/10.0 Authenticator  Initialize
ge-0/0/14.0 Authenticator  Connecting
ge-0/0/15.0 Authenticator  Initialize
ge-0/0/20.0 Authenticator  Initialize
```

A RADIUS server timeout occurs. Display the Ethernet switching table to show that the supplicant with the MAC address **00:00:00:00:00:01** previously accessing the LAN through the **default** VLAN is now being learned on the VLAN named **vlan-sf**:

```
user@switch> show ethernet-switching table
Ethernet-switching table: 3 entries, 1 learned
VLAN      MAC address      Type      Age  Interfaces
v1         *                 Flood     -    All-members
vlan-sf    00:00:00:00:00:01 Learn      1:07 ge-0/0/1.0
default   *                 Flood     -    All-members
```

Display 802.1X protocol information to show that interface **ge-0/0/1.0** is connecting and will open LAN access to supplicants:

```
user@switch> show dot1x interface brief
802.1X Information:
Interface  Role      State      MAC address  User
ge-0/0/1.0  Authenticator  Connecting
ge-0/0/10.0 Authenticator  Initialize
ge-0/0/14.0 Authenticator  Connecting
ge-0/0/15.0 Authenticator  Initialize
ge-0/0/20.0 Authenticator  Initialize
```

Meaning The command **show vlans** displays interface **ge-0/0/1.0** as a member of the **default** VLAN. The command **show dot1x interface brief** shows that a supplicant (**abc**) is authenticated on interface **ge-0/0/1.0** and has the MAC address **00:00:00:00:00:01**. A RADIUS server timeout occurs, and the authentication server cannot be reached by the

switch. The command **show-ethernet-switching table** shows that MAC address **00:00:00:00:00:01** is learned on VLAN **vlan-sf**. The supplicant has been moved from the **default** VLAN to the **vlan-sf** VLAN. The supplicant is then connected to the LAN through the VLAN named **vlan-sf**.

Related Documentation

- [Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31](#)
- [Configuring Server Fail Fallback \(CLI Procedure\) on page 30](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 67](#)
- [Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 40](#)
- [Understanding Server Fail Fallback and Authentication on Switches](#)

Understanding Guest VLANs for 802.1X on Switches

Guest VLANs can be configured on switches that are using 802.1X authentication to provide limited access—typically only to the Internet—for:

- Corporate guests
- End devices that are not 802.1X-enabled
- Nonresponsive end devices when MAC RADIUS authentication has not been configured on the switch interfaces to which the hosts are connected

A guest VLAN is not used for supplicants sending incorrect credentials. Those supplicants are directed to the server-reject VLAN instead.

For end devices that are not 802.1X-enabled, a guest VLAN can allow limited access to a server from which the non-802.1X-enabled end device can download the supplicant software and attempt authentication again.

A guest VLAN is not used when MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected. Some end devices, such as a printer, cannot be enabled for 802.1X. The hosts for such devices should be connected to switch interfaces that are configured for MAC RADIUS authentication. See [“Configuring MAC RADIUS Authentication \(CLI Procedure\)” on page 77](#).

Related Documentation

- [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 61](#)
- [Understanding Dynamic VLANs for 802.1X on Switches on page 68](#)
- [Understanding Authentication on Switches](#)

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch

802.1X on switches provides LAN access to users who do not have credentials in the RADIUS database. These users, referred to as *guests*, are authenticated and typically provided with access to the Internet.

This example describes how to create a guest VLAN and configure 802.1X authentication for it.

- [Requirements on page 61](#)
- [Overview and Topology on page 62](#)
- [Configuration of a Guest VLAN That Includes 802.1X Authentication on page 64](#)
- [Verification on page 64](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator interface access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you configure guest VLAN authentication, be sure you have:

- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch* or *Example: Setting Up Basic Bridging and a VLAN on the QFX Series*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.



NOTE: For more about ELS, see: *Getting Started with Enhanced Layer 2 Software*

Overview and Topology

As part of IEEE 802.1X Port-Based Network Access Control (PNAC), you can provide limited network access to supplicants who do not belong to a VLAN authentication group by configuring authentication for a guest VLAN. Typically, guest VLAN access is used to provide Internet access to visitors to a corporate site. However, you can also use the guest VLAN feature to provide access to a VLAN with limited resources to supplicants that fail 802.1X authentication on a corporate LAN.

Figure 7 on page 63 shows the conference room connected to the switch at interface **ge-0/0/1**.



NOTE: This figure also applies to QFX5100 switches.

Figure 7: Topology for Guest VLAN Example

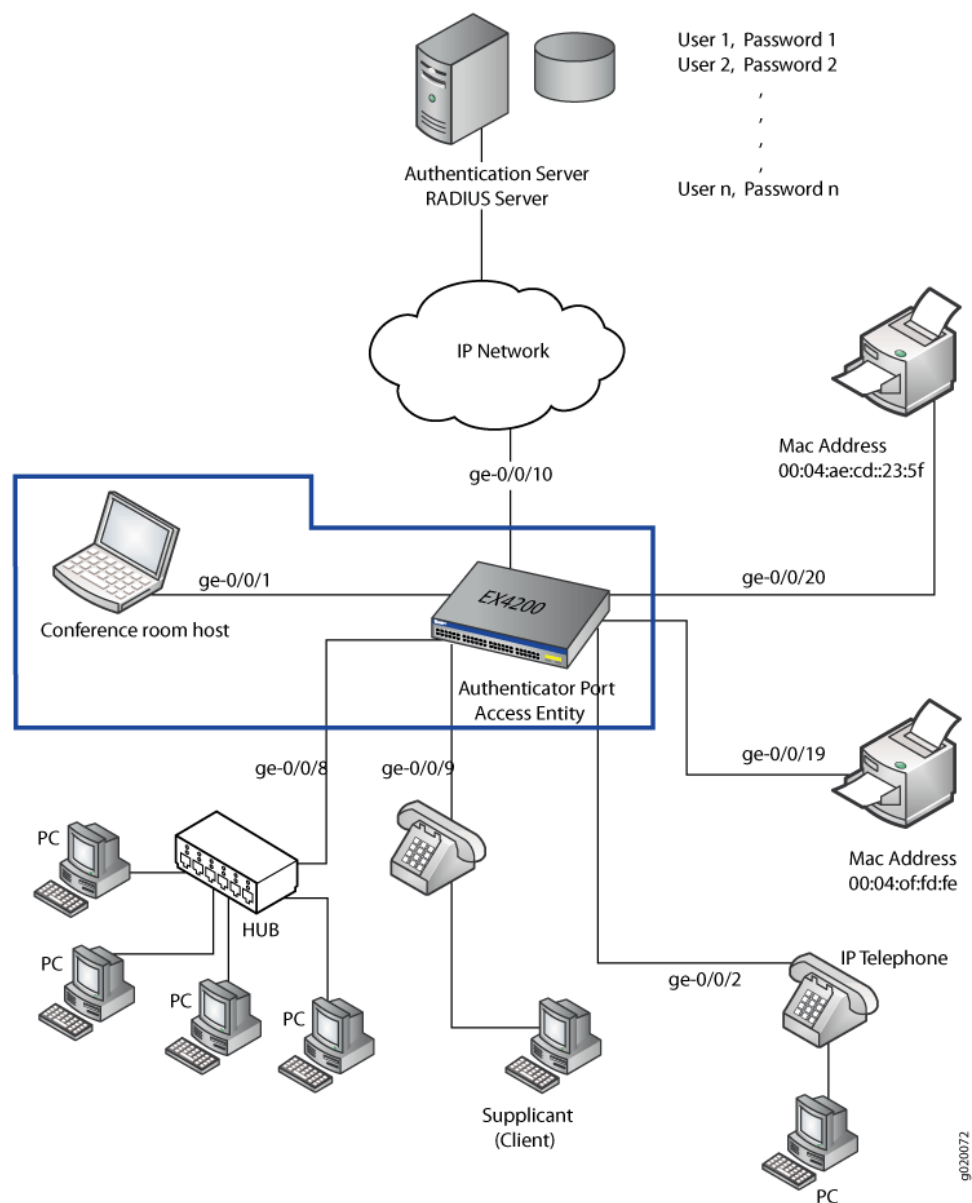


Table 11: Components of the Guest VLAN Topology

Property	Settings
Switch hardware	EX4200 switch, 24 Gigabit Ethernet interfaces: 8 PoE interfaces (ge-0/0/0 through ge-0/0/7) and 16 non-PoE interfaces (ge-0/0/8 through ge-0/0/23)
VLAN names and tag IDs	sales , tag 100 support , tag 200 guest-vlan , tag 300
One RADIUS server	Backend database connected to the switch through interface ge-0/0/10

In this example, access interface **ge-0/0/1** provides LAN connectivity in the conference room. Configure this access interface to provide LAN connectivity to visitors in the conference room who are not authenticated by the corporate VLAN.

Configuration of a Guest VLAN That Includes 802.1X Authentication

CLI Quick Configuration To quickly configure a guest VLAN, with 802.1X authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans guest-vlan vlan-id 300
set protocols dot1x authenticator interface all guest-vlan guest-vlan
```

Step-by-Step Procedure To configure a guest VLAN that includes 802.1X authentication on a switch:

1. Configure the VLAN ID for the guest VLAN:

```
[edit]
user@switch# set vlans guest-vlan vlan-id 300
```

2. Configure the guest VLAN under **dot1x** protocols:

```
[edit]
user@switch# set protocols dot1x authenticator interface all guest-vlan guest-vlan
```

Results Check the results of the configuration:

```
user@switch> show configuration
protocols {
  dot1x {
    authenticator {
      interface {
        all {
          guest-vlan {
            guest-vlan;
          }
        }
      }
    }
  }
}
vlands {
  guest-vlan {
    vlan-id 300;
  }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying That the Guest VLAN is Configured on page 64](#)

Verifying That the Guest VLAN is Configured

Purpose Verify that the guest VLAN is created and that an interface has failed authentication and been moved to the guest VLAN.



NOTE: On switches running Junos OS with support for ELS, the output for the `show vlans` command will contain additional information. If your switch runs software that supports ELS, see `show vlans`. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

Action Issue the operational mode commands:

```
user@switch> show vlans
```

Name	Tag	Interfaces
default		ge-0/0/3.0*
dynamic	40	None
guest	30	None
guest-vlan	300	ge-0/0/1.0*
vlan_dyn		None

```
user@switch> show dot1x interface ge-0/0/1.0 detail
```

```
ge-0/0/1.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: guest-vlan
  Number of connected supplicants: 1
    Supplicant: user1, 00:00:00:00:13:23
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning The output of the `show vlans` command shows **guest-vlan** as the the name of the VLAN and the VLAN ID as **300**.

The output of the `show dot1x interface ge-0/0/1.0 detail` command displays the **Guest VLAN membership** field, indicating that a supplicant at this interface failed 802.1X authentication and was passed through to the **guest-vlan**.

- Related Documentation**
- [Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25](#)
 - [Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31](#)
 - [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
 - [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 22](#)

Understanding 802.1X and RADIUS Accounting on Switches

Juniper Networks Ethernet Switches support IETF RFC 2866, *RADIUS Accounting*. By configuring RADIUS accounting on a switch, you can collect statistical data about users logging on to or out of a LAN to be collected and send that data to a RADIUS accounting server. The statistical data gathered can be used to perform general network monitoring, to analyze and track usage patterns, or to bill a user based on the amount of time or type of services accessed.

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

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

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

1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. For example, on FreeRADIUS, the default port is 1813.
2. The switch forwards an *accounting-request* packet containing an event record to the accounting server. For example, a supplicant is authenticated through 802.1X authentication and then connected to the LAN. The event record associated with this supplicant contains an *Acct-Status-Type* attribute whose value indicates the beginning of user service for this supplicant. When the supplicant's session ends, the accounting request will contain an *Acct-Status-Type* attribute value that indicates the end of user service. The RADIUS accounting server records this as a stop-accounting record that contains session information and the length of the session.
3. The RADIUS accounting server logs these events as start-accounting or stop-accounting records. The records are stored in a file. On FreeRADIUS, the file name is the server's address; for example, 122.69.1.250.
4. The accounting server sends an *accounting-response* packet back to the switch confirming it has received the accounting request.
5. If the switch does not receive a response from the server, it continues to send accounting requests until an accounting response is returned from the accounting server.

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

Related Documentation

- [802.1X for Switches Overview on page 20](#)
- [Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 67](#)

Configuring 802.1X RADIUS Accounting (CLI Procedure)

RADIUS accounting permits statistical data about users logging onto or off a LAN to be collected and sent to a RADIUS accounting server. The statistical data gathered can be used for general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

To configure basic RADIUS accounting by using the CLI:

1. Specify the accounting servers to which the switch will forward accounting statistics:

```
[edit access]
user@switch# set profile profile1 radius accounting-server [server-addresses]
```

2. Define the RADIUS accounting servers:

```
[edit access]
user@switch# set radius-server server-address secret password
user@switch# set radius-server server-address secret password
```

3. Enable accounting for an access profile:

```
[edit access]
user@switch# set profile profile-name accounting (Access Profile)
```

4. Configure the RADIUS servers to use while sending accounting messages and updates:

```
[edit access]
user@switch# set profile profile-name accounting order radius
```

5. Configure the statistics to be collected on the switch and forwarded to the accounting server:

```
[edit access]
user@switch# set profile profile-name accounting accounting-stop-on-access-deny
user@switch# set profile profile-name accounting accounting-stop-on-failure
```

6. Display accounting statistics collected on the switch:

```
user@switch> show network-access aaa statistics accounting
Accounting module statistics
  Requests received: 1
  Accounting Response failures: 0
  Accounting Response Success: 1
  Requests timedout: 0
```

7. Open an accounting log on the RADIUS accounting server by using the server's address, and view accounting statistics:

```
[root@freeradius]# cd /usr/local/var/log/radius/radacct/122.69.1.250
[root@freeradius 122.69.1.250]# ls
```

```
detail-20071214
```

```
[root@freeradius 122.69.1.250]# vi details-20071214
```

```
User-Name = "000347e1bab9"
NAS-Port = 67
Acct-Status-Type = Stop
Acct-Session-Id = "802.1x811912"
Acct-Input-Octets = 17454
Acct-Output-Octets = 4245
Acct-Session-Time = 1221041249
Acct-Input-Packets = 72
Acct-Output-Packets = 53
Acct-Terminate-Cause = Lost-Carrier
Acct-Input-Gigawords = 0
Acct-Output-Gigawords = 0
Called-Station-Id = "00-19-e2-50-52-60"
Calling-Station-Id = "00-03-47-e1-ba-b9"
Event-Timestamp = "Sep 10 2008 16:52:39 PDT"
NAS-Identifier = "esp48t-1b-01"
NAS-Port-Type = Virtual

User-Name = "000347e1bab9"
NAS-Port = 67
Acct-Status-Type = Start
Acct-Session-Id = "802.1x811219"
Called-Station-Id = "00-19-e2-50-52-60"
Calling-Station-Id = "00-03-47-e1-ba-b9"
Event-Timestamp = "Sep 10 2008 18:58:52 PDT"
NAS-Identifier = "esp48t-1b-01"
NAS-Port-Type = Virtual
```

- Related Documentation**
- [Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25](#)
 - [Understanding 802.1X and RADIUS Accounting on Switches on page 66](#)

Understanding Dynamic VLANs for 802.1X on Switches

Dynamic VLANs, in conjunction with the 802.1X authentication process, provide secure access to the LAN on a single port for end devices belonging to different VLANs.

When this feature is configured on the RADIUS server, an end device or user authenticating on the RADIUS server is assigned to the VLAN configured for it. The end device or user becomes a member of a VLAN dynamically after successful 802.1X authentication. For information on configuring dynamic VLANs on your RADIUS server, see the documentation for your RADIUS server.

Successful authentication requires that the VLAN ID or VLAN name exist on the switch and match the VLAN ID or VLAN name sent by the RADIUS server during authentication. If neither exists, the end device is unauthenticated. If a guest VLAN is established, the unauthenticated end device is automatically moved to the guest VLAN.

- Related Documentation**
- [Understanding Guest VLANs for 802.1X on Switches on page 60](#)
 - [Example: Configuring MAC RADIUS Authentication on a Switch on page 82](#)
 - [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 61](#)

Example: Configuring Fallback Options on Switches for EAP-TTLS Authentication and Odyssey Access Clients

For 802.1X user authentication, switches support RADIUS authentication servers that are using Extensible Authentication Protocol–Tunneled TLS (EAP-TTLS) to authenticate Odyssey Access Client (OAC) supplicants. OAC networking software runs on endpoint computers (desktop, laptop, or notepad computers and supported wireless devices) and provides secure access to both wired and wireless networks.

This example describes how to configure an 802.1X-enabled interface on the switch to provide fallback support for OAC users who have entered incorrect login credentials:

- [Requirements on page 69](#)
- [Overview and Topology on page 69](#)
- [Configuration on page 71](#)
- [Verification on page 73](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 11.2 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.
- One OAC end device acting as a supplicant.

Before you begin configuring the fallback option, ensure that you have:

- Set up a connection between the switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to a Switch” on page 25](#).
- Configured EAP-TTLS on the server. See your RADIUS server documentation.
- Configured users on the RADIUS server. See your RADIUS server documentation.

Overview and Topology

OAC is networking software that runs on endpoint computers (desktop, laptop, or notepad) and supported wireless devices. OAC provides full support for EAP, which is required for secure wireless LAN access.

In this topology, OAC is deployed with an 802.1X-enabled switch and a RADIUS server. The switch functions as an enforcement point in the network security architecture. This topology:

- Ensures that only authorized users can connect.
- Maintains privacy of login credentials.
- Maintains data privacy over the wireless link.

This example includes the configuration of a server-reject VLAN on the switch, which can be used to prevent accidental lockout for users who have entered incorrect login credentials. These users can be given limited LAN access.

However, this fallback configuration is complicated by the fact that the OAC supplicant and RADIUS server are using EAP-TTLS. EAP-TTLS creates a secure encrypted tunnel between the server and the end device to complete the authentication process. When the user enters an incorrect login, the RADIUS server sends EAP failure messages directly to the client through this tunnel. The EAP failure message causes the client to restart the authentication procedure, so that the switch's 802.1X authentication process tears down the session that was established with the switch using the server-reject VLAN. You can enable the remedial connection to continue by configuring:

- **eapol-block**—Enable the EAPoL block timer on the 802.1X interface that is configured to belong to the server-reject VLAN. The block timer causes the authentication port access entity to ignore EAP start messages from the client, attempting to restart the authentication procedure.



NOTE: The EAPoL block timer is triggered only after the retries on the 802.1X interface have been exhausted. You can configure retries to specify the number of times the switch attempts to authenticate the port after an initial failure. The default is three retries.

- **block-interval**—Configure the amount of time that you want the EAPoL block timer to continue to ignore EAP start messages. If you do not configure the block interval, the EAPoL block timer defaults to 120 seconds.

When the 802.1X interface ignores the EAP start messages from the client, the switch allows the existing remedial session that was established through the server-reject VLAN to remain open.

These configuration options apply to **single**, **single-secure**, and **multiple** supplicant authentication modes. In this example, the 802.1X interface is configured in single-supplicant mode.

[Figure 8 on page 71](#) shows an EX Series switch connecting an OAC end device to a RADIUS server, and indicates the protocols being used to connect the network entities.



NOTE: This figure also applies to QFX5100 switches.

Figure 8: EX Series Switch Connecting OAC to RADIUS Server Using EAP-TTLS Authentication

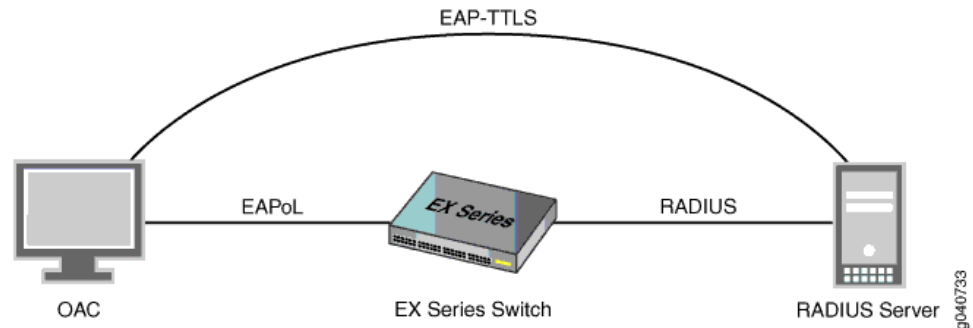


Table 12 on page 71 describes the components in this OAC deployment.

Table 12: Components of the OAC Deployment

Property	Settings
Switch hardware	EX Series switch
VLANs	default server-reject-vlan: VLAN name is remedial and VLAN ID is 700
802.1X interface	ge-0/0/8
OAC supplicant	EAP-TTLS
One RADIUS authentication server	EAP-TTLS

Configuration

To configure fallback options for EAP-TTLS and OAC supplicants, perform this task:

CLI Quick Configuration To quickly configure the fallback options for EAP-TTLS and OAC supplicants, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans remedial vlan-id 700
set protocols dot1x authenticator interface ge-0/0/8 retries 4
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan remedial
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan eapol-block
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan block-interval 130
```

Step-by-Step Procedure To configure the fallback options for EAP-TTLS and OAC supplicants:

TIP: In this example, the switch has only one server-reject VLAN. Therefore, the configuration specifies `eapol-block` and `block-interval` directly after `server-reject-vlan`. However, if you have configured multiple VLANs on the switch, you should include the VLAN name or VLAN ID directly after `server-reject-vlan` to indicate which VLAN is being modified.

1. Configure a VLAN that will function as the server-reject VLAN to provide limited LAN access for users who have entered incorrect login credentials:

```
[edit]
user@switch# set vlans remedial vlan-id 700
```
2. Configure the number of times for the client to be prompted for username and password before an incorrect login is directed to the server-reject VLAN:

```
[edit protocols dot1x authenticator interface ge-0/0/8]
user@switch# set retries 4
```
3. Configure the 802.1X authenticator interface to use the server-reject VLAN as a fallback for incorrect logins:

```
[edit protocols dot1x authenticator interface ge-0/0/8]
user@switch# set server-reject-vlan remedial
```
4. Enable the EAPoL block timer on the 802.1X interface that is configured to belong to the server-reject VLAN.

```
[edit protocols dot1x authenticator interface ge-0/0/8]
user@switch# set server-reject-vlan eapol-block
```
5. Configure the amount of time for the EAPoL block to remain in effect:

```
[edit protocols dot1x authenticator interface ge-0/0/8]
user@switch# set server-reject-vlan block-interval 130
```

Results

Check the results of the configuration:

```
user@switch> show configuration
protocols {
  dot1x {
    authenticator {
      interface {
        ge-0/0/8.0 {
          supplicant single;
          retries 4;
          server-reject-vlan remedial block-interval 130 eapol-block;
        }
      }
    }
  }
}
```

Verification

To confirm that the configuration and the fallback options are working correctly, perform this task:

- [Verifying the Configuration of the 802.1X Interface on page 73](#)

Verifying the Configuration of the 802.1X Interface

Purpose Verify that the 802.1X interface is configured with the desired options:

Action user@switch> `show dot1x interface ge-0/0/8.0 detail`
 ge-0/0/8.0
 Role: Authenticator
 Administrative state: Auto
 Supplicant mode: Single
 Number of retries: 4
 Quiet period: 60 seconds
 Transmit period: 30 seconds
 Mac Radius: Disabled
 Mac Radius Restrict: Disabled
 Reauthentication: Enabled
 Configured Reauthentication interval: 120 seconds
 Supplicant timeout: 30 seconds
 Server timeout: 30 seconds
 Maximum EAPoL requests: 2
 Guest VLAN member: guest
 Number of connected supplicants: 1
 Supplicant: tem, 2A:92:E6:F2:00:00
 Operational state: Authenticated
 Backend Authentication state: Idle
 Authentication method: Radius
 Authenticated VLAN: remedial
 Session Reauth interval: 120 seconds
 Reauthentication due in 68 seconds

Meaning The `show dot1x ge-0/0/8 detail` output shows that the `ge-0/0/8` interface is in the **Authenticated** state and that it is using the **remedial** VLAN.

Related Documentation • [Understanding Authentication on Switches](#)

Controlling Authentication Session Timeouts (CLI Procedure)

For 802.1X and MAC RADIUS authentication sessions, you can specify authentication session timeout values using the **reauthentication** statement.

The session might also end when the MAC table aging time expires, because the session is removed from the authentication session table when the MAC address is removed from the Ethernet switching table. In order to prevent the session from being removed from the authentication session table, you must disassociate the authentication table from the Ethernet switching table using the **no-mac-table-binding** statement.

Before you begin:

- Specify the RADIUS server or servers to be used as the authentication server. See [“Specifying RADIUS Server Connections on Switches \(CLI Procedure\)”](#) on page 24.
- Configure 802.1X authentication on the switch. See [“Configuring 802.1X Interface Settings \(CLI Procedure\)”](#) on page 22.

To configure the authentication session time on all interfaces:

```
[edit]
user@switch# set protocols dot1x authenticator interface all reauthentication seconds;
```

To configure the authentication session time on a single interface:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name reauthentication
seconds;
```

To disable removal of authentication sessions from the authentication session table when a MAC address ages out of the Ethernet switching table, remove the binding of the authentication table to the Ethernet switching table.

To remove the binding:

```
[edit]
user@switch# set protocols dot1x authenticator no-mac-table-binding;
```

Related Documentation

- [Configuring MAC Table Aging \(CLI Procedure\)](#)
- [Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch](#) on page 31
- [Understanding Authentication on Switches](#)
- [Understanding Authentication Session Timeout](#)

Verifying 802.1X Authentication

Purpose Verify that supplicants are being authenticated on an interface on a switch with the interface configured for 802.1X authentication, and display the method of authentication being used.

Action Display detailed information about an interface configured for 802.1X (here, the interface is ge-0/0/16):

```
user@switch> show dot1x interface ge-0/0/16.0 detail
ge-0/0/16.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Strict: Disabled
  Reauthentication: Enabled Reauthentication interval: 40 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 1
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user5, 00:30:48:8C:66:BD
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: v200
      Reauthentication due in 17 seconds
```

Meaning The sample output from the **show dot1x interface detail** command shows that the **Number of connected supplicants** is 1. The supplicant that was authenticated and is now connected to the LAN is known as **user5** on the RADIUS server and has the MAC address **00:30:48:8C:66:BD**. The supplicant was authenticated by means of the 802.1X authentication method called **Radius** authentication. When the **Radius** authentication method is used, the supplicant is configured on the RADIUS server, the RADIUS server communicates this to the switch, and the switch opens LAN access on the interface to which the supplicant is connected. The sample output also shows that the supplicant is connected to VLAN **v200**.

Other 802.1X authentication methods supported on switches in addition to the **RADIUS** method are:

- **Guest VLAN**—A nonresponsive host is granted Guest-VLAN access.
- **MAC Radius**—A nonresponsive host is authenticated based on its MAC address. The MAC address is configured as permitted on the RADIUS server, the RADIUS server lets the switch know that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected.
- **Server-fail deny**—If the RADIUS servers time out, all supplicants are denied access to the LAN, preventing traffic from flowing from the supplicant through the interface. This is the default.
- **Server-fail permit**—When the RADIUS server is unavailable, a supplicant is still permitted access to the LAN as if the supplicant had been successfully authenticated by the RADIUS server.

- **Server-fail use-cache**—If the RADIUS servers time out during reauthentication, previously authenticated supplicants are granted access, but new supplicants are denied LAN access.
- **Server-fail VLAN**—A supplicant is configured to be moved to a specified VLAN if the RADIUS server is unavailable to reauthenticate the supplicant. (The VLAN must already exist on the switch.)

**Related
Documentation**

- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 22](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 77](#)
- [Configuring Server Fail Fallback \(CLI Procedure\) on page 30](#)

CHAPTER 4

Configuring MAC RADIUS Authentication to Control Network Access

- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 77](#)
- [Specifying RADIUS Server Connections on Switches \(CLI Procedure\) on page 79](#)
- [Configuring Server Fail Fallback \(CLI Procedure\) on page 81](#)
- [Example: Configuring MAC RADIUS Authentication on a Switch on page 82](#)
- [Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on page 88](#)
- [Controlling Authentication Session Timeouts \(CLI Procedure\) on page 93](#)

Configuring MAC RADIUS Authentication (CLI Procedure)

You can permit devices that are not 802.1X-enabled LAN access by configuring MAC RADIUS authentication on the switch interfaces to which the hosts are connected.



NOTE: You can also allow non-802.1X-enabled devices to access the LAN by configuring their MAC address for static MAC bypass of authentication.

You can configure MAC RADIUS authentication on an interface that also allows 802.1X authentication, or you can configure either authentication method alone.

If both MAC RADIUS and 802.1X authentication are enabled on the interface, the switch first sends the host three EAPOL requests to the host. If there is no response from the host, the switch sends the host's MAC address to the RADIUS server to check whether it is a permitted MAC address. If the MAC address is configured as permitted on the RADIUS server, the RADIUS server sends a message to the switch that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected.

If MAC RADIUS authentication is configured on the interface but 802.1X authentication is not (by using the **mac-radius restrict** option), the switch attempts to authenticate the MAC address with the RADIUS server without delaying by attempting 802.1X authentication first.

Before you configure MAC RADIUS authentication, be sure you have:

- Configured basic access between the switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to a Switch” on page 25](#).

To configure MAC RADIUS authentication using the CLI:

- On the switch, configure the interfaces to which the nonresponsive hosts are attached for MAC RADIUS authentication, and add the **restrict** qualifier for interface **ge-0/0/20** to have it use only MAC RADIUS authentication:

```
[edit]
user@switch# set protocols dot1x authenticator interface ge-0/0/19 mac-radius
user@switch# set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
```

- On a RADIUS authentication server, create user profiles for each nonresponsive host using the MAC address (without colons) of the nonresponsive host as the username and password (here, the MAC addresses are **00:04:0f:fd:ac:fe** and **00:04:ae:cd:23:5f**):

```
[root@freeradius]#
edit /etc/raddb
vi users
00040ffdacfe Auth-type:=Local, User-Password = "00040ffdacfe"
0004aecd235f Auth-type:=Local, User-Password = "0004aecd235f"
```

Related Documentation

- [Example: Configuring MAC RADIUS Authentication on a Switch on page 82](#)
- [Verifying 802.1X Authentication on page 74](#)
- [Understanding Authentication on Switches](#)

Specifying RADIUS Server Connections on Switches (CLI Procedure)

IEEE 802.1X and MAC RADIUS authentication both provide network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from devices at the interface until the supplicant's credentials or MAC address are presented and matched on the *authentication server* (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

To use 802.1X or MAC RADIUS authentication, you must specify the connections on the switch for each RADIUS server to which you will connect.

To configure a RADIUS server on the switch:

1. Define the IP address of the RADIUS server, the RADIUS server authentication port number, and the secret password. You can define more than one RADIUS server. The secret password on the switch must match the secret password on the server:

```
[edit access]
user@switch# set radius-server 10.0.0.100 port 1812 secret abc
```



NOTE: Specifying the authentication port is optional, and port 1812 is the default. However, we recommend that you configure it in order to avoid confusion as some RADIUS servers might refer to an older default.

2. (Optional) Specify the IP address by which the switch is identified by the RADIUS server. If you do not specify this, the RADIUS server uses the address of the interface sending the RADIUS request. We recommend that you specify this IP address because if the request gets diverted on an alternate route to the RADIUS server, the interface relaying the request might not be an interface on the switch.

```
[edit access]
user@switch# set access radius-server source-address 10.93.14.100
```

3. Configure the authentication order, making **radius** the first method of authentication:

```
[edit access]
user@switch# set profile profile1 authentication-order radius
```

4. Create a profile and specify the list of RADIUS servers to be associated with the profile. For example, you might choose to group your RADIUS servers geographically by city. This feature enables easy modification whenever you want to change to a different set of authentication servers.

```
[edit access profile]
user@switch# set atlanta radius authentication-server 10.0.0.100 10.2.14.200
```

5. Specify the group of servers to be used for 802.1X or MAC RADIUS authentication by identifying the profile name:

```
[edit access profile]
user@switch# set protocols dot1x authenticator authentication-profile-name denver
```

6. Configure the IP address of the switch in the list of clients on the RADIUS server. For specifics on configuring the RADIUS server, consult the documentation for your server.

**Related
Documentation**

- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 22](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 77](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 67](#)

Configuring Server Fail Fallback (CLI Procedure)

You can use the server fail fallback feature to specify how end devices connected to the switch are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

802.1X and MAC RADIUS authentication work by using an *authenticator port access entity* (the switch) to block all traffic to and from an end device at the interface until the end device's credentials are presented and matched on the *authentication server* (a RADIUS server). When the end device has been authenticated, the switch stops blocking and opens the interface to the end device.

When you set up 802.1X or MAC RADIUS authentication on the switch, you specify a primary authentication server and one or more backup authentication servers. If the primary authentication server cannot be reached by the switch and the secondary authentication servers are also unreachable, a RADIUS server timeout occurs. Because the authentication server grants or denies access to the end devices awaiting authentication, the switch does not receive access instructions for end devices attempting access to the LAN and normal authentication cannot be completed. With server fail fallback, you can configure authentication alternatives that permit the switch to take appropriate actions toward end devices awaiting authentication or reauthentication.



NOTE: The authentication fallback method called *server-reject VLAN* provides limited access to a LAN, typically only to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials. If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is not allowed.

To configure basic server fail fallback options by using the CLI:

- Configure an interface to allow traffic to flow from a supplicant to the LAN if a RADIUS server timeout occurs (as if the end device had been successfully authenticated by a RADIUS server):

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name server-fail permit
```

- Configure an interface to prevent traffic flow from an end device to the LAN (as if the end device had failed authentication and had been rejected by the RADIUS server):

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name server-fail deny
```

- Configure an interface to move an end device to a specified VLAN if a RADIUS server timeout occurs:

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name server-fail vlan-name
```

- Configure an interface to recognize already connected end devices as reauthenticated if there is a RADIUS timeout during reauthentication (new users will be denied access):

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name server-fail use-cache
```

- Configure an interface that receives a RADIUS access-reject message from the authentication server to move end devices attempting LAN access on the interface to a specified VLAN already configured on the switch (in this case, the VLAN name is *vlan-sf*):

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name server-reject-vlan vlan-sf
```



NOTE: If an IP phone is authenticated in the server-reject VLAN, voice traffic is not allowed.

Related Documentation

- [Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to a Switch on page 54](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 22](#)
- [Monitoring 802.1X Authentication](#)
- [Understanding Server Fail Fallback and Authentication on Switches](#)

Example: Configuring MAC RADIUS Authentication on a Switch

To permit hosts that are not 802.1X-enabled to access the LAN, you can configure MAC RADIUS authentication on the switch interfaces to which the non-802.1X-enabled hosts are connected. When MAC RADIUS authentication is configured, the switch will attempt to authenticate the host with the RADIUS server using the host's MAC address.

This example describes how to configure MAC RADIUS authentication for two non-802.1X-enabled hosts:

- [Requirements on page 83](#)
- [Overview and Topology on page 83](#)
- [Configuration on page 85](#)
- [Verification on page 86](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.3 or later for EX Series switches.
- An EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- A RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you configure MAC RADIUS authentication, be sure you have:

- Configured basic access between the EX Series switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to a Switch” on page 25](#).
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch* or *Example: Setting Up Basic Bridging and a VLAN on the QFX Series*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.



NOTE: For more about ELS, see: *Getting Started with Enhanced Layer 2 Software*

- Performed basic 802.1X configuration. See [“Configuring 802.1X Interface Settings \(CLI Procedure\)” on page 22](#).

Overview and Topology

IEEE 802.1X port-based network access control (PNAC) authenticates and permits devices access to a LAN if the devices can communicate with the switch using the 802.1X protocol (are 802.1X-enabled). To permit non-802.1X-enabled end devices to access the LAN, you can configure MAC RADIUS authentication on the interfaces to which the end devices are connected. When the MAC address of the end device appears on the

interface, the switch consults the RADIUS server to check whether it is a permitted MAC address. If the MAC address of the end device is configured as permitted on the RADIUS server, the switch opens LAN access to the end device.

You can configure both MAC RADIUS authentication and 802.1X authentication methods on an interface configured for multiple supplicants. Additionally, if an interface is only connected to a non-802.1X-enabled host, you can enable MAC RADIUS and not enable 802.1X authentication using the **mac-radius restrict** option, and thus avoid the delay that occurs while the switch determines that the device does not respond to EAP messages.

Figure 9 on page 84 shows the two printers connected to the switch.



NOTE: This figure also applies to QFX5100 switches.

Figure 9: Topology for MAC RADIUS Authentication Configuration

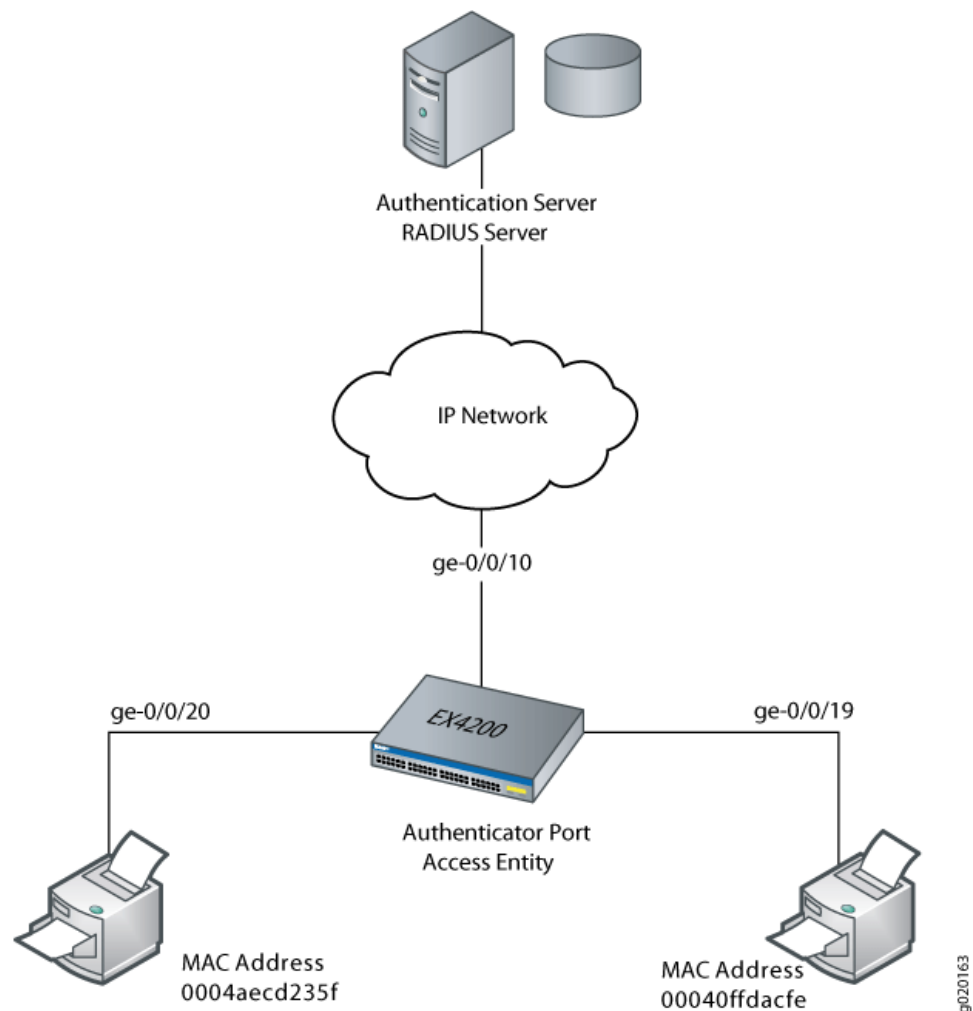


Table 13 on page 85 shows the components in the example for MAC RADIUS authentication.

Table 13: Components of the MAC RADIUS Authentication Configuration Topology

Property	Settings
Switch hardware	EX4200 ports (ge-0/0/0 through ge-0/0/23)
VLAN name	sales
Connections to printers (no PoE required)	ge-0/0/19, MAC address 00040ffdacfe ge-0/0/20, MAC address 0004aecd235f
RADIUS server	Connected to the switch on interface ge-0/0/10

The printer with the MAC address 00040ffdacfe is connected to access interface ge-0/0/19. A second printer with the MAC address 0004aecd235f is connected to access interface ge-0/0/20. In this example, both interfaces are configured for MAC RADIUS authentication on the switch, and the MAC addresses (without colons) of both printers are configured on the RADIUS server. Interface ge-0/0/20 is configured to eliminate the normal delay while the switch attempts 802.1X authentication; MAC RADIUS authentication is enabled and 802.1X authentication is disabled using the **mac radius restrict** option.

Configuration

CLI Quick Configuration

To quickly configure MAC RADIUS authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator interface ge-0/0/19 mac-radius
set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
```



NOTE: You must also configure the two MAC addresses as usernames and passwords on the RADIUS server, as is done in step 2 of the Step-by-Step Procedure.

Step-by-Step Procedure

Configure MAC RADIUS authentication on the switch and on the RADIUS server:

- On the switch, configure the interfaces to which the printers are attached for MAC RADIUS authentication, and configure the **restrict** option on interface **ge-0/0/20**, so that only MAC RADIUS authentication is used:


```
[edit]
user@switch# set protocols dot1x authenticator interface ge-0/0/19 mac-radius
user@switch# set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
```
- On the RADIUS server, configure the MAC addresses **00040ffdacfe** and **0004aecd235f** as usernames and passwords:


```
[root@freeradius]#
edit /etc/raddb
vi users
00040ffdacfe Auth-type:=EAP, User-Password = "00040ffdacfe"
0004aecd235f Auth-type:=EAP, User-Password = "0004aecd235f"
```

Results Display the results of the configuration on the switch:

```
user@switch> show configuration
protocols {
  dot1x {
    authenticator {
      authentication-profile-name profile52;
    }
    interface {
      ge-0/0/19.0 {
        mac-radius;
      }
      ge-0/0/20.0 {
        mac-radius {
          restrict;
        }
      }
    }
  }
}
```

Verification

Verify that the supplicants are authenticated:

- [Verifying That the Supplicants Are Authenticated on page 86](#)

Verifying That the Supplicants Are Authenticated

Purpose After supplicants are configured for MAC RADIUS authentication on the switch and on the RADIUS server, verify that they are authenticated and display the method of authentication:

Action Display information about 802.1X-configured interfaces **ge-0/0/19** and **ge-0/0/20** by issuing the **show dot1x interface** command:

```
user@switch> show dot1x interface ge-0/0/19.0 detail
ge-0/0/19.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds

user@switch> show dot1x interface ge-0/0/20.0 detail
ge-0/0/20.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Enabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user102, 00:04:ae:cd:23:5f
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning The sample output from the **show dot1x interface detail** command displays the MAC address of the connected end device in the **Supplicant** field. On interface **ge-0/0/19**, the MAC address is **00:04:0f:fd:ac:fe**, which is the MAC address of the first printer configured for MAC RADIUS authentication. The **Authentication method** field displays the authentication method as **MAC Radius**. On interface **ge-0/0/20**, the MAC address is **00:04:ae:cd:23:5f**, which is the MAC address of the second printer configured for MAC

RADIUS authentication. The **Authentication method** field displays the authentication method as **MAC Radius**.

Related Documentation

- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 77](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 22](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
- [Understanding Authentication on Switches](#)

Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication



NOTE: This example uses Junos OS for EX Series and QFX5100 switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

Firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server. The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.

This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

- [Requirements on page 88](#)
- [Overview and Topology on page 89](#)
- [Configuration on page 91](#)
- [Verification on page 93](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 13.2 or later for EX Series switches
- One EX4300 switch

- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

- Set up a connection between the switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to a Switch” on page 25](#).
- Configured 802.1X authentication on the switch, with the authentication mode for the interface ge-0/0/2 set to **multiple**. See [“Configuring 802.1X Interface Settings \(CLI Procedure\)” on page 22](#) and [“Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch” on page 31](#).
- Configured users on the RADIUS authentication server.

Overview and Topology

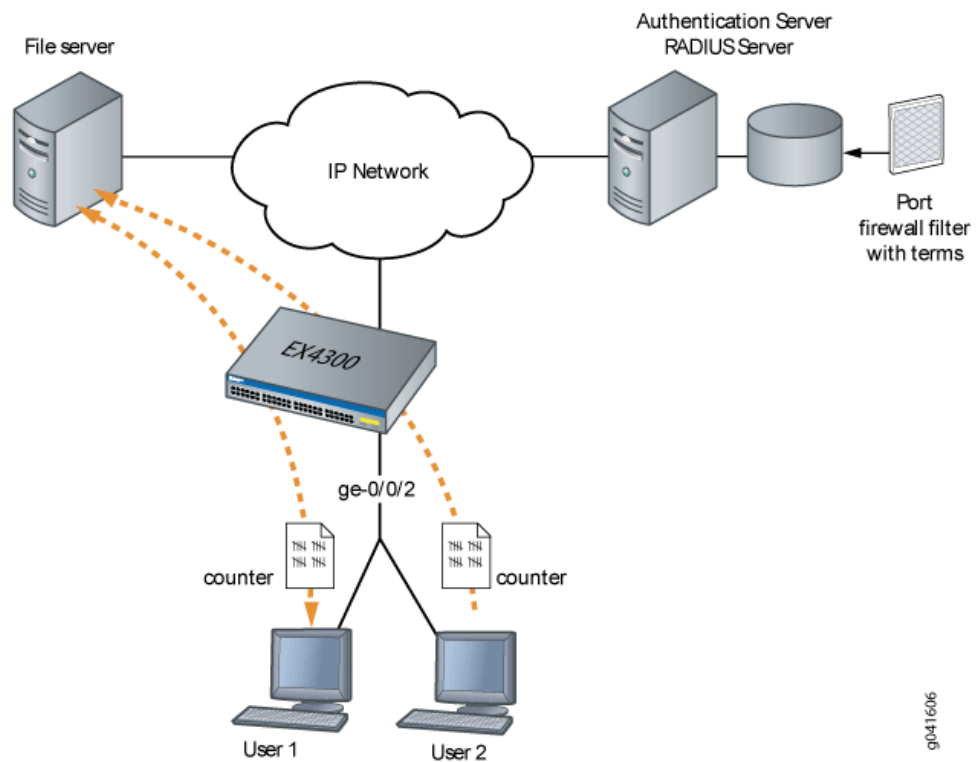
When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines the interface firewall filter with the user policies sent to the switch from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in [Figure 4 on page 51](#), when User 1 is authenticated by the EX Series switch, the system adds a term to the firewall filter **dynamic-filter-example**. When User 2 is authenticated, another term is added to the firewall filter, and so on.



NOTE: This figure also applies to QFX5100 switches.

Figure 10: Conceptual Model: Dynamic Filter Updated for Each New User



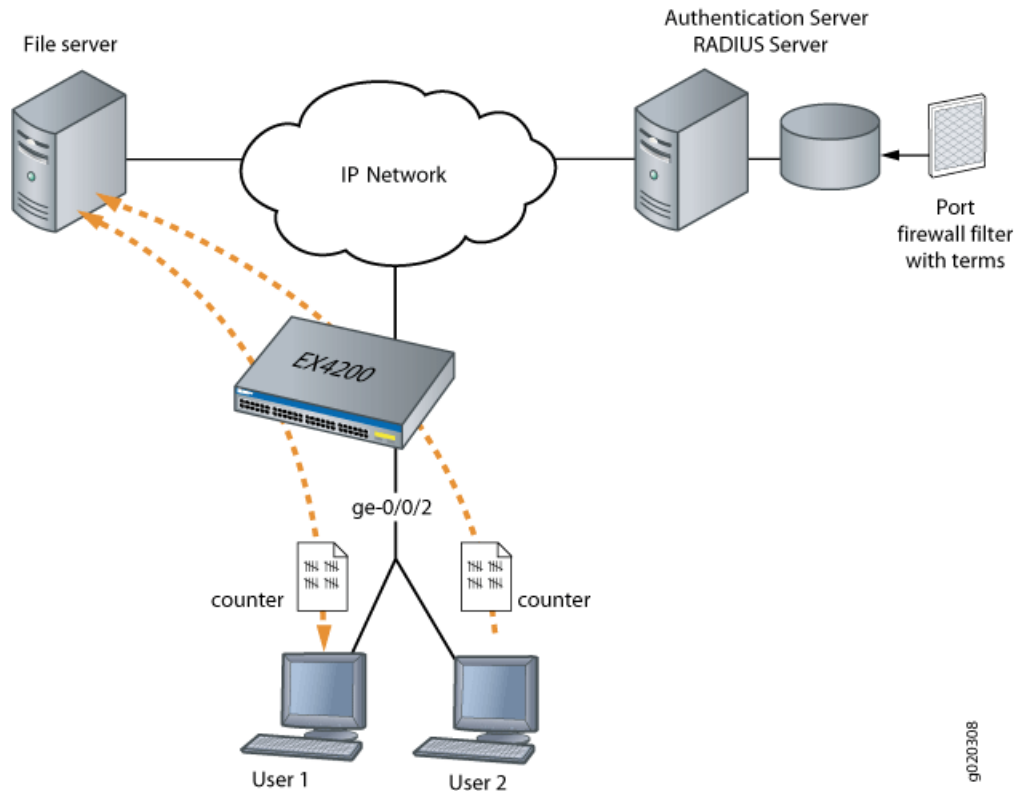
This is a conceptual model of the internal process—you cannot access or view the dynamic filter.



NOTE: If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface ge-0/0/2 to the file server, which is located on subnet 192.0.2.16/28, and set policer definitions to rate-limit the traffic. [Figure 5 on page 52](#) shows the network topology for this example.

Figure 11: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server



Configuration

Configuring Firewall Filters on Interfaces with Multiple Supplicants

CLI Quick Configuration

To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter filter1 term term1 from ip-destination-address 192.0.2.16/28
set firewall family ethernet-switching filter filter1 term term2 from ip-destination-address 192.0.2.16/28
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1500
set firewall policer p1 then discard
set firewall family ethernet-switching filter filter1 term term1 then count counter1
set firewall family ethernet-switching filter filter1 term term2 then policer p1
```

Step-by-Step Procedure

To configure firewall filters on an interface enabled for multiple supplicants:

- Set the policer definition:


```
user@switch# show policer p1 |display set
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1500
set firewall policer p1 then discard
```

2. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term term1 from ip-destination-address 192.0.2.16/28
user@switch# set filter filter1 term term2 from ip-destination-address 192.0.2.16/28
user@switch# set filter filter1 term term1 then count counter1
user@switch# set filter filter1 term term2 then policer p1
```

Results Check the results of the configuration:

```
user@switch> show configuration
```

```
firewall {
  family ethernet-switching {
    filter filter1 {
      term term1 {
        from {
          ip-destination-address {
            192.0.2.16/28;
          }
        }
        then count counter1;
      }
      term term2 {
        from {
          ip-destination-address {
            192.0.2.16/28;
          }
        }
        then policer p1;
      }
    }
  }
  policer p1 {
    if-exceeding {
      bandwidth-limit 1m;
      burst-size-limit 1500;
    }
    then discard;
  }
}
protocols {
  dot1x {
    authenticator
    interface ge-0/0/2 {
      supplicant multiple;
    }
  }
}
```

Verification

Verifying Firewall Filters on Interfaces with Multiple Supplicants

Purpose	Verify that firewall filters are functioning on the interface with multiple supplicants.
Action	<ol style="list-style-type: none"> 1. Check the results with one user authenticated on the interface. In this case, User 1 is authenticated on ge-0/0/2: <pre>user@switch> show dot1x firewall Filter: dot1x_ge-0/0/2 Counters counter1_dot1x_ge-0/0/2_user1 100</pre> 2. When a second user, User 2, is authenticated on the same interface, ge-0/0/2, you can verify that the filter includes the results for both of the users authenticated on the interface: <pre>user@switch> show dot1x firewall Filter: dot1x-filter-ge-0/0/0 Counters counter1_dot1x_ge-0/0/2_user1 100 counter1_dot1x_ge-0/0/2_user2 400</pre>
Meaning	The results displayed by the show dot1x firewall command output reflect the dynamic filter created with the authentication of each new user. User 1 accessed the file server located at the specified destination address 100 times, while User 2 accessed the same file server 400 times.
Related Documentation	<ul style="list-style-type: none"> • Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on a Switch on page 43 • Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches • Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 40

Controlling Authentication Session Timeouts (CLI Procedure)

For 802.1X and MAC RADIUS authentication sessions, you can specify authentication session timeout values using the **reauthentication** statement.

The session might also end when the MAC table aging time expires, because the session is removed from the authentication session table when the MAC address is removed from the Ethernet switching table. In order to prevent the session from being removed from the authentication session table, you must disassociate the authentication table from the Ethernet switching table using the **no-mac-table-binding** statement.

Before you begin:

- Specify the RADIUS server or servers to be used as the authentication server. See [“Specifying RADIUS Server Connections on Switches \(CLI Procedure\)” on page 24](#).

- Configure 802.1X authentication on the switch. See [“Configuring 802.1X Interface Settings \(CLI Procedure\)”](#) on page 22.

To configure the authentication session time on all interfaces:

```
[edit]
user@switch# set protocols dot1x authenticator interface all reauthentication seconds;
```

To configure the authentication session time on a single interface:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name reauthentication
seconds;
```

To disable removal of authentication sessions from the authentication session table when a MAC address ages out of the Ethernet switching table, remove the binding of the authentication table to the Ethernet switching table.

To remove the binding:

```
[edit]
user@switch# set protocols dot1x authenticator no-mac-table-binding;
```

Related Documentation

- [Configuring MAC Table Aging \(CLI Procedure\)](#)
- [Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch](#) on page 31
- [Understanding Authentication on Switches](#)
- [Understanding Authentication Session Timeout](#)

CHAPTER 5

Bypassing 802.1X and MAC RADIUS Authentication to Allow Trusted Hosts to Access the Network

- [Configuring Static MAC Bypass of Authentication \(CLI Procedure\) on page 95](#)
- [Example: Configuring Static MAC Bypass of Authentication on a Switch on page 95](#)

Configuring Static MAC Bypass of Authentication (CLI Procedure)

You can configure a static MAC bypass list (sometimes called the exclusion list) on the switch to specify MAC addresses of devices allowed access to the LAN without 802.1X or MAC RADIUS authentication requests to the RADIUS server.

To configure the static MAC bypass list:

- Specify a MAC address to bypass authentication:

```
[edit protocols dot1x]  
user@switch# set authenticator static 00:04:0f:fd:ac:fe
```
- Configure a supplicant to bypass authentication if connected through a particular interface:

```
[edit protocols dot1x]  
user@switch# set authenticator static 00:04:0f:fd:ac:fe interface ge-0/0/5
```
- You can configure a supplicant to be moved to a specific VLAN after it is authenticated:

```
[edit protocols dot1x]  
user@switch# set authenticator static 00:04:0f:fd:ac:fe interface ge-0/0/5 vlan-assignment  
default-vlan
```

Related Documentation

- [Example: Configuring Static MAC Bypass of Authentication on a Switch on page 95](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 22](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)

Example: Configuring Static MAC Bypass of Authentication on a Switch

To allow devices to access your LAN through 802.1X-configured interfaces without authentication, you can configure a static MAC bypass list on the EX Series switch. The

static MAC bypass list, also known as the *exclusion list*, specifies MAC addresses that are allowed on the switch without sending a request to an authentication server.

You can use static MAC bypass of authentication to allow connection for devices that are not 802.1X-enabled, such as printers. If a host's MAC address is compared and matched against the static MAC address list, the nonresponsive host is authenticated and an interface opened for it.

This example describes how to configure static MAC bypass of authentication for two printers:

- [Requirements on page 96](#)
- [Overview and Topology on page 96](#)
- [Configuration on page 98](#)
- [Verification on page 99](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.

Before you configure static MAC authentication, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch* or *Example: Setting Up Basic Bridging and a VLAN on the QFX Series*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

For more about ELS, see: *Getting Started with Enhanced Layer 2 Software*

- Specified the RADIUS server connections and configured an access profile on the switch. See [“Example: Connecting a RADIUS Server for 802.1X to a Switch” on page 25](#).

Overview and Topology

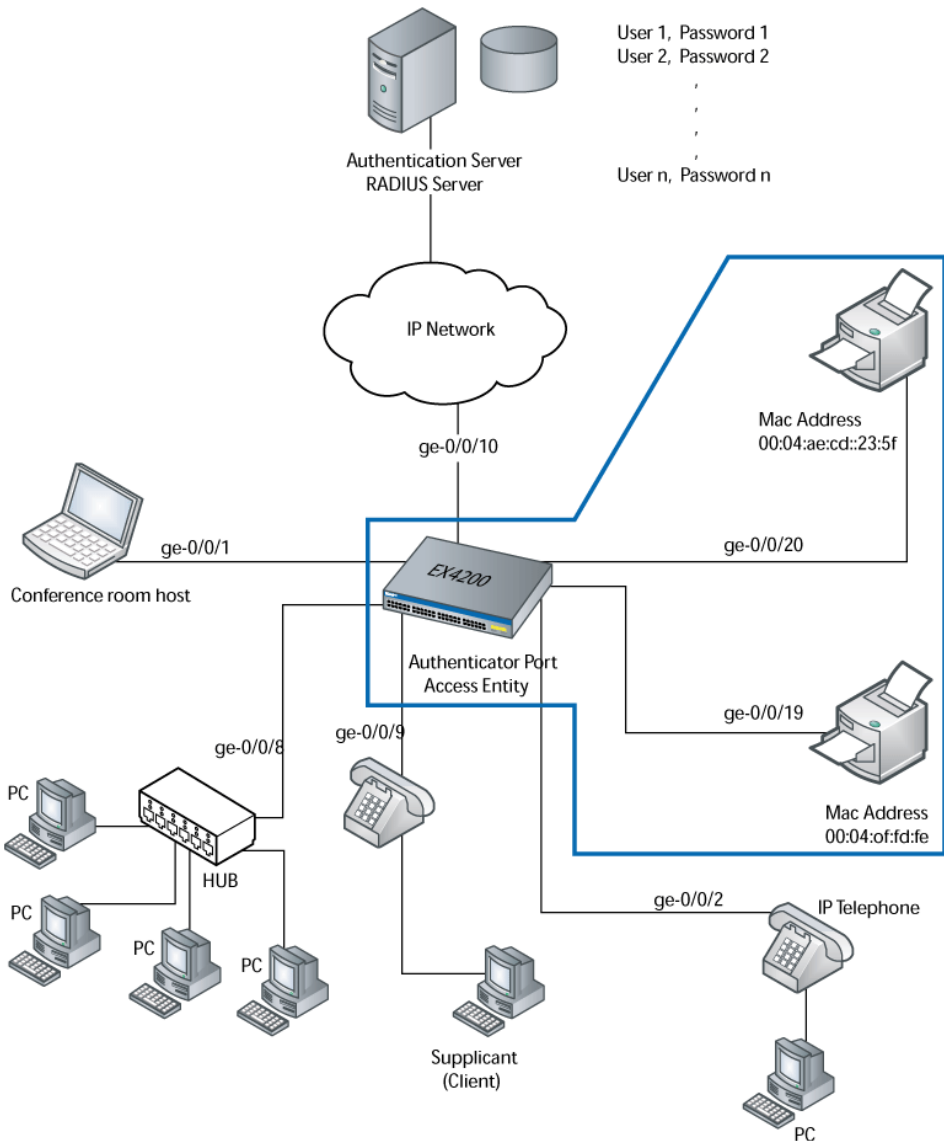
To permit printers access to the LAN, add them to the static MAC bypass list. The MAC addresses on this list are permitted access without authentication from the RADIUS server.

[Figure 12 on page 97](#) shows the two printers connected to the EX4200.



NOTE: This figure also applies to QFX5100 switches.

Figure 12: Topology for Static MAC Authentication Configuration



The interfaces shown in [Table 14 on page 97](#) will be configured for static MAC authentication.

Table 14: Components of the Static MAC Authentication Configuration Topology

Property	Settings
Switch hardware	EX4200, 24 Gigabit Ethernet ports: 8 PoE ports (ge-0/0/0 through ge-0/0/23)
VLAN name	default

Table 14: Components of the Static MAC Authentication Configuration Topology (*continued*)

Property	Settings
Connections to integrated printer/fax/copier machines (no PoE required)	ge-0/0/19 , MAC address 00:04:0f:fd:ac:fe ge-0/0/20 , MAC address 00:04:ae:cd:23:5f

The printer with the MAC address 00:04:0f:fd:ac:fe is connected to access interface **ge-0/0/19**. A second printer with the MAC address 00:04:ae:cd:23:5f is connected to access interface **ge-0/0/20**. Both printers will be added to the static list and bypass 802.1X authentication.

Configuration

CLI Quick Configuration To quickly configure static MAC authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
set protocols dot1x authenticator interface all supplicant multiple
set protocols dot1x authenticator authentication-profile-name profile1
```

Step-by-Step Procedure Configure static MAC authentication:

1. Configure MAC addresses **00:04:0f:fd:ac:fe** and **00:04:ae:cd:23:5f** as static MAC addresses:

```
[edit protocols]
user@switch# set dot1x authenticator static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
```

2. Configure the 802.1X authentication method:

```
[edit protocols]
user@switch# set dot1x authenticator interface all supplicant multiple
```

3. Configure the authentication profile name (access profile name) to use for authentication:

```
[edit protocols]
user@switch# set dot1x authenticator authentication-profile-name profile1
```



NOTE: Access profile configuration is required only for 802.1X clients, not for static MAC clients.

Results Display the results of the configuration:

```
user@switch> show
interfaces {
  ge-0/0/19 {
    unit 0 {
      family ethernet-switching {
        vlan members default;
      }
    }
  }
  ge-0/0/20 {
```

```

    unit 0 {
        family ethernet-switching {
            vlan members default;
        }
    }
}
protocols {
    dot1x {
        authenticator {
            authentication-profile-name profile1
            static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f];
            interface {
                all {
                    supplicant multiple;
                }
            }
        }
    }
}
}

```

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying Static MAC Bypass of Authentication on page 99](#)

Verifying Static MAC Bypass of Authentication

Purpose Verify that the MAC address for both printers is configured and associated with the correct interfaces.

Action Issue the operational mode command:

```
user@switch> show dot1x static-mac-address
```

MAC address	VLAN-Assignment	Interface
00:04:0f:fd:ac:fe	default	ge-0/0/19.0
00:04:ae:cd:23:5f	default	ge-0/0/20.0

Meaning The output field **MAC address** shows the MAC addresses of the two printers.

The output field **Interface** shows that the MAC address **00:04:0f:fd:ac:fe** can connect to the LAN through interface **ge-0/0/19.0** and that the MAC address **00:04:ae:cd:23:5f** can connect to the LAN through interface **ge-0/0/20.0**.

- Related Documentation**
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
 - [Configuring Static MAC Bypass of Authentication \(CLI Procedure\) on page 95](#)
 - [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 22](#)
 - [Understanding Authentication on Switches](#)

CHAPTER 6

Configuring Device Discovery Using LLDP and LLDP-MED

- Understanding 802.1X and LLDP and LLDP-MED on page 101
- Configuring LLDP (CLI Procedure) on page 104
- Configuring LLDP-MED (CLI Procedure) on page 107

Understanding 802.1X and LLDP and LLDP-MED

Juniper Networks switches use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information allows the switch to quickly identify a variety of devices, resulting in a LAN that interoperates smoothly and efficiently.

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

LLDP-MED goes one step further than LLDP, exchanging IP-telephony messages between the switch and the IP telephone.



NOTE: If your IP telephone is configured for voice over IP (VoIP), the switch automatically detects the configuration and assigns the telephone to the voice VLAN. The implementation of a voice VLAN on an IP telephone is vendor-specific. Consult the documentation that came with your IP telephone for instructions on configuring a voice VLAN. For example, on an Avaya phone, you can ensure that the phone gets the correct VoIP VLAN ID even in the absence of LLDP-MED by enabling DHCP option 176.

LLDP and LLDP-MED also provide PoE power management capabilities. LLDP power negotiation allows the switch to manage PoE power by negotiating with LLDP-enabled powered devices to dynamically allocate PoE power as needed. LLDP power priority allows an LLDP-enabled powered device to set the PoE power priority on the switch interface to which it connects.



NOTE: PoE is not supported on QFX5100 switches.

The switch also uses these protocols to ensure that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p CoS and 802.1Q tag information can be sent to the IP telephone.

EX Series switches and QFX5100 switches support the following basic TLVs:

- **Chassis Identifier**—The MAC address associated with the local system.



NOTE: The Chassis ID TLV has a subtype for Network Address Family. LLDP frames are validated only if this subtype has a value of 1 (IPv4) or 2 (IPv6). For any other value, the transmitting device is detected by LLDP as a neighbor and displayed in the output of the "show lldp neighbors" command, but is not assigned to the VLAN.

- **Port Identifier**—The port identification for the specified port in the local system.
- **Port Description**—Textual description of the interface or the logical unit. The description for the logical unit is used, if available; otherwise, the Port Description TLV will contain the description configured on the physical interface. For example, LAG member interfaces do not contain a logical unit, so only the description configured on the physical interface can be used.
- **System Name**—The user-configured name of the local system. The system name can be a maximum of 256 characters.
- **System Description**—The system description containing information about the software and current image running on the system. This information is not configurable, but taken from the software.
- **System Capabilities**—The primary function performed by the system. The capabilities that system supports; for example, bridge or router. This information is not configurable, but based on the model of the product.
- **Management Address**—The IPv4 or IPv6 management address of the local system.

EX Series switches and QFX5100 switches support the following 802.3 TLVs:

- **Power via MDI**—A TLV that advertises MDI power support, PSE power pair, and power class information.
- **MAC/PHY Configuration Status**—A TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information is not configurable, but based on the physical interface structure.



NOTE: The MAC/PHY Configuration Status TLV has a subtype for the PMD Auto-Negotiation Advertised Capability field. This field will contain a value of **other** or **unknown** if the LLDP packet was transmitted from a 10-gigabit SFP+ port.

- **Link Aggregation**—A TLV that advertises if the port is aggregated and its aggregated port ID.
- **Maximum Frame Size**—A TLV that advertises the Maximum Transmission Unit (MTU) of the interface sending LLDP frames.
- **Port Vlan**—A TLV that advertises the VLAN name configured on the interface.

EX Series switches and QFX5100 switches support the following LLDP-MED TLVs:

- **LLDP MED Capabilities**—A TLV that advertises the primary function of the port. The capabilities values range 0 through 15:
 - **0**—Capabilities
 - **1**—Network Policy
 - **2**—Location Identification
 - **3**—Extended Power via MDI-PSE
 - **4**—Inventory
 - **5–15**—Reserved
- **LLDP-MED Device Class Values:**
 - **0**—Class not defined.
 - **1**—Class 1 Device.
 - **2**—Class 2 Device.
 - **3**—Class 3 Device.
 - **4**—Network Connectivity Device
 - **5–255**—Reserved.
- **Network Policy**—A TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types, such as voice or streaming video, 802.1Q VLAN tagging, and 802.1p priority bits and Diffserv code points.
- **Endpoint Location**—A TLV that advertises the physical location of the endpoint.
- **Extended Power via MDI**—A TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.

- Related Documentation**
- [Understanding Layer 2 Protocol Tunneling on EX Series Switches](#)
 - [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
 - [Configuring LLDP \(CLI Procedure\) on page 104](#)
 - [Configuring LLDP-MED \(CLI Procedure\) on page 107](#)
 - [Understanding PoE on EX Series Switches](#)

Configuring LLDP (CLI Procedure)

Devices use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information enables the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.

This topic describes:

- [Enabling LLDP on Interfaces on page 104](#)
- [Adjusting LLDP Advertisement Settings on page 105](#)
- [Adjusting SNMP Notification Settings of LLDP Changes on page 105](#)
- [Specifying a Management Address for the LLDP Management TLV on page 106](#)
- [Configuring LLDP Power Negotiation on page 106](#)

Enabling LLDP on Interfaces

LLDP is enabled on all interfaces by default. If it is disabled, you can enable LLDP by configuring it on all interfaces or on specific interfaces.

- To configure LLDP on all interfaces:

```
[edit protocols lldp]
user@switch# set interface all
```

- To configure LLDP on a specific interface:

```
[edit protocols lldp]
user@switch# set interface interface-name
```



NOTE: On EX4300 and QFX5100 switches, LLDP cannot be configured on the me0 or vme interface. Issuing the command `set protocols lldp interface me0` generates the following error message:

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

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

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

Adjusting LLDP Advertisement Settings

You can adjust the following settings for LLDP advertisements for troubleshooting or verification purposes. The default values are applied when LLDP is enabled. For normal operations, we recommend that you do not change the default values.

- To specify the frequency at which LLDP advertisements are sent (in seconds):

```
[edit protocols lldp]
user@switch# set advertisement-interval seconds
```

For example, using the default value:

```
[edit protocols lldp]
user@switch# set advertisement-interval 45
```

- To specify the number of seconds that LLDP information is held before it is discarded (the multiplier value is used in combination with the **advertisement-interval** value):

```
[edit protocols lldp]
user@switch# set hold-multiplier seconds
```

For example, using the default value:

```
[edit protocols lldp]
user@switch# set hold-multiplier 5
```

- To specify the number of seconds the device delays before sending advertisements to neighbors after a change is made in a TLV (type, length, or value) element in LLDP or in the state of the local system, such as a change in hostname or management address, set the transmit delay. The transmit delay is enabled by default on switches to reduce the delay in notifying neighbors of a change in the local system. The default value is 2 seconds (if the **advertisement-interval** value is set to 8 seconds or more) or 1 second (if the **advertisement-interval** value is set to less than 8 seconds).

```
[edit protocols lldp]
user@switch# set transmit-delay seconds
```

For example:

```
[edit protocols lldp]
user@switch# set transmit-delay 2
```



NOTE: The advertisement-interval value must be greater than or equal to four times the transmit-delay value; otherwise, an error is returned when you attempt to commit the configuration.

Adjusting SNMP Notification Settings of LLDP Changes

You can adjust the following settings for SNMP notifications of LLDP changes. If the values are not specified or if the interval values are set to 0, the notifications are disabled.

- To specify the frequency at which LLDP database changes are sent (in seconds):

```
[edit protocols lldp]
user@switch# set lldp-configuration-notification-interval seconds
```

For example:

```
[edit protocols lldp]
user@switch# set lldp-configuration-notification-interval 600
```

- To configure the time interval for SNMP trap notifications to wait for topology changes (in seconds):

```
[edit protocols lldp]
user@switch# set ptopo-configuration-trap-interval seconds
```

For example:

```
[edit protocols lldp]
user@switch# set ptopo-configuration-trap-interval 600
```

- To specify the holding time (used in combination with the **ptopo-configuration-trap-interval** value) to maintain dynamic topology entries (in seconds):

```
[edit protocols lldp]
user@switch# set ptopo-configuration-maximum-hold-time seconds
```

For example:

```
[edit protocols lldp]
user@switch# set ptopo-configuration-maximum-hold-time 2147483647
```

Specifying a Management Address for the LLDP Management TLV

You can configure an IPv4 or IPv6 management address to be used in the LLDP Management Address type, length, and value (TLV) messages. Only out-of-band management addresses must be used as the value for the **management-address** statement.

To configure the management address:

```
[edit protocols lldp]
user@switch# set management-address ip-address
```



NOTE: Ensure that the interface with the configured management address has LLDP enabled using the **set protocols lldp interface** command. If you configure a customized management address for LLDP on an interface that has LLDP disabled, the **show lldp local-information** command output will not display the correct interface information.

Configuring LLDP Power Negotiation

LLDP power negotiation enables the switch's Power over Ethernet (PoE) controller to dynamically allocate PoE power to PoE interfaces, based on the needs of the powered device, by negotiating with LLDP-enabled powered devices.



NOTE: LLDP power negotiation is not supported on EX3200 and EX4200 (except EX4200-24P and EX4200-48P models) switches.

LLDP power negotiation is supported on switches running PoE controller software version 4.04 or later. For information about upgrading the PoE controller software, see *Upgrading the PoE Controller Software*.

LLDP power negotiation is automatically enabled when the PoE management mode is set to **class**.

- To disable LLDP power negotiation on switch interfaces:

```
[edit protocols lldp interface all power-negotiation]
user@switch# disable
```

- To disable LLDP power negotiation on a specific switch interface:

```
[edit protocols lldp interface interface-name power-negotiation]
user@switch# disable
```

**Related
Documentation**

- [Configuring LLDP \(J-Web Procedure\)](#)
- [Configuring LLDP-MED \(CLI Procedure\) on page 107](#)
- [Understanding 802.1X and LLDP and LLDP-MED on page 101](#)

Configuring LLDP-MED (CLI Procedure)

Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) is an extension of LLDP. The switch uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations.

LLDP-MED is turned on by default.

This topic describes:

- [Enabling LLDP-MED on Interfaces on page 107](#)
- [Configuring Location Information Advertised by the Switch on page 108](#)
- [Configuring for Fast Start on page 108](#)

Enabling LLDP-MED on Interfaces

LLDP-MED is enabled on all interfaces by default. If it is disabled, you can enable LLDP-MED by configuring it on all interfaces or on specific interfaces.



NOTE: On switches running Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style, configure LLDP-MED on the physical interface—for example, on ge-0/0/2. For more about ELS, see *Getting Started with Enhanced Layer 2 Software*.

To configure LLDP-MED on all interfaces or on a specific interface:

```
[edit protocols lldp-med]
user@switch# set interface (LLDP-MED) ge-0/0/2.0
```

Configuring Location Information Advertised by the Switch

You can configure the location information that is advertised from the switch to the LLDP-MED device. You can specify a civic-based location (geographic location) or a location based on an ELIN (Emergency Location Identification Number):

- To specify a location by geography:

```
[edit protocols lldp-med]
user@switch# set interface ge-0/0/2.0 location civic-based country-code US
user@switch# set interface ge-0/0/2.0 location civic-based ca-type 1 ca-value "El Dorado
County"
user@switch# set interface ge-0/0/2.0 location civic-based ca-type 2 ca-value CA
user@switch# set interface ge-0/0/2.0 location civic-based ca-type 3 ca-value Somerset
user@switch# set interface ge-0/0/2.0 location civic-based ca-type 6 ca-value "Mount Aukum
Road"
user@switch# set interface ge-0/0/2.0 location civic-based ca-type 19 ca-value 6450
user@switch# set interface ge-0/0/2.0 location civic-based ca-type 21 ca-value "Holiday
Market"
```

- To specify a location using an elin string:

```
[edit protocols lldp-med]
user@switch# set interface ge-0/0/2.0 location elin 4085551212
```

Configuring for Fast Start

You can specify the number of LLDP-MED advertisements sent from the switch in the first second after it has detected an LLDP-MED device. The default is 3; to set it to another value:

```
[edit protocols lldp-med]
user@switch# set fast-start 6
```



NOTE: If an interface is configured as a VoIP interface, then the switch does not wait for an attached phone to identify itself as an LLDP-MED device before it performs an LLDP-MED fast start after a graceful Routing Engine switchover (GRES) or a reboot. Instead, it immediately performs an LLDP-MED fast start after a GRES or reboot. This behavior prevents certain models of IP phones from resetting after a GRES.

Related Documentation

- [Configuring LLDP \(J-Web Procedure\)](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on a Switch on page 111](#)
- [Configuring LLDP \(CLI Procedure\) on page 104](#)
- [Understanding 802.1X and LLDP and LLDP-MED on page 101](#)

CHAPTER 7

Configuring VoIP

- [Understanding 802.1X and VoIP on page 109](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on a Switch on page 111](#)
- [Example: Configuring VoIP on a Switch Without Including 802.1X Authentication on page 120](#)

Understanding 802.1X and VoIP

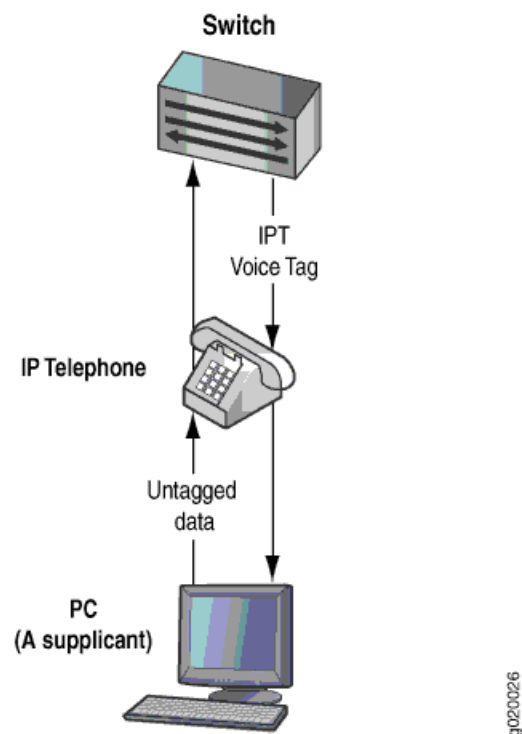
When you use Voice over IP (VoIP), you can connect IP telephones to the switch and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. The 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.

VoIP is a protocol used for the transmission of voice through packet-switched networks. VoIP transmits voice calls using a network connection instead of an analog phone line.

When VoIP is used with 802.1X, the RADIUS server authenticates the phone, and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) provides the class-of-service (CoS) parameters to the phone.

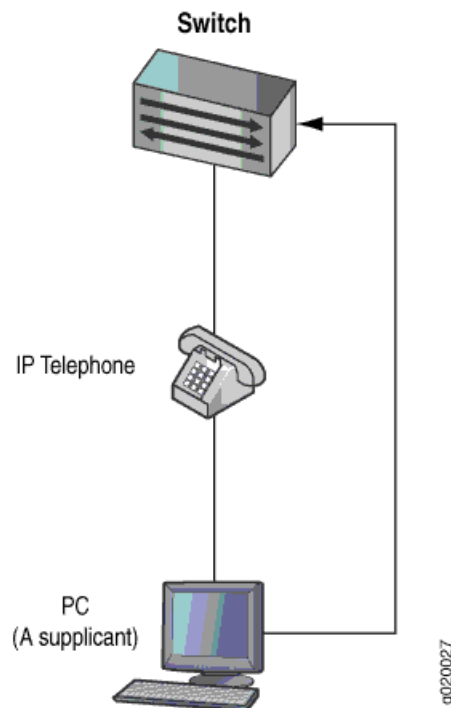
You can configure 802.1X authentication to work with VoIP in multiple supplicant or single supplicant mode. In *multiple-supplicant* mode, the 802.1X process allows multiple supplicants to connect to the interface. Each supplicant will be authenticated individually. For an example of a VoIP multiple supplicant topology, see [Figure 13 on page 110](#).

Figure 13: VoIP Multiple Supplicant Topology



If an 802.1X-compatible IP telephone does not have an 802.1X host but has another 802.1X-compatible device connected to its data port, you can connect the phone to an interface in single-supplicant mode. In *single-supplicant* mode, the 802.1X process authenticates only the first supplicant. All other supplicants who connect later to the interface are allowed full access without any further authentication. They effectively “piggyback” on the first supplicant’s authentication. For an example of a VoIP single supplicant topology, see [Figure 14 on page 111](#).

Figure 14: VoIP Single Supplicant Topology



If an IP telephone does not support 802.1X, you can configure VoIP to bypass 802.1X and LLDP-MED and have the packets forwarded to a VoIP VLAN,

Related Documentation

- [Understanding 802.1X and LLDP and LLDP-MED on page 101](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
- [Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication](#)
- [Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support](#)

Example: Setting Up VoIP with 802.1X and LLDP-MED on a Switch



NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style but also applies to QFX5100 switches. If your switch runs software that does not support ELS, see [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#). For ELS details, see [Getting Started with Enhanced Layer 2 Software](#).

You can configure voice over IP (VoIP) on a switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol forwards VoIP parameters from the switch to the phone. You also configure 802.1X authentication to allow the telephone access to the LAN. Authentication is done through a backend RADIUS server.

This example describes how to configure VoIP on a switch to support an Avaya IP phone, as well as the LLDP-MED protocol and 802.1X authentication:

- [Requirements on page 112](#)
- [Overview and Topology on page 113](#)
- [Configuration on page 115](#)
- [Verification on page 117](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 13.2X50 or later for EX Series switches
- One EX4300 switch acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An Avaya IP telephone that supports LLDP-MED and 802.1X

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See the installation information for your switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch* or *Example: Setting Up Basic Bridging and a VLAN on the QFX Series*.
- Configured the RADIUS server for 802.1X authentication and set up the access profile. See [“Example: Connecting a RADIUS Server for 802.1X to a Switch” on page 25](#).
- (Optional) Configured the interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see *Configuring PoE on EX Series Switches (CLI Procedure)*.



NOTE: If the IP address is not configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the `voip` statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN's ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).

Overview and Topology

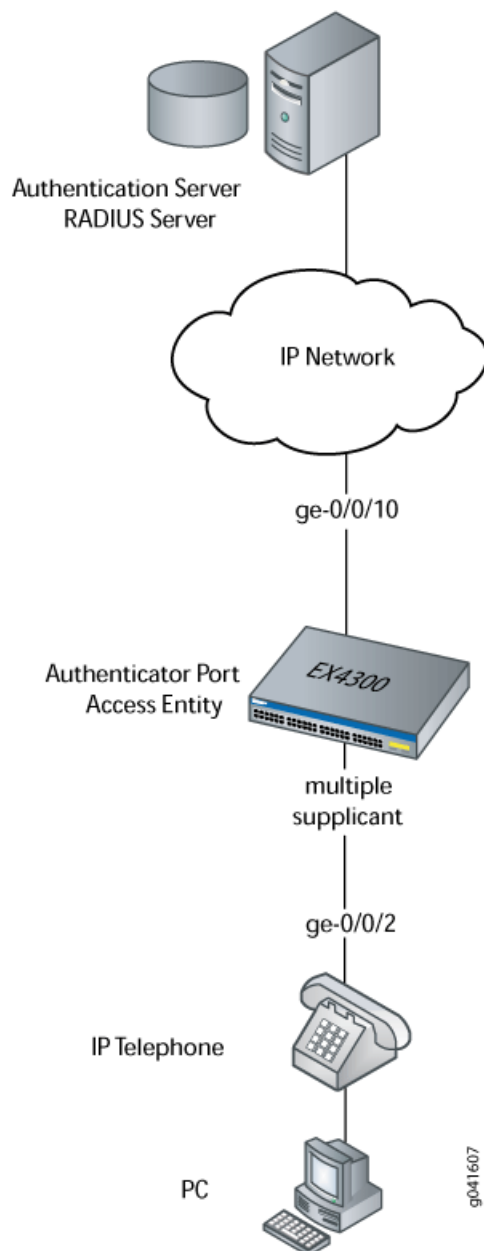
Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

In this example, the access interface ge-0/0/2 on the EX4300 switch is connected to an Avaya IP telephone. Avaya phones have a built-in bridge that allows you to connect a desktop PC to the phone, so the desktop and phone in a single office require only one interface on the switch. The EX Series switch is connected to a RADIUS server on the ge-0/0/10 interface (see [Figure 15 on page 114](#)).



NOTE: This figure also applies to QFX5100 switches.

Figure 15: VoIP Topology



In this example, you configure VoIP parameters and specify the forwarding class **assured-forward** for voice traffic to provide the highest quality of service.

Table 15 on page 114 describes the components used in this VoIP configuration example.

Table 15: Components of the VoIP Configuration Topology

Property	Settings
Switch hardware	EX4300 switch

Table 15: Components of the VoIP Configuration Topology (*continued*)

Property	Settings
VLAN names	data-vlan voice-vlan
Connection to Avaya phone—with integrated hub, to connect phone and desktop PC to a single interface (requires PoE)	ge-0/0/2
One RADIUS server	Provides backend database connected to the switch through interface ge-0/0/10 .

As well as configuring a VoIP for interface ge-0/0/2, you configure:

- 802.1X authentication. Authentication is set to **multiple** supplicant mode to support more than one supplicant's access to the LAN through interface ge-0/0/2.
- LLDP-MED protocol information. The switch uses LLDP-MED to forward VoIP parameters to the phone. Using LLDP-MED ensures that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p class of service and 802.1Q tag information can be sent to the IP telephone.



NOTE: A PoE configuration is not necessary if an IP telephone is using a power adapter.

Configuration

CLI Quick Configuration

To quickly configure VoIP, LLDP-MED, and 802.1X, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan switch-options interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set switch-options voip interface ge-0/0/2.0 vlan voice-vlan
set switch-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Step-by-Step Procedure

To configure VoIP with LLDP-MED and 802.1X:

1. Configure the VLANs for voice and data:


```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```
2. Associate the VLAN **data-vlan** with the interface:


```
[edit vlans]
user@switch# set data-vlan switch-options interface ge-0/0/2.0
```
3. Configure the interface as an access interface, configure support for Ethernet switching, and add the **data-vlan** VLAN:

- ```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching interface-mode access
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
```
4. Configure VoIP on the interface and specify the **assured-forwarding** forwarding class to provide the most dependable class of service:

```
[edit switch-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```
  5. Configure LLDP-MED protocol support:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/2
```
  6. To authenticate an IP phone and a PC connected to the IP phone on the interface, configure 802.1X authentication support and specify **multiple** supplicant mode:



**NOTE:** If you do not want to authenticate any device, skip the 802.1X configuration on this interface.

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

**Results** Display the results of the configuration:

```
[edit]
user@switch# show configuration
interfaces {
 ge-0/0/2 {
 unit 0 {
 family ethernet-switching {
 interface-mode access;
 vlan {
 members data-vlan;
 }
 }
 }
 }
}
protocols {
 lldp-med {
 interface ge-0/0/2;
 }
 dot1x {
 authenticator {
 interface {
 ge-0/0/2.0 {
 supplicant multiple;
 }
 }
 }
 }
}
vllans {
 data-vlan {
```

```
 vlan-id 77;
 switch-options {
 interface ge-0/0/2.0;
 }
}
voice-vlan {
 vlan-id 99;
}
}
switch-options {
 voip {
 interface ge-0/0/2.0 {
 vlan voice-vlan;
 forwarding-class assured-forwarding;
 }
 }
}
```

## Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying LLDP-MED Configuration on page 117](#)
- [Verifying 802.1X Authentication for IP Phone and Desktop PC on page 118](#)
- [Verifying the VLAN Association with the Interface on page 119](#)

### Verifying LLDP-MED Configuration

**Purpose** Verify that LLDP-MED is enabled on the interface.

**Action** user@switch> `show lldp detail`

```
LLDP : Enabled
Advertisement interval : 30 seconds
Transmit delay : 2 seconds
Hold timer : 120 seconds
Notification interval : 0 Second(s)
Config Trap Interval : 0 seconds
Connection Hold timer : 300 seconds
```

```
LLDP MED : Enabled
MED fast start count : 3 Packets
```

```
Port ID TLV subtype : locally-assigned
```

| Interface      | Parent Interface | LLDP    | LLDP-MED | Power Negotiation |
|----------------|------------------|---------|----------|-------------------|
| Neighbor count |                  |         |          |                   |
| all            | -                | Enabled | Enabled  | Enabled           |
| 0              |                  |         |          |                   |
| ge-0/0/2       | -                | -       | Enabled  | -                 |
| 0              |                  |         |          |                   |

| Interface | Parent Interface | Vlan-id | Vlan-name |
|-----------|------------------|---------|-----------|
| ge-0/0/0  | -                | 1       | vlan-1    |
| ge-0/0/1  | -                | 1       | vlan-1    |
| ge-0/0/2  | -                | 77      | vlan-77   |
| ge-0/0/2  | -                | 99      | vlan-99   |
| ge-0/0/3  | -                | 1       | vlan-1    |
| ge-0/0/4  | -                | 1       | vlan-1    |
| ge-0/0/5  | -                | 1       | vlan-1    |
| ge-0/0/6  | -                | 1       | vlan-1    |
| ge-0/0/7  | -                | 1       | vlan-1    |
| ge-0/0/8  | -                | 1       | vlan-1    |
| ge-0/0/9  | -                | 1       | vlan-1    |
| ge-0/0/10 | -                | 1       | vlan-1    |

Basic Management TLVs supported:  
End Of LLDPDU, Chassis ID, Port ID, Time To Live, Port Description, System Name,  
System Description, System Capabilities, Management Address

Organizationally Specific TLVs supported:  
MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum Frame Size,  
Port VLAN tag, Port VLAN name.

**Meaning** The `show lldp detail` output shows that both LLDP and LLDP-MED are configured on the ge-0/0/2 interface. The end of the output shows the list of supported LLDP basic management TLVs and organizationally specific TLVs that are supported.

### Verifying 802.1X Authentication for IP Phone and Desktop PC

**Purpose** Display the 802.1X configuration to confirm that the VoIP interface has access to the LAN.

**Action** user@switch> `show dot1x interface ge-0/0/2.0 detail`  
 ge-0/0/2.0  
 Role: Authenticator  
 Administrative state: Auto  
 Supplicant mode: Multiple  
 Number of retries: 3  
 Quiet period: 60 seconds  
 Transmit period: 30 seconds  
 Mac Radius: Disabled  
 Mac Radius Restrict: Disabled  
 Reauthentication: Enabled  
 Configured Reauthentication interval: 3600 seconds  
 Supplicant timeout: 30 seconds  
 Server timeout: 30 seconds  
 Maximum EAPOL requests: 2  
 Guest VLAN member: <not configured>  
 Number of connected supplicants: 1  
 Supplicant: user101, 00:04:0f:fd:ac:fe  
 Operational state: Authenticated  
 Authentication method: Radius  
 Authenticated VLAN: vo11  
 Dynamic Filter: match source-dot1q-tag 10 action deny  
 Session Reauth interval: 60 seconds  
 Reauthentication due in 50 seconds

**Meaning** The field **Role** shows that the ge-0/0/2.0 interface is in the authenticator state. The **Supplicant** field shows that the interface is configured in multiple supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

### Verifying the VLAN Association with the Interface

**Purpose** Display the interface's VLAN membership.

**Action** user@switch> `show ethernet-switching interface ge-0/0/2.0`  
 Routing Instance Name : default-switch  
 Logical Interface flags (DL - disable learning, AD - packet action drop,  
 LH - MAC limit hit, DN - interface down )  

| Logical interface | Vlan members  | TAG | MAC limit | STP state  | Logical interface flags | Tagging  |
|-------------------|---------------|-----|-----------|------------|-------------------------|----------|
| ge-0/0/2.0        | voice-vlan 99 |     | 65535     |            |                         | untagged |
|                   |               |     | 65535     | Discarding |                         |          |
|                   | data-vlan 77  |     | 65535     | Discarding |                         |          |

**Meaning** The field **VLAN members** shows that the ge-0/0/2.0 interface supports both the **data-vlan** VLAN and **voice-vlan** VLAN.

**Related Documentation**

- [Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25](#)
- [Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31](#)
- [Defining CoS Forwarding Classes \(CLI Procedure\)](#)

- [Defining CoS Forwarding Classes \(J-Web Procedure\)](#)
- [Configuring LLDP-MED \(CLI Procedure\) on page 107](#)

## Example: Configuring VoIP on a Switch Without Including 802.1X Authentication

---



**NOTE:** This example uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

You can configure voice over IP (VoIP) on a switch to support IP telephones.

To configure VoIP on an EX Series switch to support an IP phone that does not support 802.1X authentication, you must either add the MAC address of the phone to the static MAC bypass list or enable MAC RADIUS authentication on the switch.

This example describes how to configure VoIP on a switch without 802.1X authentication by using static MAC bypass of authentication:

- [Requirements on page 120](#)
- [Overview on page 121](#)
- [Configuration on page 121](#)
- [Verification on page 123](#)

### Requirements

This example uses the following hardware and software components:



**NOTE:** This figure also applies to QFX5100 switches.

- One EX4300 switch.
- Junos OS Release 13.2 or later for EX Series switches
- An Avaya IP telephone

Before you configure VoIP, be sure you have:

- Installed your switch. See the installation information for your switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch* or *Example: Setting Up Basic Bridging and a VLAN on the QFX Series*.

- Configured the RADIUS server for 802.1X authentication and set up the access profile. See [“Example: Connecting a RADIUS Server for 802.1X to a Switch” on page 25](#).
- (Optional) Configured the interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see *Configuring PoE on EX Series Switches (CLI Procedure)*.



**NOTE:** If the IP address is not configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the `voip` statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN's ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).

## Overview

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

In this example, the access interface ge-0/0/2 on the EX4300 switch is connected to a non-802.1X IP phone.

To configure VoIP on an EX Series switch to support an IP phone that does not support 802.1X authentication, add the MAC address of the phone as a static entry in the authenticator database and set the supplicant mode to multiple.

## Configuration

### CLI Quick Configuration

To quickly configure VoIP without using 802.1X authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan switch-options interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set switch-options voip interface ge-0/0/2.0 vlan voice-vlan
set switch-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2
set protocols dot1x authenticator authentication-profile-name auth-profile
set protocols dot1x authenticator static 00:04:f2:11:aa:a7
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

**Step-by-Step Procedure**

To configure VoIP without 802.1X authentication:

1. Configure the VLANs for voice and data:  

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```
2. Associate the VLAN **data-vlan** with the interface:  

```
[edit vlans]
user@switch# set data-vlan switch-options interface ge-0/0/2.0
```
3. Configure the interface as an access interface, configure support for Ethernet switching, and add the **data-vlan** VLAN:  

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching interface-mode access
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
```
4. Configure VoIP on the interface and specify the **assured-forwarding** forwarding class to provide the most dependable class of service:  

```
[edit switch-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```
5. Configure LLDP-MED protocol support:  

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/2
```
6. Set the authentication profile (see [“Configuring 802.1X Interface Settings \(CLI Procedure\)” on page 22](#) and [“Configuring 802.1X RADIUS Accounting \(CLI Procedure\)” on page 67](#)):  

```
[edit protocols]
set dot1x authenticator authentication-profile-name auth-profile
```
7. Add the MAC address of the phone to the static MAC bypass list:  

```
[edit protocols]
set dot1x authenticator static 00:04:f2:11:aa:a7
```
8. Set the supplicant mode to **multiple**:  

```
[edit protocols]
set dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

**Results**

Display the results of the configuration:

```
[edit]
user@switch# show configuration
interfaces {
 ge-0/0/2 {
 unit 0 {
 family ethernet-switching {
 interface-mode access;
 vlan {
 members data-vlan;
 }
 }
 }
 }
}
protocols {
```

```

lldp-med {
 interface ge-0/0/2;
}
dot1x {
 authenticator {
 authentication-profile-name auth-profile;
 static {
 00:04:f2:11:aa:a7;
 }
 }
 interface {
 ge-0/0/2.0 {
 supplicant multiple;
 }
 }
}
vlls {
 data-vlan {
 vlan-id 77;
 switch-options {
 interface ge-0/0/2.0;
 }
 }
 voice-vlan {
 vlan-id 99;
 }
}
switch-options {
 voip {
 interface ge-0/0/2.0 {
 vlan voice-vlan;
 forwarding-class assured-forwarding;
 }
 }
}
}

```

## Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying LLDP-MED Configuration on page 123](#)
- [Verifying Authentication for the Desktop PC on page 124](#)
- [Verifying the VLAN Association with the Interface on page 125](#)

### Verifying LLDP-MED Configuration

**Purpose** Verify that LLDP-MED is enabled on the interface.

**Action** user@switch> `show lldp detail`

```
LLDP : Enabled
Advertisement interval : 30 seconds
Transmit delay : 2 seconds
Hold timer : 120 seconds
Notification interval : 0 Second(s)
Config Trap Interval : 0 seconds
Connection Hold timer : 300 seconds
```

```
LLDP MED : Enabled
MED fast start count : 3 Packets
```

```
Port ID TLV subtype : locally-assigned
```

| Interface      | Parent Interface | LLDP    | LLDP-MED | Power Negotiation |
|----------------|------------------|---------|----------|-------------------|
| Neighbor count |                  |         |          |                   |
| all            | -                | Enabled | Enabled  | Enabled           |
| 0              |                  |         |          |                   |
| ge-0/0/2       | -                | -       | Enabled  | -                 |
| 0              |                  |         |          |                   |

| Interface | Parent Interface | Vlan-id | Vlan-name |
|-----------|------------------|---------|-----------|
| ge-0/0/0  | -                | 1       | vlan-1    |
| ge-0/0/1  | -                | 1       | vlan-1    |
| ge-0/0/2  | -                | 77      | vlan-77   |
| ge-0/0/2  | -                | 99      | vlan-99   |
| ge-0/0/3  | -                | 1       | vlan-1    |
| ge-0/0/4  | -                | 1       | vlan-1    |
| ge-0/0/5  | -                | 1       | vlan-1    |
| ge-0/0/6  | -                | 1       | vlan-1    |
| ge-0/0/7  | -                | 1       | vlan-1    |
| ge-0/0/8  | -                | 1       | vlan-1    |
| ge-0/0/9  | -                | 1       | vlan-1    |
| ge-0/0/10 | -                | 1       | vlan-1    |

Basic Management TLVs supported:  
End Of LLDPDU, Chassis ID, Port ID, Time To Live, Port Description, System Name,  
System Description, System Capabilities, Management Address

Organizationally Specific TLVs supported:  
MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum Frame Size,  
Port VLAN tag, Port VLAN name.

**Meaning** The `show lldp detail` output shows that both LLDP and LLDP-MED are configured on the ge-0/0/2 interface. The end of the output shows the list of supported LLDP basic management TLVs and organizationally specific TLVs that are supported.

### Verifying Authentication for the Desktop PC

**Purpose** Display the 802.1X configuration for the desktop PC connected to the VoIP interface through the IP phone.

**Action** user@switch> `show dot1x interface ge-0/0/2.0 detail`

```

ge-0/0/2.0
 Role: Authenticator
 Administrative state: Auto
 Supplicant mode: Multiple
 Number of retries: 3
 Quiet period: 60 seconds
 Transmit period: 30 seconds
 Mac Radius: Disabled
 Mac Radius Restrict: Disabled
 Reauthentication: Enabled
 Configured Reauthentication interval: 3600 seconds
 Supplicant timeout: 30 seconds
 Server timeout: 30 seconds
 Maximum EAPOL requests: 2
 Guest VLAN member: <not configured>
 Number of connected supplicants: 1
 Supplicant: user101, 00:04:0f:fd:ac:fe
 Operational state: Authenticated
 Authentication method: Radius
 Authenticated VLAN: vo11
 Dynamic Filter: match source-dot1q-tag 10 action deny
 Session Reauth interval: 60 seconds
 Reauthentication due in 50 seconds

```

**Meaning** The field **Role** shows that the ge-0/0/2.0 interface is in the authenticator state. The **Supplicant** field shows that the interface is configured in multiple supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

### Verifying the VLAN Association with the Interface

**Purpose** Display the interface's VLAN membership.

**Action** user@switch> `show ethernet-switching interface ge-0/0/2.0`

```

Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
 LH - MAC limit hit, DN - interface down)

```

| Logical interface | Vlan members  | TAG | MAC limit | STP state  | Logical interface flags | Tagging  |
|-------------------|---------------|-----|-----------|------------|-------------------------|----------|
| ge-0/0/2.0        | voice-vlan 99 |     | 65535     |            |                         | untagged |
|                   |               |     | 65535     | Discarding |                         |          |
|                   | data-vlan 77  |     | 65535     | Discarding |                         |          |

**Meaning** The field **VLAN members** shows that the ge-0/0/2.0 interface supports both the **data-vlan** VLAN and **voice-vlan** VLAN.

**Related Documentation**

- [Example: Setting Up VoIP with 802.1X and LLDP-MED on a Switch on page 111](#)
- [Understanding 802.1X and VoIP on page 109](#)
- [Understanding 802.1X and LLDP and LLDP-MED on page 101](#)



## CHAPTER 8

# Configuring and Managing Root Users

- [Configuring Management Access on page 127](#)
- [Configuring Access Privilege Levels on page 127](#)
- [Configuring Login Tips on page 128](#)
- [Recovering the Root Password on page 128](#)
- [Example: Configuring a Plain-Text Password for Root Logins on page 130](#)
- [Example: Configuring SSH Authentication for Root Logins on page 132](#)
- [Understanding Troubleshooting Resources on page 132](#)
- [Troubleshooting Overview on page 134](#)
- [Recovering the Root Password on page 136](#)

### Configuring Management Access

---

To define the management access settings for the routing platform:

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

#### Related Documentation

- [Configuring Junos OS User Accounts on page 169](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands](#)
- [Example: Configuring Access Privilege Levels on page 148](#)

### Configuring Access Privilege Levels

---

Each top-level command-line interface (CLI) command and each configuration statement have an access privilege level associated with it. Users can execute only those commands and configure and view only those statements for which they have access privileges.

To configure access privilege levels, include the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level:

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

**Related  
Documentation**

- [Example: Configuring Access Privilege Levels on page 148](#)
- [Understanding Junos OS Access Privilege Levels on page 9](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands](#)
- [permissions](#)

---

## Configuring Login Tips

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

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

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

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

**Related  
Documentation**

- [CLI User Interface Overview](#)
- [Defining Junos OS Login Classes](#)
- [login-tip](#)

---

## Recovering the Root Password

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



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



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

To recover the root password:

1. Power off the switch by switching off the AC power outlet of the device or, if necessary, by pulling the power cords out of the device's power supplies.
2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with the device into the RJ-45-to-DB-9 serial port adapter supplied with the device.

4. Plug the RJ-45-to-DB-9 serial port adapter into the serial port on the management device.
5. Connect the other end of the Ethernet rollover cable to the console port on the device.
6. Turn on the power to the management device.
7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate **COM** port to use (for example, **COM1**).
8. Configure the port settings as follows:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
9. Power on the device by (if necessary) plugging the power cords into the device's power supply, or turning on the power to the device by switching on the AC power outlet the device is plugged into.

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

10. When the following prompt appears, press the Spacebar to access the device's bootstrap loader command prompt:  
  
Hit [Enter] to boot immediately, or space bar for command prompt.  
Booting [kernel] in 9 seconds...
11. At the following prompt, enter **boot -s** to start up the system in single-user mode.  
  
ok **boot -s**
12. At the following prompt, enter **recovery** to start the root password recovery procedure.  
  
Enter full pathname of shell or 'recovery' for root password recovery or RETURN for /bin/sh: **recovery**
13. Enter configuration mode in the CLI.
14. Set the root password. For example:  
  
user@switch# **set system root-authentication plain-text-password**
15. At the following prompt, enter the new root password. For example:  
  
New password: **juniper1**  
Retype new password:
16. At the second prompt, reenter the new root password.
17. After you have finished configuring the password, commit the configuration.  
  
root@host# **commit**  
commit complete
18. Exit configuration mode in the CLI.

19. Exit operational mode in the CLI.
20. At the prompt, enter **y** to reboot the device.

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

**Related Documentation**

- [Configuring the Root Password](#)

---

## Example: Configuring a Plain-Text Password for Root Logins

This example shows how to configure the authentication methods for the root-level user, whose username is “root”.

- [Requirements on page 130](#)
- [Overview on page 130](#)
- [Configuration on page 130](#)
- [Verification on page 131](#)

### Requirements

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

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

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

### Overview

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

### Configuration

|                         |                                                                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| CLI Quick Configuration | [edit system]<br>set root-authentication plain-text-password<br>New password: <i>new-password</i><br>Retype new password: <i>new-password</i> |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|

### Configuring [item]

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

To configure a plain-text password:

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

```
[edit]
user@host# set system root-authentication plain-text-password
New password:
```
2. Type the new password next to the **New password:** prompt and press Enter.  

```
user@host# new-password
Retype new password:
```
3. Retype the same password next to the next prompt and press Enter.

### Results

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

```
root-authentication {
 encrypted-password "1ASwBkGYd$YUcEwgd0IO4QkRzzlQdmT/"; ## SECRET-DATA
}
```

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

After you have confirmed that the interfaces are configured, enter the **commit** command in configuration mode.

## Verification

- [Verifying the Configuration of a Plain-Text Password for Root Logins on page 131](#)

### Verifying the Configuration of a Plain-Text Password for Root Logins

**Purpose** Verify the configuration of a plain-text password.

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

```
user@host> show configuration system
root-authentication {
 encrypted-password "1ASwBkGYd$YUcEwgd0IO4QkRzzlQdmT/"; ## SECRET-DATA
}
```

**Meaning** If you use a clear-text password, Junos OS displays the password as an encrypted string so that users viewing the configuration cannot see it. As you enter the password in plain

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

**Related Documentation**

- *root-authentication*
- [Special Requirements for Junos OS Plain-Text Passwords on page 142](#)
- *Configuring Special Requirements for Plain-Text Passwords*
- *Changing the Requirements for Junos OS Plain-Text Passwords*

## Example: Configuring SSH Authentication for Root Logins

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

```
[edit system]
root-authentication {
 encrypted-password "$1$1wp5tqMX$uy/u5H7OdXTwfWTmeJWXe/";
 ## SECRET-DATA;
 ssh-dsa "2354 95 9304@boojum.per";
 ssh-dsa "0483 02 8362@ecbatana.per";
}
```

**Related Documentation**

- *Configuring the Root Password*
- [Special Requirements for Junos OS Plain-Text Passwords on page 142](#)

## Understanding Troubleshooting Resources

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

[Table 16 on page 132](#) provides a list of some of the troubleshooting resources.

**Table 16: Troubleshooting Resources on the QFX and OCX Series**

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

Table 16: Troubleshooting Resources on the QFX and OCX Series (*continued*)

| Troubleshooting Resource                      | Description                                                                                                                                                                                                                                                                                                                                                                                                | Documentation                                                                                                                                                                           |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface alarms                              | A predefined alarm (red or yellow) for an interface type is triggered when an interface of that type goes down.                                                                                                                                                                                                                                                                                            | <i>Interface Alarm Messages</i>                                                                                                                                                         |
| System alarms                                 | A predefined alarm is triggered by a missing rescue configuration or problem with the software license.                                                                                                                                                                                                                                                                                                    | <i>Understanding Alarms</i>                                                                                                                                                             |
| System log messages                           | The system log includes details of system and user events, including errors. Specify the severity and type of system log messages you wish to view or save, and configure the output to be sent to local or remote hosts.                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>• <i>Overview of Single-Chassis System Logging Configuration</i></li> <li>• <i>Junos OS System Log Configuration Statements</i></li> </ul>       |
| Junos OS operational mode commands            | Operational mode commands can be used to monitor switch performance and current activity on the network. For example, use the <b>traceroute monitor</b> command to locate points of failure in a network.                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>• <i>Monitoring System Process Information</i></li> <li>• <i>Monitoring System Properties</i></li> <li>• <i>traceroute monitor</i></li> </ul>    |
| Junos OS automation scripts (event scripts)   | Event scripts can be used to automate network troubleshooting and management tasks.                                                                                                                                                                                                                                                                                                                        | <i>Junos OS Automation Library</i>                                                                                                                                                      |
| Junos OS XML operational tags                 | XML operational tags are equivalent in function to operational mode commands in the CLI, which you can use to retrieve status information for a device.                                                                                                                                                                                                                                                    | <i>Junos XML API Operational Developer Reference</i>                                                                                                                                    |
| NETCONF XML management protocol               | The NETCONF XML management protocol defines basic operations that are equivalent to Junos OS CLI configuration mode commands. Client applications use the protocol operations to display, edit, and commit configuration statements (among other operations), just as administrators use CLI configuration mode commands such as <b>show</b> , <b>set</b> , and <b>commit</b> to perform those operations. | <i>NETCONF XML Management Protocol Developer Guide</i>                                                                                                                                  |
| SNMP MIBs and traps                           | MIBs enable the monitoring of network devices from a central location. For example, use the Traceroute MIB to monitor devices remotely.                                                                                                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>• <i>SNMP MIBs Support</i></li> <li>• <i>SNMP Traps Support</i></li> <li>• <i>Using the Traceroute MIB for SNMP Remote Operations</i></li> </ul> |
| AI-Scripts and Advanced Insight Manager (AIM) | AI-Scripts installed on the switch can automatically detect and monitor faults on the switch, and depending on the configuration on the AIM application, send notifications of potential problems and submit problem reports to Juniper Support Systems.                                                                                                                                                   | <a href="#">Advanced Insight Scripts (AI-Scripts) Release Notes</a>                                                                                                                     |

Table 16: Troubleshooting Resources on the QFX and OCX Series (*continued*)

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

## Troubleshooting Overview

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

[Table 17 on page 134](#) provides a list of problem categories, summary of the symptom or problem, and recommended actions with links to the troubleshooting documentation.

Table 17: Troubleshooting on the QFX Series

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

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

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

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

| Problem Category                   | Symptom or Problem                                                                                                                                                    | Recommended Action                                                                                                                                                                                                                                                                                       |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Software upgrade and configuration | Failed software upgrade.                                                                                                                                              | See <i>Recovering from a Failed Software Installation</i> .                                                                                                                                                                                                                                              |
|                                    | Active partition becomes inactive after upgrade.                                                                                                                      |                                                                                                                                                                                                                                                                                                          |
|                                    | Problem with the active configuration file.                                                                                                                           | See the following topics: <ul style="list-style-type: none"> <li>• <i>Loading a Previous Configuration File</i></li> <li>• <i>Reverting to the Default Factory Configuration</i></li> <li>• <i>Reverting to the Rescue Configuration</i></li> <li>• <i>Performing a Recovery Installation</i></li> </ul> |
|                                    | Root password is lost or forgotten.                                                                                                                                   | Recover the root password. See <a href="#">"Recovering the Root Password"</a> on page 128.                                                                                                                                                                                                               |
| Network interfaces                 | An aggregated Ethernet interface is down.                                                                                                                             | See <i>Troubleshooting an Aggregated Ethernet Interface</i> .                                                                                                                                                                                                                                            |
|                                    | Interface on built-in network port is down.                                                                                                                           | See <i>Troubleshooting Network Interfaces</i> .                                                                                                                                                                                                                                                          |
|                                    | Interface on port in which SFP or SFP+ transceiver is installed in an SFP+ uplink module is down.                                                                     |                                                                                                                                                                                                                                                                                                          |
| Ethernet switching                 | A MAC address entry in the Ethernet switching table is not updated after the device with that MAC address has been moved from one interface to another on the switch. | See <i>Troubleshooting Ethernet Switching</i> .                                                                                                                                                                                                                                                          |
| Firewall filter                    | Firewall configuration exceeded available Ternary Content Addressable Memory (TCAM) space.                                                                            | See <i>Troubleshooting Firewall Filter Configuration</i> .                                                                                                                                                                                                                                               |

## Recovering the Root Password

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



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



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

To recover the root password:

1. Power off the switch by switching off the AC power outlet of the device or, if necessary, by pulling the power cords out of the device's power supplies.
2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with the device into the RJ-45-to-DB-9 serial port adapter supplied with the device.
4. Plug the RJ-45-to-DB-9 serial port adapter into the serial port on the management device.
5. Connect the other end of the Ethernet rollover cable to the console port on the device.
6. Turn on the power to the management device.
7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate **COM** port to use (for example, **COM1**).
8. Configure the port settings as follows:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
9. Power on the device by (if necessary) plugging the power cords into the device's power supply, or turning on the power to the device by switching on the AC power outlet the device is plugged into.

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

10. When the following prompt appears, press the Spacebar to access the device's bootstrap loader command prompt:  
  
Hit [Enter] to boot immediately, or space bar for command prompt.  
Booting [kernel] in 9 seconds...
11. At the following prompt, enter **boot -s** to start up the system in single-user mode.  
  
ok **boot -s**
12. At the following prompt, enter **recovery** to start the root password recovery procedure.  
  
Enter full pathname of shell or 'recovery' for root password recovery or RETURN for /bin/sh: **recovery**
13. Enter configuration mode in the CLI.
14. Set the root password. For example:  
  
user@switch# **set system root-authentication plain-text-password**
15. At the following prompt, enter the new root password. For example:  
  
New password: **juniper1**  
Retype new password:

16. At the second prompt, reenter the new root password.
17. After you have finished configuring the password, commit the configuration.

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

18. Exit configuration mode in the CLI.
19. Exit operational mode in the CLI.
20. At the prompt, enter **y** to reboot the device.

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

**Related Documentation**

- *Configuring the Root Password*

## CHAPTER 9

# Configuring and Managing User Accounts

- [Junos OS User Accounts Overview on page 139](#)
- [Junos OS Login Classes Overview on page 141](#)
- [Special Requirements for Junos OS Plain-Text Passwords on page 142](#)
- [Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 144](#)
- [Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands on page 145](#)
- [Defining Access Privileges Using allow or deny configuration Statements on page 146](#)
- [Example: Configuring User Accounts on page 147](#)
- [Example: Configuring Access Privilege Levels on page 148](#)
- [Example: Configuring Access Privileges for Operational Mode Commands on page 149](#)
- [Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 149](#)
- [Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions on page 151](#)
- [Understanding Troubleshooting Resources on page 152](#)
- [Troubleshooting Overview on page 154](#)
- [Recovering the Root Password on page 156](#)

## Junos OS User Accounts Overview

---

User accounts provide one way for users to access the switch. (Users can access the switch without accounts if you configured RADIUS or TACACS+ servers, as described in [“Junos OS User Authentication Methods” on page 14](#).) For each account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

For each user account, you can define the following:

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

- User identifier (UID)—(Optional) Numeric identifier that is associated with the user account name. The identifier must be in the range from 100 through 64,000 and must be unique within the switch. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.
- You must ensure that the UID is unique. However, it is possible to assign the same UID to different users. If you do this, the CLI displays a warning when you commit the configuration and then assigns the duplicate UID.
- User's access privilege—(Required) One of the login classes you defined in the **class** statement at the **[edit system login]** hierarchy level, or one of the default classes listed in ["Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies"](#) on page 144.
- Authentication method or methods and passwords that the user can use to access the switch—(Optional) You can use SSH or a Message Digest 5 (MD5) password, or you can enter a plain-text password that Junos OS encrypts using MD5-style encryption before entering it in the password database. For each method, you can specify the user's password. If you configure the **plain-text-password** option, you are prompted to enter and confirm the password:

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

The default requirements for plain-text passwords are:

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

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

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

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

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

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

```
[edit system]
user@switch# show
root-authentication {
 ssh-rsa "1024 35 9727638204084251055468226757249864241630322
207404962528390382038690141584534964170019610608358722961563
475784918273603361276441874265946893207739108344813125957722
625461667999278316123500438660915866283822489746732605661192
181489539813862940327687806538169602027491641637359132693963
44008443 boojum@juniper.net"; # SECRET-DATA
}
```

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

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

- Related Documentation**
- [Configuring Junos OS User Accounts on page 169](#)
  - [Junos OS Login Classes Overview on page 141](#)

## Junos OS Login Classes Overview

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

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

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

The Junos operating system (Junos OS) contains a few predefined login classes, which are listed in [Table 18 on page 141](#). The predefined login classes cannot be modified.

**Table 18: Predefined System Login Classes**

| Login Class                    | Permission Flag Set                    |
|--------------------------------|----------------------------------------|
| <b>operator</b>                | clear, network, reset, trace, and view |
| <b>read-only</b>               | view                                   |
| <b>superuser or super-user</b> | all                                    |
| <b>unauthorized</b>            | None                                   |

**NOTE:**

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

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

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

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

**Related Documentation**

- Defining Junos OS Login Classes*
- Defining Junos OS Login Classes*
- Understanding QFabric System Login Classes*

## Special Requirements for Junos OS Plain-Text Passwords

Junos OS has special requirements when you create plain-text passwords on a router or switch. [Table 19 on page 142](#) shows the default requirements.

**Table 19: Special Requirements for Plain-Text Passwords**

| Junos OS                                                                                                                                                                                       | Junos-FIPS                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The password must be between 6 and 128 characters long.                                                                                                                                        | FIPS passwords must be between 10 and 20 characters long                                                                                                                                       |
| You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended. | You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended. |
| Valid passwords must contain at least one change of case or character class.                                                                                                                   | Passwords must use at least three of the five defined character classes (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters).                      |

You can change the requirements for plain-text passwords.

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

- Lowercase letters
- Uppercase letters
- Numbers

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

Control characters are not recommended.

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

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

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

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

For example, the following password:

MyPassWd@2

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

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

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

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



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

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

must be 20 characters or less. The range for Junos OS maximum-length passwords is from 20 to 128 characters.

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

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

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

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

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

```
[edit system login]
passwords {
 change-type set-transitions;
 format sha1;
 maximum-length 20;
 minimum-changes 3;
 minimum-length 10;
}
```

**Related  
Documentation**

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

## Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies

Use extended regular expressions to specify which configuration mode hierarchies are denied or allowed. You specify these regular expressions in the **allow/deny-configuration-regexps** and **allow/deny-configuration** statements at the **[edit system login class]** hierarchy level, or by specifying Juniper Networks vendor-specific TACACS+ or RADIUS attributes in your authentication server's configuration. If regular expressions are received during TACACS+ or RADIUS authentication, they merge with any regular expressions configured on the local router or switch.

[Table 20 on page 145](#) lists common regular expression operators that you can use for allowing or denying configuration mode .

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

**Table 20: Configuration Mode Hierarchies—Common Regular Expression Operators**

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

**Related Documentation**

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

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

Use extended regular expressions to specify which operational mode commands are denied or allowed. [Table 21 on page 146](#) lists common regular expression operators that can be used in the operational mode commands. Command regular expressions implement the extended (modern) regular expressions as defined in POSIX 1003.2.

**Table 21: Common Regular Expression Operators to Allow or Deny Operational Mode Commands**

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

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

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

#### Related Documentation

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

## Defining Access Privileges Using allow or deny configuration Statements

The following examples show how to configure access privileges for individual configuration mode hierarchy levels.

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot configure telnet parameters:

```
[edit system login class class-name]
user@switch# set deny-configuration "system services telnet"
```

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot issue login class commands within any login class whose name begins with "m":

```
[edit system login class class-name]
user@switch# set deny-configuration "system login class m.*"
```

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot edit a configuration or issue commands (such as **commit**) at the login class or system services hierarchy levels:

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

The following example shows how to configure permissions for individual configuration mode hierarchies:

```
[edit]
system {
 login { # This login class has operator privileges and the additional ability to edit
 # configuration at the system services hierarchy level.
 class only-system-services {
 permissions [configure];
 allow-configuration "system services";
 }
 # services commands.
 class all-except-system-services { # This login class has operator privileges but
 # cannot edit any system services configuration.
 permissions [all];
 deny-configuration "system services";
 }
 }
}
```

#### Related Documentation

- *Specifying Access Privileges Using allow/deny-configuration Statements*
- *Specifying Access Privileges for Junos OS Configuration Mode Hierarchies*

## Example: Configuring User Accounts

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

```
[edit]
system {
 login {
 user philip {
 full-name "Philip of Macedonia";
 uid 1001;
 class super-user;
 authentication {
 encrypted-password "1poPPeY";
 }
 }
 }
}
```

```
}
user alexander {
 full-name "Alexander the Great";
 uid 1002;
 class view;
 authentication {
 encrypted-password "$1$14c5.$sBopasdFFdssdfFFdsdfs0";
 ssh-dsa "8924 37 5678 5678@gaugamela.per";
 ssh-dsa "6273 94 9283@boojum.per";
 }
}
user darius {
 full-name "Darius King of Persia";
 uid 1003;
 class operator;
 authentication {
 ssh-rsa "1024 37 12341234@ecbatana.per";
 }
}
user anonymous {
 class unauthorized;
}
user remote {
 full-name "All remote users";
 uid 9999;
 class read-only;
}
}
```

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

---

## Example: Configuring Access Privilege Levels

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

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

- Related Documentation**
- [Configuring Access Privilege Levels on page 127](#)

## Example: Configuring Access Privileges for Operational Mode Commands

The following example shows how to configure access privileges for different login classes for individual operational mode commands:

```
[edit]
system {
 # This login class has operator privileges and the additional ability
 # to reboot the router.
 login {
 # This login class has operator privileges and the additional ability to reboot the
 # router or switch.
 class operator-and-boot {
 permissions [clear network reset trace view];
 allow-commands "request system reboot";
 }
 # This login class has operator privileges but can't use any commands beginning
 # with "set".
 # This login class has operator privileges
 # but cannot use any commands beginning with "set"
 class operator-no-set {
 permissions [clear network reset trace view];
 deny-commands "^set";
 }
 # This login class has operator privileges and can install software but not view
 # BGP information, and can issue the show route command, without specifying
 # commands or arguments under it.
 class operator-and-install-but-no-bgp {
 permissions [clear network reset trace view];
 allow-commands "(request system software add)|(show route$)";
 deny-commands "show bgp";
 }
 }
}
```

**Related Documentation**

- [Specifying Access Privileges for Junos OS Operational Mode Commands](#)

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

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

- [Requirements on page 150](#)
- [Overview on page 150](#)
- [Configuration on page 150](#)

## Requirements

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

## Overview

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

## Configuration

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

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

---

### Configuring Requirements for Plain-Text Passwords

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

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

```
user@host> edit
[edit]
user@host# edit system login password
```
2. Set a minimum length requirement of 12 characters and a maximum length requirement of 22 characters for user passwords.

```
[edit system login password]
user@host# set minimum-length 12
[edit system login password]
user@host# set maximum-length 22
```
3. Require users to set a password that has at least one lower-case letter and at least one upper-case letter.

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

```

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

```

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

```

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

```

## Results

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

```

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

```

### Related Documentation

- [Special Requirements for Junos OS Plain-Text Passwords on page 142](#)
- *password (Login)*

## Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions

The following example shows how to limit the user to four attempts when the user enters a password while logging in through SSH or Telnet. Set the **backoff-threshold** to 2, the **backoff-factor** to 5 seconds, and the **minimum-time** to 40 seconds. The user experiences a delay of 5 seconds after the second attempt to enter a correct password fails. After each subsequent failed attempt, the delay increases by 5 seconds. After the fourth and final failed attempt to enter a correct password, the user experiences an additional 10-second delay, and the connection closes after a total of 40 seconds.

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

```

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

```

```
}
}
```



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

#### Related Documentation

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

## Understanding Troubleshooting Resources

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

Table 16 on page 132 provides a list of some of the troubleshooting resources.

**Table 22: Troubleshooting Resources on the QFX and OCX Series**

| Troubleshooting Resource              | Description                                                                                                                                                                                                               | Documentation                                                                                                                                                                     |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Chassis alarms                        | Chassis alarms indicate a failure on the switch or one of its components. A chassis alarm count is displayed on the LCD panel on the front of the switch.                                                                 | <i>Chassis Alarm Messages on a QFX3500 Device</i>                                                                                                                                 |
| Chassis Status LEDs and Fan Tray LEDs | A blinking amber Power, Fan, or Fan Tray LED indicates a hardware component error. A blinking amber Status LED indicates a software error.                                                                                | <i>Chassis Status LEDs on a QFX3500 Device</i>                                                                                                                                    |
| Interface alarms                      | A predefined alarm (red or yellow) for an interface type is triggered when an interface of that type goes down.                                                                                                           | <i>Interface Alarm Messages</i>                                                                                                                                                   |
| System alarms                         | A predefined alarm is triggered by a missing rescue configuration or problem with the software license.                                                                                                                   | <i>Understanding Alarms</i>                                                                                                                                                       |
| System log messages                   | The system log includes details of system and user events, including errors. Specify the severity and type of system log messages you wish to view or save, and configure the output to be sent to local or remote hosts. | <ul style="list-style-type: none"> <li>• <i>Overview of Single-Chassis System Logging Configuration</i></li> <li>• <i>Junos OS System Log Configuration Statements</i></li> </ul> |

Table 22: Troubleshooting Resources on the QFX and OCX Series (*continued*)

| Troubleshooting Resource                      | Description                                                                                                                                                                                                                                                                                                                                                                                                | Documentation                                                                                                                                                                           |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Junos OS operational mode commands            | Operational mode commands can be used to monitor switch performance and current activity on the network. For example, use the <b>traceroute monitor</b> command to locate points of failure in a network.                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>• <i>Monitoring System Process Information</i></li> <li>• <i>Monitoring System Properties</i></li> <li>• <i>traceroute monitor</i></li> </ul>    |
| Junos OS automation scripts (event scripts)   | Event scripts can be used to automate network troubleshooting and management tasks.                                                                                                                                                                                                                                                                                                                        | <i>Junos OS Automation Library</i>                                                                                                                                                      |
| Junos OS XML operational tags                 | XML operational tags are equivalent in function to operational mode commands in the CLI, which you can use to retrieve status information for a device.                                                                                                                                                                                                                                                    | <i>Junos XML API Operational Developer Reference</i>                                                                                                                                    |
| NETCONF XML management protocol               | The NETCONF XML management protocol defines basic operations that are equivalent to Junos OS CLI configuration mode commands. Client applications use the protocol operations to display, edit, and commit configuration statements (among other operations), just as administrators use CLI configuration mode commands such as <b>show</b> , <b>set</b> , and <b>commit</b> to perform those operations. | <i>NETCONF XML Management Protocol Developer Guide</i>                                                                                                                                  |
| SNMP MIBs and traps                           | MIBs enable the monitoring of network devices from a central location. For example, use the Traceroute MIB to monitor devices remotely.                                                                                                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>• <i>SNMP MIBs Support</i></li> <li>• <i>SNMP Traps Support</i></li> <li>• <i>Using the Traceroute MIB for SNMP Remote Operations</i></li> </ul> |
| AI-Scripts and Advanced Insight Manager (AIM) | AI-Scripts installed on the switch can automatically detect and monitor faults on the switch, and depending on the configuration on the AIM application, send notifications of potential problems and submit problem reports to Juniper Support Systems.                                                                                                                                                   | <i>Advanced Insight Scripts (AI-Scripts) Release Notes</i>                                                                                                                              |
| Junos Space Service Now                       | This application enables you to display and manage information about problem events. When problems are detected on the switch by Advanced Insight Scripts (AI-Scripts) that are installed on the switch, the data is collected and sent to Service Now for your review and action.                                                                                                                         | <i>Service Automation</i>                                                                                                                                                               |

Table 22: Troubleshooting Resources on the QFX and OCX Series (*continued*)

| Troubleshooting Resource        | Description                                                                                                                                                                                                                                                                                                                                 | Documentation                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| Junos Space Service Insight     | This application helps in accelerating operational analysis and managing the exposure to known issues. You can identify devices that are nearing their End Of Life (EOL) and also discover and prevent issues that could occur in your network. The functionality of Service Insight is dependent on the information sent from Service Now. | <i>Service Automation</i>                                 |
| Juniper Networks Knowledge Base | You can search in this database for Juniper Networks product information, including alerts and troubleshooting tips.                                                                                                                                                                                                                        | <a href="http://kb.juniper.net">http://kb.juniper.net</a> |

## Troubleshooting Overview

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

[Table 17 on page 134](#) provides a list of problem categories, summary of the symptom or problem, and recommended actions with links to the troubleshooting documentation.

Table 23: Troubleshooting on the QFX Series

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

Table 23: Troubleshooting on the QFX Series (*continued*)

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

Table 23: Troubleshooting on the QFX Series (*continued*)

| Problem Category                   | Symptom or Problem                                                                                                                                                    | Recommended Action                                                                                                                                                                                                                                                                                       |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Software upgrade and configuration | Failed software upgrade.                                                                                                                                              | See <i>Recovering from a Failed Software Installation</i> .                                                                                                                                                                                                                                              |
|                                    | Active partition becomes inactive after upgrade.                                                                                                                      |                                                                                                                                                                                                                                                                                                          |
|                                    | Problem with the active configuration file.                                                                                                                           | See the following topics: <ul style="list-style-type: none"> <li>• <i>Loading a Previous Configuration File</i></li> <li>• <i>Reverting to the Default Factory Configuration</i></li> <li>• <i>Reverting to the Rescue Configuration</i></li> <li>• <i>Performing a Recovery Installation</i></li> </ul> |
|                                    | Root password is lost or forgotten.                                                                                                                                   | Recover the root password. See <a href="#">"Recovering the Root Password" on page 128</a> .                                                                                                                                                                                                              |
| Network interfaces                 | An aggregated Ethernet interface is down.                                                                                                                             | See <i>Troubleshooting an Aggregated Ethernet Interface</i> .                                                                                                                                                                                                                                            |
|                                    | Interface on built-in network port is down.                                                                                                                           | See <i>Troubleshooting Network Interfaces</i> .                                                                                                                                                                                                                                                          |
|                                    | Interface on port in which SFP or SFP+ transceiver is installed in an SFP+ uplink module is down.                                                                     |                                                                                                                                                                                                                                                                                                          |
| Ethernet switching                 | A MAC address entry in the Ethernet switching table is not updated after the device with that MAC address has been moved from one interface to another on the switch. | See <i>Troubleshooting Ethernet Switching</i> .                                                                                                                                                                                                                                                          |
| Firewall filter                    | Firewall configuration exceeded available Ternary Content Addressable Memory (TCAM) space.                                                                            | See <i>Troubleshooting Firewall Filter Configuration</i> .                                                                                                                                                                                                                                               |

## Recovering the Root Password

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



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



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

To recover the root password:

1. Power off the switch by switching off the AC power outlet of the device or, if necessary, by pulling the power cords out of the device's power supplies.
2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with the device into the RJ-45-to-DB-9 serial port adapter supplied with the device.
4. Plug the RJ-45-to-DB-9 serial port adapter into the serial port on the management device.
5. Connect the other end of the Ethernet rollover cable to the console port on the device.
6. Turn on the power to the management device.
7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate **COM** port to use (for example, **COM1**).
8. Configure the port settings as follows:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
9. Power on the device by (if necessary) plugging the power cords into the device's power supply, or turning on the power to the device by switching on the AC power outlet the device is plugged into.

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

10. When the following prompt appears, press the Spacebar to access the device's bootstrap loader command prompt:  
  
Hit [Enter] to boot immediately, or space bar for command prompt.  
Booting [kernel] in 9 seconds...
11. At the following prompt, enter **boot -s** to start up the system in single-user mode.  
  
ok **boot -s**
12. At the following prompt, enter **recovery** to start the root password recovery procedure.  
  
Enter full pathname of shell or 'recovery' for root password recovery or RETURN for /bin/sh: **recovery**
13. Enter configuration mode in the CLI.
14. Set the root password. For example:  
  
user@switch# **set system root-authentication plain-text-password**
15. At the following prompt, enter the new root password. For example:  
  
New password: **juniper1**  
Retype new password:

16. At the second prompt, reenter the new root password.
17. After you have finished configuring the password, commit the configuration.

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

18. Exit configuration mode in the CLI.
19. Exit operational mode in the CLI.
20. At the prompt, enter **y** to reboot the device.

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

**Related Documentation**

- *Configuring the Root Password*

## PART 3

# Configuring Authentication

- [Configuring and Managing Local Password Authentication on page 161](#)
- [Configuring and Managing TACACS+ Authentication on page 175](#)
- [Configuring and Managing RADIUS Authentication on page 187](#)
- [Configuring and Managing RADIUS Accounting on page 201](#)
- [Configuring and Managing RADIUS Template Accounts on page 217](#)
- [Configuring and Managing VSAs for RADIUS and TACACS+ on page 219](#)



## CHAPTER 10

# Configuring and Managing Local Password Authentication

- [Junos OS User Accounts Overview on page 161](#)
- [Junos OS User Authentication Methods on page 163](#)
- [Junos OS Login Classes Overview on page 164](#)
- [Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 165](#)
- [Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands on page 166](#)
- [Special Requirements for Junos OS Plain-Text Passwords on page 167](#)
- [Configuring Junos OS User Accounts on page 169](#)
- [Example: Configuring User Login Accounts on page 169](#)
- [Example: Creating Login Classes with Specific Privileges on page 170](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 171](#)
- [Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 173](#)

### Junos OS User Accounts Overview

---

User accounts provide one way for users to access the switch. (Users can access the switch without accounts if you configured RADIUS or TACACS+ servers, as described in [“Junos OS User Authentication Methods” on page 14](#).) For each account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

For each user account, you can define the following:

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

- User identifier (UID)—(Optional) Numeric identifier that is associated with the user account name. The identifier must be in the range from 100 through 64,000 and must be unique within the switch. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.
- You must ensure that the UID is unique. However, it is possible to assign the same UID to different users. If you do this, the CLI displays a warning when you commit the configuration and then assigns the duplicate UID.
- User's access privilege—(Required) One of the login classes you defined in the **class** statement at the **[edit system login]** hierarchy level, or one of the default classes listed in ["Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies"](#) on page 144.
- Authentication method or methods and passwords that the user can use to access the switch—(Optional) You can use SSH or a Message Digest 5 (MD5) password, or you can enter a plain-text password that Junos OS encrypts using MD5-style encryption before entering it in the password database. For each method, you can specify the user's password. If you configure the **plain-text-password** option, you are prompted to enter and confirm the password:

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

The default requirements for plain-text passwords are:

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

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

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

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

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

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

```
[edit system]
user@switch# show
root-authentication {
 ssh-rsa "1024 35 9727638204084251055468226757249864241630322
207404962528390382038690141584534964170019610608358722961563
475784918273603361276441874265946893207739108344813125957722
625461667999278316123500438660915866283822489746732605661192
181489539813862940327687806538169602027491641637359132693963
44008443 boojum@juniper.net"; # SECRET-DATA
}
```

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

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

**Related Documentation**

- [Configuring Junos OS User Accounts on page 169](#)
- [Junos OS Login Classes Overview on page 141](#)

## Junos OS User Authentication Methods

The Junos OS supports three methods of user authentication: local password authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+).

With local password authentication, you configure a password for each user allowed to log in to the router or switch.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the router or switch using telnet. They are both distributed client-server systems—the RADIUS and TACACS+ clients run on the router or switch, and the server runs on a remote network system.

You can configure the router or switch to be both a RADIUS and TACACS+ client, and you can also configure authentication passwords in the Junos OS configuration file. You can prioritize the methods to configure the order in which the software tries the different authentication methods when verifying user access.

**Related Documentation**

- [Configuring RADIUS Authentication](#)
- [Configuring TACACS+ Authentication](#)
- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 175](#)
- [Configuring RADIUS Authentication \(QFX Series or OCX Series\) on page 192](#)
- [Configuring TACACS+ Authentication \(QFX Series\) on page 180](#)

## Junos OS Login Classes Overview

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

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

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

The Junos operating system (Junos OS) contains a few predefined login classes, which are listed in [Table 18 on page 141](#). The predefined login classes cannot be modified.

**Table 24: Predefined System Login Classes**

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



### NOTE:

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

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

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

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

### Related Documentation

- [Defining Junos OS Login Classes](#)
- [Defining Junos OS Login Classes](#)
- [Understanding QFabric System Login Classes](#)

Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies

Use extended regular expressions to specify which configuration mode hierarchies are denied or allowed. You specify these regular expressions in the **allow/deny-configuration-regexps** and **allow/deny-configuration** statements at the **[edit system login class]** hierarchy level, or by specifying Juniper Networks vendor-specific TACACS+ or RADIUS attributes in your authentication server's configuration. If regular expressions are received during TACACS+ or RADIUS authentication, they merge with any regular expressions configured on the local router or switch.

Table 20 on page 145 lists common regular expression operators that you can use for allowing or denying configuration mode .

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

Table 25: Configuration Mode Hierarchies—Common Regular Expression Operators

| Operator | Match                                                                                                                                                                                                                                                                                      |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | One of two or more terms separated by the pipe. Each term must be a complete standalone expression enclosed in parentheses ( ), with no spaces between the pipe and the adjacent parentheses. For example, (show system alarms) (show system software).                                    |
| ^        | At the beginning of an expression, used to denote where the command begins, where there might be some ambiguity.                                                                                                                                                                           |
| \$       | Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, allow-commands "show interfaces\$" means that the user can issue the show interfaces command but cannot issue show interfaces detail or show interfaces extensive. |
| [ ]      | Range of letters or digits. To separate the start and end of a range, use a hyphen ( - ).                                                                                                                                                                                                  |
| ( )      | A group of commands, indicating a complete, standalone expression to be evaluatedhe result is then evaluated as part of the overall expression. Parentheses must be used in conjunction with pipe operators as explained .                                                                 |
| *        | Zero or more terms.                                                                                                                                                                                                                                                                        |
| +        | One or more terms.                                                                                                                                                                                                                                                                         |
| .        | Any character except for a space " ".                                                                                                                                                                                                                                                      |

Related Documentation

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

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

Use extended regular expressions to specify which operational mode commands are denied or allowed. [Table 21 on page 146](#) lists common regular expression operators that can be used in the operational mode commands. Command regular expressions implement the extended (modern) regular expressions as defined in POSIX 1003.2.

**Table 26: Common Regular Expression Operators to Allow or Deny Operational Mode Commands**

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

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

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

### Related Documentation

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

## Special Requirements for Junos OS Plain-Text Passwords

Junos OS has special requirements when you create plain-text passwords on a router or switch. [Table 19 on page 142](#) shows the default requirements.

**Table 27: Special Requirements for Plain-Text Passwords**

| Junos OS                                                                                                                                                                                       | Junos-FIPS                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The password must be between 6 and 128 characters long.                                                                                                                                        | FIPS passwords must be between 10 and 20 characters long                                                                                                                                       |
| You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended. | You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended. |
| Valid passwords must contain at least one change of case or character class.                                                                                                                   | Passwords must use at least three of the five defined character classes (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters).                      |

You can change the requirements for plain-text passwords.

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

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

Control characters are not recommended.

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

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

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

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

For example, the following password:

MyPassWd@2

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

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

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

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



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

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

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

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

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

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

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

```
[edit system login]
```

```

passwords {
 change-type set-transitions;
 format sha1;
 maximum-length 20;
 minimum-changes 3;
 minimum-length 10;
}

```

**Related Documentation**

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

## Configuring Junos OS User Accounts

User accounts provide one way for users to access the router or switch. For each account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

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

```

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

```

**Related Documentation**

- [Example: Configuring User Accounts on page 147](#)
- [Example: Configuring User Login Accounts on page 169](#)
- [Junos OS User Accounts Overview on page 139](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)

## Example: Configuring User Login Accounts

The following example shows how to configure the local administrator account (**user admin**). If RADIUS fails or becomes unreachable, the login process reverts to password authentication on the local accounts on the router or switch.

```

[edit]

```

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

**Related Documentation**

- *Configuring Junos OS User Accounts*

---

## Example: Creating Login Classes with Specific Privileges

The following example shows how to create several user classes, each with specific privileges. In this example, you configure timeouts to disconnect the class members after a period of inactivity. Users' privilege levels, and therefore the classes of which they are members, should be dependent on their responsibilities within the organization, and the permissions shown here are only examples.

The first class of users (called "observation") can only view statistics and configuration. They are not allowed to modify any configuration. The second class of users (called "operation") can view and modify the configuration. The third class of users (called "engineering") has unlimited access and control.

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

**Related Documentation**

- *Defining Junos OS Login Classes*

## Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication

The following example shows how to configure system authentication for RADIUS, TACACS+, and password authentication.

In this example, only the user Philip and users authenticated by a remote RADIUS server can log in. If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the router or switch. If the RADIUS server is not available, the user is authenticated using the **password** authentication method and allowed access to the router or switch. For more information about the password authentication method, see [“Using Local Password Authentication” on page 176](#).

When Philip tries to log in to the system, if the RADIUS server authenticates him, he is given access and privileges for the **super-user** class. Local accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same user ID (UID) 9999 and the privileges associated with the **operator** class.

```
[edit]
system {
 authentication-order radius;
 login {
 user philip {
 full-name "Philip";
 uid 1001;
 class super-user;
 }
 user remote {
 full-name "All remote users";
 uid 9999;
 class operator;
 }
 }
}
```



**NOTE:** For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time. For example, when you create a remote template account, a set of remote users can concurrently share a single UID. For more information about template accounts, see [“Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 217](#).

When a user logs in to a device, the user's login name is used by the RADIUS or TACACS+ server for authentication. If the user is authenticated successfully by the authentication server and the user is not configured at the **[edit system login user]** hierarchy level, the device uses the default remote template user account for the user, provided a remote template account is configured at the **edit system login user remote** hierarchy level. The remote template account serves as a default template user account for all users that

are authenticated by the authentication server but not having a locally configured user account on the device. Such users share the same login class and UID.

To configure an alternate template user, specify the **user-name** parameter returned in the RADIUS authentication response packet. Not all RADIUS servers allow you to change this parameter. The following shows a sample Junos OS configuration:

```
[edit]
system {
 authentication-order radius;
 login {
 user philip {
 full-name "Philip";
 uid 1001;
 class super-user;
 }
 user operator {
 full-name "All operators";
 uid 9990;
 class operator;
 }
 user remote {
 full-name "All remote users";
 uid 9999;
 class read-only;
 }
 }
}
```

Assume your RADIUS server is configured with the following information:

- User Philip with password “olympia”
- User Alexander with password “bucephalus” and username “operator”
- User Darius with password “redhead” and username “operator”
- User Roxane with password “athena”

Philip would be given access as a superuser (**super-user**) because he has his own local user account. Alexander and Darius share UID 9990 and have access as operators. Roxane has no template-user override, so she shares access with all the other remote users, getting read-only access.

**Related  
Documentation**

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

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

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

- [Requirements on page 173](#)
- [Overview on page 173](#)
- [Configuration on page 173](#)

### Requirements

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

### Overview

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

### Configuration

#### CLI Quick Configuration

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

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

### Configuring Requirements for Plain-Text Passwords

#### Step-by-Step Procedure

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

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

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

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

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

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

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

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

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

---

## Results

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

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

### Related Documentation

- [Special Requirements for Junos OS Plain-Text Passwords on page 142](#)
- *password (Login)*

## CHAPTER 11

# Configuring and Managing TACACS+ Authentication

- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 175](#)
- [Configuring TACACS+ Authentication \(QFX Series\) on page 180](#)
- [Juniper Networks Vendor-Specific TACACS+ Attributes on page 182](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 184](#)

## Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication

Using the **authentication-order** statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch.

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

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

## Using RADIUS or TACACS+ Authentication

You can configure the Junos OS to be both a RADIUS and TACACS+ authentication client.

If an authentication method included in the **[authentication-order]** statement is not available, or if the authentication is available but returns a reject response, the Junos OS tries the next authentication method included in the **authentication-order** statement.

The RADIUS or TACACS+ server authentication might fail because of the following reasons:

- The authentication method is configured, but the corresponding authentication servers are not configured. For instance, the RADIUS and TACACS+ authentication methods are included in the **authentication-order** statement, but the corresponding RADIUS or

TACACS+ servers are not configured at the respective **[edit system radius-server]** and **[edit system tacplus-server]** hierarchy levels.

- The RADIUS or TACACS+ server does not respond within the timeout period configured at the **[edit system radius-server]** or **[edit system tacplus-server]** hierarchy levels.
- The RADIUS or TACACS+ server is not reachable because of a network problem.

The RADIUS or TACACS+ server authentication might return a reject response because of the following reasons:

- The user profiles of users accessing a router or switch might not be configured on the RADIUS or TACACS+ server.
- The user enters incorrect logon credentials.

## Using Local Password Authentication

You can explicitly configure the password authentication method or use this method as a fallback mechanism when remote authentication servers fail. The password authentication method consults the local user profiles configured at the **[edit system login]** hierarchy level. Users can log in to a router or switch using their local username and password in the following scenarios:

- The password authentication method (password) is explicitly configured as one of the authentication methods in the **[authentication-order authentication-methods]** statement. In this case, the password authentication method is tried if no previous authentication accepts the logon credentials. This is true whether the previous authentication method fails to respond or returns a reject response because of an incorrect username or password.
- The password authentication method is not explicitly configured as one of the authentication methods in the **authentication-order authentication-methods** statement. In this case, the password authentication method is tried only if all configured authentication methods fail to respond. It is not consulted if any configured authentication method returns a reject response because of an incorrect username or password.

## Order of Authentication Attempts

[Table 28 on page 177](#) describes how the **authentication-order** statement at the **[edit system]** hierarchy level determines the procedure that the Junos OS uses to authenticate users for access to a router or switch.

Table 28: Order of Authentication Attempts

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

Table 28: Order of Authentication Attempts (*continued*)

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

Table 28: Order of Authentication Attempts (*continued*)

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



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

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

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

#### Related Documentation

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 217](#)
- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 171](#)

## Configuring TACACS+ Authentication (QFX Series)

---

TACACS+ authentication is a method of authenticating users who attempt to access the router or switch. Tasks to configure TACACS+ configuration are:

- [Configuring TACACS+ Server Details on page 180](#)
- [Specifying a Source Address for the Junos OS to Access External TACACS+ Servers on page 181](#)
- [Configuring the Same Authentication Service for Multiple TACACS+ Servers on page 181](#)
- [Configuring Juniper Networks Vendor-Specific TACACS+ Attributes on page 182](#)

### Configuring TACACS+ Server Details

To use TACACS+ authentication on the router or switch, configure information about one or more TACACS+ servers on the network by including the **tacplus-server** statement at the **[edit system]** hierarchy level:

```
[edit system]
tacplus-server server-address {
 port port-number;
 secret password;
 single-connection;
 timeout seconds;
}
```

***server-address*** is the address of the TACACS+ server.

***port-number*** is the TACACS+ server port number.

You must specify a secret (password) by using the **secret** statement. The local router or switch passes the **secret** to the TACACS+ client. If the password included spaces, enclose the password in quotation marks. The secret used by the local router or switch must match that used by the server.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a TACACS+ server by including the **timeout** statement. By default, the router or switch waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds.

Optionally, you can use the **single-connection** statement to have the software maintain one open Transmission Control Protocol (TCP) connection to the server for multiple requests, rather than opening a connection for each connection attempt.



**NOTE:** Early versions of the TACACS+ server do not support the **single-connection** option. If you specify this option and the server does not support it, Junos OS will be unable to communicate with that TACACS+ server.

---

To configure multiple TACACS+ servers, include multiple **tacplus-server** statements.

On a TX Matrix router, TACACS+ accounting should be configured only under the groups **re0** and **re1**.



**NOTE:** Accounting should not be configured at the **[edit system]** hierarchy level; on a TX Matrix router, control is done under the switch-card chassis only.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the **user** statement at the **[edit system login]** hierarchy level.

## Specifying a Source Address for the Junos OS to Access External TACACS+ Servers

You can specify which source address Junos OS uses when accessing your network to contact an external TACACS+ server for authentication. You can also specify which source address Junos OS uses when contacting a TACACS+ server for sending accounting information.

To specify a source address for a TACACS+ server for authentication, include the **source-address** statement at the **[edit system tacplus-server *server-address*]** hierarchy level:

```
[edit system tacplus-server server-address]
source-address source-address;
```

***source-address*** is a valid IP address configured on one of the router or switch interfaces.

To specify a source address for a TACACS+ server for system accounting, include the **source-address** statement at the **[edit system accounting destination tacplus server *server-address*]** hierarchy level:

```
[edit system accounting destination tacplus server server-address]
source-address source-address;
```

***source-address*** is a valid IP address configured on one of the router or switch interfaces.

## Configuring the Same Authentication Service for Multiple TACACS+ Servers

To configure the same authentication service for multiple TACACS+ servers, include statements at the **[edit system tacplus-server]** and **[edit system tacplus-options]** hierarchy levels. For information about how to configure a TACACS+ server at the **[edit system tacplus-server]** hierarchy level.

To assign the same authentication service to multiple TACACS+ servers, include the **service-name** statement at the **[edit system tacplus-options]** hierarchy level:

```
[edit system tacplus-options]
service-name service-name;
```

***service-name*** is the name of the authentication service. By default, the service name is set to **junos-exec**.

The following example shows how to configure the same authentication service for multiple TACACS+ servers:

```
[edit system]
tacplus-server {
 10.2.2.2 secret "$9$2dgoJGDiqP5ZG9A"; ## SECRET-DATA
 10.3.3.3 secret "$9$2dgoJGDiqP5ZG9A"; ## SECRET-DATA
}
tacplus-options {
 service-name bob;
}
```

## Configuring Juniper Networks Vendor-Specific TACACS+ Attributes

The Juniper Networks vendor-specific TACACS+ attributes enable you to configure access privileges for users on a TACACS+ server. They are specified in the TACACS+ server configuration file on a per-user basis. Junos OS retrieves these attributes through an authorization request of the TACACS+ server after authenticating a user. You do not need to configure these attributes to run Junos OS with TACACS+.

To specify these attributes, include a **service** statement of the following form in the TACACS+ server configuration file:

```
service = junos-exec {
 local-user-name = <username-local-to-router>
 allow-commands = "<allow-commands-regex>"
 allow-configuration = "<allow-configuration-regex>"
 deny-commands = "<deny-commands-regex>"
 deny-configuration = "<deny-configuration-regex>"
}
```

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

### Related Documentation

- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 194](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 171](#)
- [Juniper Networks Vendor-Specific TACACS+ Attributes on page 182](#)
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 217](#)
- [Junos OS User Authentication Methods on page 14](#)

---

## Juniper Networks Vendor-Specific TACACS+ Attributes

Junos OS supports the configuration of Juniper Networks TACACS+ vendor-specific attributes (VSAs). These VSAs are encapsulated in a TACACS+ vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. [Table 29 on page 183](#) lists the Juniper Networks VSAs you can configure.

Table 29: Juniper Networks Vendor-Specific TACACS+ Attributes

| Name                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Length | String                                                                                                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>local-user-name</b>     | Indicates the name of the user template used by this user when logging in to a device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | ≥3     | One or more octets containing printable ASCII characters.                                                                                                                                                                         |
| <b>allow-commands</b>      | Contains an extended regular expression that enables the user to run operational mode commands in addition to those commands authorized by the user's login class permission bits.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ≥3     | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See <a href="#">Table 21 on page 146</a> .                                                                               |
| <b>allow-configuration</b> | Contains an extended regular expression that enables the user to run configuration mode commands in addition to those commands authorized by the user's login class permission bits.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | ≥3     | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See <a href="#">"Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies" on page 144</a> . |
| <b>deny-commands</b>       | Contains an extended regular expression that denies the user permission to run operational mode commands authorized by the user's login class permission bits.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | ≥3     | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See <a href="#">Table 21 on page 146</a> .                                                                               |
| <b>deny-configuration</b>  | Contains an extended regular expression that denies the user permission to run configuration mode commands authorized by the user's login class permission bits.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | ≥3     | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See <a href="#">Table 20 on page 145</a> .                                                                               |
| <b>user-permissions</b>    | <p>Contains information the server uses to specify user permissions.</p> <p><b>NOTE:</b> When the <b>user-permissions</b> attribute is configured to grant the Junos OS <b>maintenance</b> or <b>all</b> permissions on an IPv4 or IPv6 TACACS+ server, the UNIX wheel group membership is not automatically added to a user's list of group memberships. Some operations such as running the <b>su root</b> command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions <b>maintenance</b> or <b>all</b>, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account.</p> | ≥3     | One or more octets containing printable ASCII characters. See <a href="#">Table 4 on page 10</a> .                                                                                                                                |
| <b>authentication-type</b> | Indicates the authentication method (local database, or TACACS+ server) used to authenticate a user. If the user is authenticated using a local database, the attribute value shows 'local'. If the user is authenticated using TACACS+ server, the attribute value shows 'remote'.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | ≥5     | One or more octets containing printable ASCII characters.                                                                                                                                                                         |

Table 29: Juniper Networks Vendor-Specific TACACS+ Attributes (*continued*)

| session-port | Indicates the source port number of the established session. | size of integer | Integer |
|--------------|--------------------------------------------------------------|-----------------|---------|
|--------------|--------------------------------------------------------------|-----------------|---------|

**Related Documentation**

- [Configuring TACACS+ Authentication](#)
- [Configuring TACACS+ Authentication \(QFX Series\) on page 180](#)

## Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication

The following example shows how to configure system authentication for RADIUS, TACACS+, and password authentication.

In this example, only the user Philip and users authenticated by a remote RADIUS server can log in. If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the router or switch. If the RADIUS server is not available, the user is authenticated using the **password** authentication method and allowed access to the router or switch. For more information about the password authentication method, see [“Using Local Password Authentication” on page 176](#).

When Philip tries to log in to the system, if the RADIUS server authenticates him, he is given access and privileges for the **super-user** class. Local accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same user ID (UID) 9999 and the privileges associated with the **operator** class.

```
[edit]
system {
 authentication-order radius;
 login {
 user philip {
 full-name "Philip";
 uid 1001;
 class super-user;
 }
 user remote {
 full-name "All remote users";
 uid 9999;
 class operator;
 }
 }
}
```



**NOTE:** For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time. For example, when you create a remote template account, a set of remote users can concurrently share a single UID. For more information about template accounts, see [“Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 217](#).

When a user logs in to a device, the user's login name is used by the RADIUS or TACACS+ server for authentication. If the user is authenticated successfully by the authentication server and the user is not configured at the **[edit system login user]** hierarchy level, the device uses the default remote template user account for the user, provided a remote template account is configured at the **edit system login user remote** hierarchy level. The remote template account serves as a default template user account for all users that are authenticated by the authentication server but not having a locally configured user account on the device. Such users share the same login class and UID.

To configure an alternate template user, specify the **user-name** parameter returned in the RADIUS authentication response packet. Not all RADIUS servers allow you to change this parameter. The following shows a sample Junos OS configuration:

```
[edit]
system {
 authentication-order radius;
 login {
 user philip {
 full-name "Philip";
 uid 1001;
 class super-user;
 }
 user operator {
 full-name "All operators";
 uid 9990;
 class operator;
 }
 user remote {
 full-name "All remote users";
 uid 9999;
 class read-only;
 }
 }
}
```

Assume your RADIUS server is configured with the following information:

- User Philip with password “olympia”
- User Alexander with password “bucephalus” and username “operator”
- User Darius with password “redhead” and username “operator”
- User Roxane with password “athena”

Philip would be given access as a superuser (**super-user**) because he has his own local user account. Alexander and Darius share UID 9990 and have access as operators. Roxane has no template-user override, so she shares access with all the other remote users, getting read-only access.

#### Related Documentation

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



## CHAPTER 12

# Configuring and Managing RADIUS Authentication

- Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 187
- Configuring RADIUS Authentication (QFX Series or OCX Series) on page 192
- Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 194
- Example: Configuring RADIUS Authentication on page 196
- Example: Configuring RADIUS Template Accounts on page 197
- Example: Configuring User Login Accounts on page 197
- Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 198

### Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication

Using the **authentication-order** statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch.

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

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

### Using RADIUS or TACACS+ Authentication

You can configure the Junos OS to be both a RADIUS and TACACS+ authentication client.

If an authentication method included in the **[authentication-order]** statement is not available, or if the authentication is available but returns a reject response, the Junos OS tries the next authentication method included in the **authentication-order** statement.

The RADIUS or TACACS+ server authentication might fail because of the following reasons:

- The authentication method is configured, but the corresponding authentication servers are not configured. For instance, the RADIUS and TACACS+ authentication methods are included in the **authentication-order** statement, but the corresponding RADIUS or TACACS+ servers are not configured at the respective **[edit system radius-server]** and **[edit system tacplus-server]** hierarchy levels.
- The RADIUS or TACACS+ server does not respond within the timeout period configured at the **[edit system radius-server]** or **[edit system tacplus-server]** hierarchy levels.
- The RADIUS or TACACS+ server is not reachable because of a network problem.

The RADIUS or TACACS+ server authentication might return a reject response because of the following reasons:

- The user profiles of users accessing a router or switch might not be configured on the RADIUS or TACACS+ server.
- The user enters incorrect logon credentials.

## Using Local Password Authentication

You can explicitly configure the password authentication method or use this method as a fallback mechanism when remote authentication servers fail. The password authentication method consults the local user profiles configured at the **[edit system login]** hierarchy level. Users can log in to a router or switch using their local username and password in the following scenarios:

- The password authentication method (password) is explicitly configured as one of the authentication methods in the **[authentication-order authentication-methods]** statement. In this case, the password authentication method is tried if no previous authentication accepts the logon credentials. This is true whether the previous authentication method fails to respond or returns a reject response because of an incorrect username or password.
- The password authentication method is not explicitly configured as one of the authentication methods in the **authentication-order authentication-methods** statement. In this case, the password authentication method is tried only if all configured authentication methods fail to respond. It is not consulted if any configured authentication method returns a reject response because of an incorrect username or password.

## Order of Authentication Attempts

[Table 28 on page 177](#) describes how the **authentication-order** statement at the **[edit system]** hierarchy level determines the procedure that the Junos OS uses to authenticate users for access to a router or switch.

Table 30: Order of Authentication Attempts

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

Table 30: Order of Authentication Attempts (*continued*)

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

Table 30: Order of Authentication Attempts (*continued*)

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



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

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

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

#### Related Documentation

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 217](#)
- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 171](#)

## Configuring RADIUS Authentication (QFX Series or OCX Series)

RADIUS authentication is a method of authenticating users who attempt to access the router or switch. Tasks to configure RADIUS authentication are:



**NOTE:** The `source-address` statement is not supported at the `[edit system radius-options]` or `[edit system-radius-server name]` hierarchies on the QFabric system.

- [Configuring RADIUS Server Details on page 192](#)
- [Configuring MS-CHAPv2 for Password-Change Support on page 193](#)
- [Specifying a Source Address for the Junos OS to Access External RADIUS Servers on page 194](#)

### Configuring RADIUS Server Details

To use RADIUS authentication on the router or switch, configure information about one or more RADIUS servers on the network by including one **radius-server** statement at the `[edit system]` hierarchy level for each RADIUS server:

```
[edit system]
radius-server server-address {
 accounting-port port-number;
 port number;
 retry number;
 secret password;
 source-address source-address;
 timeout seconds;
}
```

**server-address** is the address of the RADIUS server.

You can specify a port on which to contact the RADIUS server. By default, port number **1812** is used (as specified in RFC 2865). You can also specify an accounting port to send accounting packets. The default is **1813** (as specified in RFC 2866).

You must specify a password in the **secret password** statement. If the password contains spaces, enclose it in quotation marks. The secret used by the local router or switch must match that used by the server.

Optionally, you can specify the amount of time that the local router or switch waits to receive a response from a RADIUS server (in the **timeout** statement) and the number of times that the router or switch attempts to contact a RADIUS authentication server (in the **retry** statement). By default, the router or switch waits 3 seconds. You can configure this to be a value from 1 through 90 seconds. By default, the router or switch retries connecting to the server three times. You can configure this to be a value from 1 through 10 times.

You can use the **source-address** statement to specify a logical address for individual or multiple RADIUS servers.

To configure multiple RADIUS servers, include multiple **radius-server** statements.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the **user** statement at the **[edit system login]** hierarchy level, as described in [“Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 217](#).

You can also configure RADIUS authentication at the **[edit access]** and **[edit access profile]** hierarchy level. Junos OS uses the following search order to determine which set of servers are used for authentication:

1. **[edit access profile *profile-name* radius-server *server-address*]**
2. **[edit access radius-server *server-address*]**
3. **[edit system radius-server *server-address*]**

## Configuring MS-CHAPv2 for Password-Change Support

You can configure the Microsoft implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the router or switch to support changing of passwords. This feature provides users accessing a router or switch the option of changing the password when the password expires, is reset, or is configured to be changed at the next login.

Before you configure MS-CHAPv2 for password-change support, ensure that you:

- Configure the RADIUS server authentication parameters
- Set the **authentication-order** to use the RADIUS server for the initial password attempt

To configure MS-CHAP-v2, include the following statements at the **[edit system radius-options]** hierarchy level:

```
[edit system radius-options]
password-protocol mschap-v2;
```

The following example shows statements for configuring the MS-CHAPv2 password protocol, password authentication order, and user accounts:

```
[edit]
system {
 authentication-order [radius password];
 radius-server {
 192.168.69.149 secret "9G-j.5Qz6tpBk.1hrlXxUjiq5Qn/C"; ## SECRET-DATA
 }
 radius-options {
 password-protocol mschap-v2;
 }
 login {
 user bob {
 class operator;
```

```
 }
 }
}
```

## Specifying a Source Address for the Junos OS to Access External RADIUS Servers

You can specify which source address Junos OS uses when accessing your network to contact an external RADIUS server for authentication. You can also specify which source address Junos OS uses when contacting a RADIUS server for sending accounting information.

To specify a source address for a RADIUS server, include the **source-address** statement at the **[edit system radius-server server-address]** hierarchy level:

```
[edit system radius-server server-address]
source-address source-address;
```

**source-address** is a valid IP address configured on one of the router or switch interfaces.

### Related Documentation

- [Example: Configuring RADIUS Authentication on page 196](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 171](#)
- [Juniper Networks Vendor-Specific RADIUS Attributes on page 207](#)
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 217](#)
- [Example: Configuring RADIUS Template Accounts on page 197](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 194](#)
- [Junos OS User Authentication Methods on page 14](#)

## Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands

---

Use regular expressions to specify which operational or configuration mode commands are allowed or denied when you use a RADIUS or TACACS+ server for user authentication. You can specify the regular expressions using the appropriate Juniper Networks vendor-specific RADIUS or TACACS+ attributes in your authentication server configuration.

You can specify **allow-configuration**, **deny-configuration**, **allow-commands**, or **deny-commands** in a single extended regular expression, enclosing multiple commands in parentheses and separating them using the pipe symbol. For example, you can specify multiple **allow-commands** parameters using: **allow-commands= (cmd1 | cmd2 | cmdn)**. You can specify **user-permissions** as a list of comma-separated values, and not as a regular expression.

On a RADIUS or TACACS+ server, you can also use a simplified version for regular expressions where you specify each individual expression on a separate line. The simplified version is valid for **allow-commands**, **deny-commands**, **allow-configuration**, **deny-configuration**, and **permissions** vendor-specific attributes.

For a RADIUS server, specify the individual regular expressions using the following syntax:

```
Juniper-Allow-Commands+= "cmd1"
Juniper-Allow-Commands+= "cmd2"
Juniper-Allow-Commands+= "cmdn"
Juniper-Deny-Commands+= "cmd1"
Juniper-Deny-Commands+= "cmd2"
Juniper-Deny-Commands+= "cmdn"
Juniper-Allow-Configuration+= "regex1"
Juniper-Allow-Configuration+= "regex2"
Juniper-Allow-Configuration+= "regexn"
Juniper-Deny-Configuration+= "regex1"
Juniper-Deny-Configuration+= "regex2"
Juniper-Deny-Configuration+= "regexn"
Juniper-User-Permissions+= "permission-flag1"
Juniper-User-Permissions+= "permission-flag2"
Juniper-User-Permissions+= "permission-flagn"
```

For TACACS+ server, specify the individual regular expressions using the following syntax:

```
allow-commands1="cmd1"
allow-commands2="cmd2"
allow-commandsn="cmdn"
deny-commands1="cmd1"
deny-commands2="cmd2"
deny-commandsn="cmdn"
allow-configuration1="regex1"
allow-configuration2="regex2"
allow-configurationn="regexn"
deny-configuration1="regex1"
deny-configuration2="regex2"
deny-configurationn="regexn"
user-permissions1="permission-flag1"
user-permissions2="permission-flag2"
user-permissionsn="permission-flagn"
```



#### NOTE:

- Numeric values 1 to *n* in the syntax (for TACACS+ server) must be unique but need not be sequential. For example, the following syntax is valid:

```
allow-commands1="cmd1"
allow-commands3="cmd3"
allow-commands2="cmd2"
deny-commands3="cmd3"
deny-commands2="cmd2"
deny-commands1="cmd1"
```

- The limit on the number of lines of individual regular expressions is imposed by the TACACS+ or RADIUS server.
- When you issue the `show cli authorization` command, the command output displays the regular expression in a single line, even if you specify each individual expression on a separate line.

For more information about Juniper Networks vendor-specific RADIUS and TACACS+ attributes, see [“Juniper Networks Vendor-Specific RADIUS Attributes” on page 207](#) and [“Juniper Networks Vendor-Specific TACACS+ Attributes” on page 182](#).



**NOTE:** When RADIUS or TACACS+ authentication is configured for a router, regular expressions configured on the RADIUS or TACACS+ server merge with any regular expressions configured on the local router at the [edit system login class] hierarchy level using the allow-commands, deny-commands, allow-configuration, deny-configuration, or permissions statements. If the final expression has a syntax error, the overall result is an invalid regular expression.

**Related  
Documentation**

- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 175](#)

---

## Example: Configuring RADIUS Authentication

---

The Junos OS supports two protocols for central authentication of users on multiple routers: RADIUS and TACACS+. We recommend RADIUS because it is a multivendor IETF standard, and its features are more widely accepted than those of TACACS+ or other proprietary systems. In addition, we recommend using a one-time-password system for increased security, and all vendors of these systems support RADIUS.

The Junos OS uses one or more template accounts to perform user authentication. You create the template account or accounts, and then configure the user access to use that account. If the RADIUS server is unavailable, the fallback is for the login process to use the local account that set up on the router or switch.

The following example shows how to configure RADIUS authentication:

```
[edit]
system {
 authentication-order [radius password];
 root-authentication {
 encrypted-password "9aHlj8gqQ1gjyjjhgjgiiii"; # SECRET-DATA
 }
 name-server {
 10.1.1.1;
 10.1.1.2;
 }
}
```

The following example shows how to enable RADIUS authentication and define the shared secret between the client and the server. The secret enables the client and server to determine that they are talking to the trusted peer.

Define a timeout value for each server, so that if there is no response within the specified number of seconds, the router can try either the next server or the next authentication mechanism.

```
[edit]
```

```

system {
 radius-server {
 10.1.2.1 {
 secret "9aH1j8gqQ1sdjerrhser"; # SECRET-DATA
 timeout 5;
 }
 10.1.2.2 {
 secret "9aH1j8gqQ1csdoiuardwefoiud"; # SECRET-DATA
 timeout 5;
 }
 }
}

```

**Related Documentation**

- [Configuring RADIUS Authentication](#)

## Example: Configuring RADIUS Template Accounts

The following example shows how to configure RADIUS template accounts for different users or groups of users:

```

[edit]
system {
 login {
 user observation {
 uid 1001;
 class observation;
 }
 user operation {
 uid 1002;
 class operation;
 }
 user engineering {
 uid 1003;
 class engineering;
 }
 }
}

```

**Related Documentation**

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 217](#)

## Example: Configuring User Login Accounts

The following example shows how to configure the local administrator account (**user admin**). If RADIUS fails or becomes unreachable, the login process reverts to password authentication on the local accounts on the router or switch.

```

[edit]
system {
 login {
 user admin {
 uid 1000;
 class engineering;
 }
 }
}

```

```

 authentication {
 encrypted-password "<PASSWORD>"; # SECRET-DATA
 }
 }
}

```

Related Documentation • [Configuring Junos OS User Accounts](#)

## Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication

The following example shows how to configure system authentication for RADIUS, TACACS+, and password authentication.

In this example, only the user Philip and users authenticated by a remote RADIUS server can log in. If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the router or switch. If the RADIUS server is not available, the user is authenticated using the **password** authentication method and allowed access to the router or switch. For more information about the password authentication method, see [“Using Local Password Authentication” on page 176](#).

When Philip tries to log in to the system, if the RADIUS server authenticates him, he is given access and privileges for the **super-user** class. Local accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same user ID (UID) 9999 and the privileges associated with the **operator** class.

```

[edit]
system {
 authentication-order radius;
 login {
 user philip {
 full-name "Philip";
 uid 1001;
 class super-user;
 }
 user remote {
 full-name "All remote users";
 uid 9999;
 class operator;
 }
 }
}

```



**NOTE:** For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time. For example, when you create a remote template account, a set of remote users can concurrently share a single UID. For more information about template accounts, see [“Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 217](#).

When a user logs in to a device, the user's login name is used by the RADIUS or TACACS+ server for authentication. If the user is authenticated successfully by the authentication server and the user is not configured at the **[edit system login user]** hierarchy level, the device uses the default remote template user account for the user, provided a remote template account is configured at the **edit system login user remote** hierarchy level. The remote template account serves as a default template user account for all users that are authenticated by the authentication server but not having a locally configured user account on the device. Such users share the same login class and UID.

To configure an alternate template user, specify the **user-name** parameter returned in the RADIUS authentication response packet. Not all RADIUS servers allow you to change this parameter. The following shows a sample Junos OS configuration:

```
[edit]
system {
 authentication-order radius;
 login {
 user philip {
 full-name "Philip";
 uid 1001;
 class super-user;
 }
 user operator {
 full-name "All operators";
 uid 9990;
 class operator;
 }
 user remote {
 full-name "All remote users";
 uid 9999;
 class read-only;
 }
 }
}
```

Assume your RADIUS server is configured with the following information:

- User Philip with password “olympia”
- User Alexander with password “bucephalus” and username “operator”
- User Darius with password “redhead” and username “operator”
- User Roxane with password “athena”

Philip would be given access as a superuser (**super-user**) because he has his own local user account. Alexander and Darius share UID 9990 and have access as operators. Roxane has no template-user override, so she shares access with all the other remote users, getting read-only access.

#### Related Documentation

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



# Configuring and Managing RADIUS Accounting

- [Understanding RADIUS Accounting on page 201](#)
- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 202](#)
- [Juniper Networks Vendor-Specific RADIUS Attributes on page 207](#)
- [Configuring RADIUS System Accounting on page 209](#)
- [Configuring RADIUS Authentication \(QFX Series or OCX Series\) on page 211](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 214](#)
- [Example: Configuring RADIUS System Accounting on page 215](#)

## Understanding RADIUS Accounting

---

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

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

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

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

1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. For example, on FreeRADIUS, the default port is 1813.
2. The device forwards an *accounting-request* packet containing an event record to the accounting server. The event record associated with this supplicant contains an *Acct-Status-Type* attribute whose value indicates the beginning of user service for this supplicant. When the supplicant's session ends, the accounting request contains an *Acct-Status-Type* attribute value indicating the end of user service. The RADIUS accounting server records this as a stop-accounting record containing session information and the length of the session.
3. The RADIUS accounting server logs these events in a file as start-accounting or stop-accounting records. On FreeRADIUS, the filename is the server's address; for example, 122.69.1.250.
4. The accounting server sends an *accounting-response* packet back to the device confirming it has received the accounting request.
5. If the device does not receive a response from the server, it continues to send accounting requests until an accounting response is returned from the accounting server.

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

**Related Documentation** • [Configuring RADIUS System Accounting on page 209](#)

## Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication

Using the **authentication-order** statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch.

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

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

### Using RADIUS or TACACS+ Authentication

You can configure the Junos OS to be both a RADIUS and TACACS+ authentication client.

If an authentication method included in the **[authentication-order]** statement is not available, or if the authentication is available but returns a reject response, the Junos OS tries the next authentication method included in the **authentication-order** statement.

The RADIUS or TACACS+ server authentication might fail because of the following reasons:

- The authentication method is configured, but the corresponding authentication servers are not configured. For instance, the RADIUS and TACACS+ authentication methods are included in the **authentication-order** statement, but the corresponding RADIUS or TACACS+ servers are not configured at the respective **[edit system radius-server]** and **[edit system tacplus-server]** hierarchy levels.
- The RADIUS or TACACS+ server does not respond within the timeout period configured at the **[edit system radius-server]** or **[edit system tacplus-server]** hierarchy levels.
- The RADIUS or TACACS+ server is not reachable because of a network problem.

The RADIUS or TACACS+ server authentication might return a reject response because of the following reasons:

- The user profiles of users accessing a router or switch might not be configured on the RADIUS or TACACS+ server.
- The user enters incorrect logon credentials.

## Using Local Password Authentication

You can explicitly configure the password authentication method or use this method as a fallback mechanism when remote authentication servers fail. The password authentication method consults the local user profiles configured at the **[edit system login]** hierarchy level. Users can log in to a router or switch using their local username and password in the following scenarios:

- The password authentication method (password) is explicitly configured as one of the authentication methods in the **[authentication-order authentication-methods]** statement. In this case, the password authentication method is tried if no previous authentication accepts the logon credentials. This is true whether the previous authentication method fails to respond or returns a reject response because of an incorrect username or password.
- The password authentication method is not explicitly configured as one of the authentication methods in the **authentication-order authentication-methods** statement. In this case, the password authentication method is tried only if all configured authentication methods fail to respond. It is not consulted if any configured authentication method returns a reject response because of an incorrect username or password.

## Order of Authentication Attempts

[Table 28 on page 177](#) describes how the **authentication-order** statement at the **[edit system]** hierarchy level determines the procedure that the Junos OS uses to authenticate users for access to a router or switch.

Table 31: Order of Authentication Attempts

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

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

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

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

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



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

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

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

#### Related Documentation

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 217](#)
- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 171](#)

## Juniper Networks Vendor-Specific RADIUS Attributes

Junos OS supports the configuration of Juniper Networks RADIUS vendor-specific attributes (VSAs). These VSAs are encapsulated in a RADIUS vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. [Table 32 on page 207](#) lists the Juniper Networks VSAs you can configure.

**Table 32: Juniper Networks Vendor-Specific RADIUS Attributes**

| Name                        | Description                                                                                                                                                                                                                              | Type | Length | String                                                                                                                                                                                                                            |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Juniper-Local-User-Name     | Indicates the name of the user template used by this user when logging in to a device. This attribute is used only in Access-Accept packets.                                                                                             | 1    | ≥3     | One or more octets containing printable ASCII characters.                                                                                                                                                                         |
| Juniper-Allow-Commands      | Contains an extended regular expression that enables the user to run operational mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.   | 2    | ≥3     | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See <a href="#">“Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands” on page 145</a> .      |
| Juniper-Deny-Commands       | Contains an extended regular expression that denies the user permission to run operation mode commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.                       | 3    | ≥3     | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See <a href="#">“Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands” on page 145</a> .      |
| Juniper-Allow-Configuration | Contains an extended regular expression that enables the user to run configuration mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets. | 4    | ≥3     | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See <a href="#">“Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies” on page 144</a> . |
| Juniper-Deny-Configuration  | Contains an extended regular expression that denies the user permission to run configuration commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.                        | 5    | ≥3     | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See <a href="#">“Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies” on page 144</a> . |

Table 32: Juniper Networks Vendor-Specific RADIUS Attributes (*continued*)

| Name                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Type | Length | String                                                                                                                                                                                                                                        |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Juniper-Interactive-Command  | Indicates the interactive command entered by the user. This attribute is used only in Accounting-Request packets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 8    | ≥3     | One or more octets containing printable ASCII characters.                                                                                                                                                                                     |
| Juniper-Configuration-Change | Indicates the interactive command that results in a configuration (database) change. This attribute is used only in Accounting-Request packets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 9    | ≥3     | One or more octets containing printable ASCII characters.                                                                                                                                                                                     |
| Juniper-User-Permissions     | <p>Contains information the server uses to specify user permissions. This attribute is used only in Access-Accept packets.</p> <p><b>NOTE:</b> When the <b>Juniper-User-Permissions</b> attribute is configured to grant the Junos OS <b>maintenance</b> or <b>all</b> permissions on a RADIUS server, the UNIX wheel group membership is not automatically added to a user's list of group memberships. Some operations such as running the <b>su root</b> command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions <b>maintenance</b> or <b>all</b>, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account.</p> | 10   | ≥3     | <p>One or more octets containing printable ASCII characters.</p> <p>The string is a list of permission flags separated by a space. The exact name of each flag must be specified in its entirety. See <a href="#">Table 4 on page 10</a>.</p> |
| Juniper-Authentication-Type  | Indicates the authentication method (local database, or RADIUS server) used to authenticate a user. If the user is authenticated using a local database, the attribute value shows 'local'. If the user is authenticated using RADIUS server, the attribute value shows 'remote'.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 11   | ≥5     | One or more octets containing printable ASCII characters.                                                                                                                                                                                     |

Table 32: Juniper Networks Vendor-Specific RADIUS Attributes (*continued*)

| Name                 | Description                                                  | Type | Length          | String  |
|----------------------|--------------------------------------------------------------|------|-----------------|---------|
| Juniper-Session-Port | Indicates the source port number of the established session. | 12   | size of integer | Integer |

For more information about the VSAs, see RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*.

**Related Documentation**

- [Configuring RADIUS Authentication](#)
- [Configuring RADIUS Authentication \(QFX Series or OCX Series\) on page 192](#)

## Configuring RADIUS System Accounting

With RADIUS accounting enabled, Juniper Networks routers or switches, acting as RADIUS clients, can notify the RADIUS server about user activities such as software logins, configuration changes, and interactive commands. The framework for RADIUS accounting is described in RFC 2866.

Tasks for configuring RADIUS system accounting are:

1. [Configuring Auditing of User Events on a RADIUS Server on page 209](#)
2. [Specifying RADIUS Server Accounting and Auditing Events on page 209](#)
3. [Configuring RADIUS Server Accounting on page 210](#)

### Configuring Auditing of User Events on a RADIUS Server

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

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

### Specifying RADIUS Server Accounting and Auditing Events

To specify the events you want to audit when using a RADIUS server for authentication, include the **events** statement at the **[edit system accounting]** hierarchy level:

```
[edit system accounting]
events [events];
```

**events** is one or more of the following:

- **login**—Audit logins
- **change-log**—Audit configuration changes
- **interactive-commands**—Audit interactive commands (any command-line input)

## Configuring RADIUS Server Accounting

To configure RADIUS server accounting, include the **server** statement at the **[edit system accounting destination radius]** hierarchy level:

```
server {
 server-address {
 accounting-port port-number;
 secret password;
 source-address address;
 retry number;
 timeout seconds;
 }
}
```

**server-address** specifies the address of the RADIUS server. To configure multiple RADIUS servers, include multiple **server** statements.



**NOTE:** If no RADIUS servers are configured at the **[edit system accounting destination radius]** statement hierarchy level, the Junos OS uses the RADIUS servers configured at the **[edit system radius-server]** hierarchy level.

**accounting-port *port-number*** specifies the RADIUS server accounting port number.

The default port number is 1813.



**NOTE:** If you enable RADIUS accounting at the **[edit access profile *profile-name* accounting-order]** hierarchy level, accounting is triggered on the default port of 1813 even if you do not specify a value for the **accounting-port** statement.

You must specify a secret (password) that the local router or switch passes to the RADIUS client by including the **secret** statement. If the password contains spaces, enclose the entire password in quotation marks (" ").

In the **source-address** statement, specify a source address for the RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. The source address is a valid IPv4 address configured on one of the router or switch interfaces.

Optionally, you can specify the number of times that the router or switch attempts to contact a RADIUS authentication server by including the **retry** statement. By default, the

router or switch retries three times. You can configure the router or switch to retry from 1 through 10 times.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a RADIUS server by including the **timeout** statement. By default, the router or switch waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

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

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

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

## Configuring RADIUS Authentication (QFX Series or OCX Series)

RADIUS authentication is a method of authenticating users who attempt to access the router or switch. Tasks to configure RADIUS authentication are:



**NOTE:** The **source-address** statement is not supported at the **[edit system radius-options]** or **[edit system-radius-server name]** hierarchies on the QFabric system.

- [Configuring RADIUS Server Details on page 211](#)
- [Configuring MS-CHAPv2 for Password-Change Support on page 212](#)
- [Specifying a Source Address for the Junos OS to Access External RADIUS Servers on page 213](#)

## Configuring RADIUS Server Details

To use RADIUS authentication on the router or switch, configure information about one or more RADIUS servers on the network by including one **radius-server** statement at the **[edit system]** hierarchy level for each RADIUS server:

```
[edit system]
radius-server server-address {
 accounting-port port-number;
 port number;
 retry number;
 secret password;
 source-address source-address;
 timeout seconds;
}
```

**server-address** is the address of the RADIUS server.

You can specify a port on which to contact the RADIUS server. By default, port number **1812** is used (as specified in RFC 2865). You can also specify an accounting port to send accounting packets. The default is **1813** (as specified in RFC 2866).

You must specify a password in the **secret password** statement. If the password contains spaces, enclose it in quotation marks. The secret used by the local router or switch must match that used by the server.

Optionally, you can specify the amount of time that the local router or switch waits to receive a response from a RADIUS server (in the **timeout** statement) and the number of times that the router or switch attempts to contact a RADIUS authentication server (in the **retry** statement). By default, the router or switch waits 3 seconds. You can configure this to be a value from 1 through 90 seconds. By default, the router or switch retries connecting to the server three times. You can configure this to be a value from 1 through 10 times.

You can use the **source-address** statement to specify a logical address for individual or multiple RADIUS servers.

To configure multiple RADIUS servers, include multiple **radius-server** statements.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the **user** statement at the **[edit system login]** hierarchy level, as described in [“Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 217](#).

You can also configure RADIUS authentication at the **[edit access]** and **[edit access profile]** hierarchy level. Junos OS uses the following search order to determine which set of servers are used for authentication:

1. **[edit access profile profile-name radius-server server-address]**
2. **[edit access radius-server server-address]**
3. **[edit system radius-server server-address]**

## Configuring MS-CHAPv2 for Password-Change Support

You can configure the Microsoft implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the router or switch to support changing of passwords. This feature provides users accessing a router or switch the option of changing the password when the password expires, is reset, or is configured to be changed at the next login.

Before you configure MS-CHAPv2 for password-change support, ensure that you:

- Configure the RADIUS server authentication parameters
- Set the **authentication-order** to use the RADIUS server for the initial password attempt

To configure MS-CHAP-v2, include the following statements at the **[edit system radius-options]** hierarchy level:

```
[edit system radius-options]
password-protocol mschap-v2;
```

The following example shows statements for configuring the MS-CHAPv2 password protocol, password authentication order, and user accounts:

```
[edit]
system {
 authentication-order [radius password];
 radius-server {
 192.168.69.149 secret "9G-j.5Qz6tpBk.1hrlXxUjiq5Qn/C"; ## SECRET-DATA
 }
 radius-options {
 password-protocol mschap-v2;
 }
 login {
 user bob {
 class operator;
 }
 }
}
```

## Specifying a Source Address for the Junos OS to Access External RADIUS Servers

You can specify which source address Junos OS uses when accessing your network to contact an external RADIUS server for authentication. You can also specify which source address Junos OS uses when contacting a RADIUS server for sending accounting information.

To specify a source address for a RADIUS server, include the **source-address** statement at the **[edit system radius-server server-address]** hierarchy level:

```
[edit system radius-server server-address]
source-address source-address;
```

**source-address** is a valid IP address configured on one of the router or switch interfaces.

### Related Documentation

- [Example: Configuring RADIUS Authentication on page 196](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 171](#)
- [Juniper Networks Vendor-Specific RADIUS Attributes on page 207](#)
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 217](#)
- [Example: Configuring RADIUS Template Accounts on page 197](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 194](#)
- [Junos OS User Authentication Methods on page 14](#)

## Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands

---

Use regular expressions to specify which operational or configuration mode commands are allowed or denied when you use a RADIUS or TACACS+ server for user authentication. You can specify the regular expressions using the appropriate Juniper Networks vendor-specific RADIUS or TACACS+ attributes in your authentication server configuration.

You can specify **allow-configuration**, **deny-configuration**, **allow-commands**, or **deny-commands** in a single extended regular expression, enclosing multiple commands in parentheses and separating them using the pipe symbol. For example, you can specify multiple **allow-commands** parameters using: **allow-commands= (cmd1 | cmd2 | cmdn)**. You can specify **user-permissions** as a list of comma-separated values, and not as a regular expression.

On a RADIUS or TACACS+ server, you can also use a simplified version for regular expressions where you specify each individual expression on a separate line. The simplified version is valid for **allow-commands**, **deny-commands**, **allow-configuration**, **deny-configuration**, and **permissions** vendor-specific attributes.

For a RADIUS server, specify the individual regular expressions using the following syntax:

```
Juniper-Allow-Commands+= "cmd1"
Juniper-Allow-Commands+= "cmd2"
Juniper-Allow-Commands+= "cmdn"
Juniper-Deny-Commands+= "cmd1"
Juniper-Deny-Commands+= "cmd2"
Juniper-Deny-Commands+= "cmdn"
Juniper-Allow-Configuration+= "regex1"
Juniper-Allow-Configuration+= "regex2"
Juniper-Allow-Configuration+= "regextn"
Juniper-Deny-Configuration+= "regex1"
Juniper-Deny-Configuration+= "regex2"
Juniper-Deny-Configuration+= "regextn"
Juniper-User-Permissions+= "permission-flag1"
Juniper-User-Permissions+= "permission-flag2"
Juniper-User-Permissions+= "permission-flagn"
```

For TACACS+ server, specify the individual regular expressions using the following syntax:

```
allow-commands1= "cmd1"
allow-commands2= "cmd2"
allow-commandsn= "cmdn"
deny-commands1= "cmd1"
deny-commands2= "cmd2"
deny-commandsn= "cmdn"
allow-configuration1= "regex1"
allow-configuration2= "regex2"
allow-configurationn= "regextn"
deny-configuration1= "regex1"
deny-configuration2= "regex2"
deny-configurationn= "regextn"
user-permissions1= "permission-flag1"
```

```
user-permissions2="permission-flag2"
user-permissionsn="permission-flagn "
```

**NOTE:**

- Numeric values 1 to *n* in the syntax (for TACACS+ server) must be unique but need not be sequential. For example, the following syntax is valid:
 

```
allow-commands1="cmd1"
allow-commands3="cmd3"
allow-commands2="cmd2"
deny-commands3="cmd3"
deny-commands2="cmd2"
deny-commands1="cmd1"
```
- The limit on the number of lines of individual regular expressions is imposed by the TACACS+ or RADIUS server.
- When you issue the `show cli authorization` command, the command output displays the regular expression in a single line, even if you specify each individual expression on a separate line.

For more information about Juniper Networks vendor-specific RADIUS and TACACS+ attributes, see [“Juniper Networks Vendor-Specific RADIUS Attributes” on page 207](#) and [“Juniper Networks Vendor-Specific TACACS+ Attributes” on page 182](#).



**NOTE:** When RADIUS or TACACS+ authentication is configured for a router, regular expressions configured on the RADIUS or TACACS+ server merge with any regular expressions configured on the local router at the [edit system login class] hierarchy level using the `allow-commands`, `deny-commands`, `allow-configuration`, `deny-configuration`, or `permissions` statements. If the final expression has a syntax error, the overall result is an invalid regular expression.

- Related Documentation**
- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 175](#)

## Example: Configuring RADIUS System Accounting

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

```
system {
 accounting {
 events [login change-log interactive-commands];
 destination {
 radius {
 server {
 10.5.5.5 {
 accounting-port 3333;
 secret 9dkafeqwrew;
```

```
 source-address 10.1.1.1;
 retry 3;
 timeout 3;
 }
 10.6.6.6 secret $$fe3erqwrez;
 10.7.7.7 secret $$f34929ftby;
}
}
}
```

**Related Documentation**

- [Configuring RADIUS System Accounting on page 209](#)

# Configuring and Managing RADIUS Template Accounts

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 217](#)
- [Example: Configuring RADIUS Template Accounts on page 217](#)

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

---

When you use local password authentication, you must create a local user account for every user who wants to access the system. However, when you are using RADIUS or TACACS+ authentication, you can create single accounts (for authorization purposes) that are shared by a set of users. You create these accounts using the remote and local user template accounts. When a user is using a template account, the command-line interface (CLI) username is the login name; however, the privileges, file ownership, and effective user ID are inherited from the template account.

### Related Documentation

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

## Example: Configuring RADIUS Template Accounts

---

The following example shows how to configure RADIUS template accounts for different users or groups of users:

```
[edit]
system {
 login {
 user observation {
 uid 1001;
 class observation;
 }
 user operation {
 uid 1002;
 class operation;
 }
 user engineering {
 uid 1003;
```

```
 class engineering;
 }
}
}
```

**Related Documentation**

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 217](#)

## CHAPTER 15

# Configuring and Managing VSAs for RADIUS and TACACS+

- [Understanding VSAs on page 219](#)
- [VSA Match Conditions and Actions on page 220](#)
- [Juniper Networks Vendor-Specific TACACS+ Attributes on page 222](#)

### Understanding VSAs

---

Devices support the configuration of RADIUS server attributes specific to Juniper Networks. These attributes are known as vendor-specific attributes (VSAs) and are described in RFC 2138, *Remote Authentication Dial In User Service* (RADIUS).

Through VSAs, you can configure port-filtering attributes on the RADIUS server. VSAs are cleartext fields sent from the RADIUS server to the device as a result of authentication success or failure. Authentication prevents unauthorized user access by blocking a supplicant at the port until the device is authenticated by the RADIUS server. The VSA attributes are interpreted by the device during authentication, and the device takes appropriate actions. Implementing port-filtering attributes with authentication on the RADIUS server provides a central location for controlling LAN access for supplicants.

These port-filtering attributes specific to Juniper Networks are encapsulated in a RADIUS server VSA with the vendor ID set to the Juniper Networks ID number, 2636.

As well as configuring port-filtering attributes through VSAs, you can apply a port firewall filter that has already been configured on the device directly to the RADIUS server. Like port-filtering attributes, the filter is applied during the authentication process, and its actions are applied at the device port. Adding a port firewall filter to a RADIUS server eliminates the need to add the filter to multiple ports and devices.

#### Related Documentation

- [Configuring Firewall Filters](#)
- [Configuring RADIUS Authentication \(QFX Series or OCX Series\) on page 192](#)
- [VSA Match Conditions and Actions on page 38](#)

## VSA Match Conditions and Actions

Devices support the configuration of RADIUS server attributes specific to Juniper Networks. These attributes are known as vendor-specific attributes (VSAs). They are configured on RADIUS servers and work in combination with 802.1X authentication. Using VSAs, you can apply port firewall filter attributes as a subset of match conditions and actions sent from the RADIUS server to the switch as a result of successful 802.1X authentication.

Each term in a VSA configured through the RADIUS server consists of *match conditions* and an *action*. Match conditions are the values or fields that the packet must contain. You can define single, multiple, or no match conditions. If no match conditions are specified for the term, the packet is accepted by default. The action is the action that the switch takes if a packet matches the match conditions for the specific term. Allowed actions are to accept a packet or to discard a packet.

The following guidelines apply when you specify match conditions and actions for VSAs:

- Both **match** and **action** statements are mandatory.
- Any or all options (separated by commas) may be included in each **match** and **action** statement.
- Fields separated by commas will be ANDed if they are of a different type. The same types cannot be repeated.
- For OR cases (for example, match **10.1.1.0/24 OR 11.1.1.0/24**), apply multiple VSAs to the 802.1X supplicant.
- In order for the **forwarding-class** option to be applied, the forwarding class must be configured on the switch. If it is not configured on the switch, this option is ignored.

[Table 7 on page 38](#) describes the match conditions you can specify when configuring a VSA using the **match** command on the RADIUS server. The string that defines a match condition is called a *match statement*.

**Table 33: Match Conditions**

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

Table 33: Match Conditions (*continued*)

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

When you define one or more terms that specify the filtering criteria, you also define the action to take if the packet matches all criteria. [Table 8 on page 39](#) shows the actions that you can specify in a term.

Table 34: Actions for VSAs

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

- Related Documentation**
- [Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 40](#)
  - [Understanding 802.1X and VSAs on Switches on page 37](#)
  - [Understanding VSAs on page 219](#)

## Juniper Networks Vendor-Specific TACACS+ Attributes

Junos OS supports the configuration of Juniper Networks TACACS+ vendor-specific attributes (VSAs). These VSAs are encapsulated in a TACACS+ vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. [Table 29 on page 183](#) lists the Juniper Networks VSAs you can configure.

**Table 35: Juniper Networks Vendor-Specific TACACS+ Attributes**

| Name                       | Description                                                                                                                                                                          | Length | String                                                                                                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>local-user-name</b>     | Indicates the name of the user template used by this user when logging in to a device.                                                                                               | ≥3     | One or more octets containing printable ASCII characters.                                                                                                                                                                         |
| <b>allow-commands</b>      | Contains an extended regular expression that enables the user to run operational mode commands in addition to those commands authorized by the user's login class permission bits.   | ≥3     | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See <a href="#">Table 21 on page 146</a> .                                                                               |
| <b>allow-configuration</b> | Contains an extended regular expression that enables the user to run configuration mode commands in addition to those commands authorized by the user's login class permission bits. | ≥3     | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See <a href="#">"Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies" on page 144</a> . |
| <b>deny-commands</b>       | Contains an extended regular expression that denies the user permission to run operational mode commands authorized by the user's login class permission bits.                       | ≥3     | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See <a href="#">Table 21 on page 146</a> .                                                                               |
| <b>deny-configuration</b>  | Contains an extended regular expression that denies the user permission to run configuration mode commands authorized by the user's login class permission bits.                     | ≥3     | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See <a href="#">Table 20 on page 145</a> .                                                                               |

Table 35: Juniper Networks Vendor-Specific TACACS+ Attributes (*continued*)

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

- Related Documentation**
- [Configuring TACACS+ Authentication](#)
  - [Configuring TACACS+ Authentication \(QFX Series\) on page 180](#)



## PART 4

# Configuration Statements and Operational Commands

- [Configuration Statements on page 227](#)
- [Operational Commands on page 335](#)



## CHAPTER 16

# Configuration Statements

- [access](#) on page 230
- [accounting \(Access Profile\)](#) on page 231
- [accounting-options](#) on page 232
- [accounting-server](#) on page 234
- [accounting-stop-on-access-deny](#) on page 235
- [accounting-stop-on-failure](#) on page 236
- [advertisement-interval](#) on page 237
- [agent-address](#) on page 238
- [archival](#) on page 239
- [archive-sites \(Configuration File\)](#) on page 240
- [authentication-order](#) on page 241
- [authentication-server](#) on page 242
- [authenticator](#) on page 243
- [authorization](#) on page 244
- [block-interval](#) on page 245
- [categories](#) on page 245
- [client-list](#) on page 246
- [client-list-name](#) on page 246
- [clients](#) on page 247
- [commit-delay](#) on page 247
- [community \(SNMP\)](#) on page 248
- [configuration](#) on page 249
- [connection-limit](#) on page 250
- [contact](#) on page 251
- [disable \(802.1X\)](#) on page 251
- [disable \(LLDP\)](#) on page 252
- [dot1x](#) on page 253
- [eapol-block](#) on page 254

- [falling-threshold \(Health Monitor\) on page 255](#)
- [filter-duplicates on page 255](#)
- [full-name on page 256](#)
- [guest-vlan on page 256](#)
- [health-monitor on page 257](#)
- [hold-multiplier on page 258](#)
- [idle-timeout \(Access\) on page 259](#)
- [interface \(802.1X\) on page 260](#)
- [interface \(LLDP\) on page 262](#)
- [interface \(Static MAC Bypass\) on page 263](#)
- [interval \(Health Monitor\) on page 264](#)
- [lldp on page 265](#)
- [lldp-med \(Ethernet Switching\) on page 267](#)
- [lldp-med-bypass on page 268](#)
- [lldp-configuration-notification-interval on page 268](#)
- [location on page 269](#)
- [mac-radius on page 270](#)
- [management-address on page 271](#)
- [maximum-requests on page 272](#)
- [name on page 272](#)
- [nas-ip-address on page 273](#)
- [no-mac-table-binding \(802.1X\) on page 273](#)
- [nonvolatile on page 274](#)
- [no-reauthentication on page 274](#)
- [oid on page 275](#)
- [order on page 276](#)
- [port \(RADIUS Server\) on page 277](#)
- [profile on page 278](#)
- [protocols on page 279](#)
- [protocol-version on page 292](#)
- [ptopo-configuration-maximum-hold-time on page 293](#)
- [ptopo-configuration-trap-interval on page 293](#)
- [quiet-period on page 294](#)
- [radius on page 295](#)
- [radius-options \(edit system\) on page 296](#)
- [radius-options \(Protocols 802.1X\) on page 297](#)
- [radius-server on page 298](#)

- [rate-limit on page 299](#)
- [reauthentication on page 300](#)
- [remote-debug-permission on page 301](#)
- [retries on page 302](#)
- [retry on page 303](#)
- [rising-threshold \(Health Monitor\) on page 304](#)
- [root-login on page 305](#)
- [server-fail on page 306](#)
- [server-timeout on page 307](#)
- [services \(Switches\) on page 308](#)
- [snmp on page 309](#)
- [ssh on page 313](#)
- [static \(Protocols 802.1X\) on page 314](#)
- [supplicant on page 315](#)
- [supplicant-timeout on page 316](#)
- [system on page 317](#)
- [tacplus-options on page 323](#)
- [targets on page 324](#)
- [transmit-period on page 324](#)
- [traceoptions \(LLDP\) on page 325](#)
- [transfer-interval \(Configuration\) on page 327](#)
- [transfer-on-commit on page 328](#)
- [trap-group on page 329](#)
- [trap-options on page 330](#)
- [user \(Access\) on page 331](#)
- [version on page 332](#)
- [vlan-assignment on page 333](#)
- [voip on page 334](#)

## access

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> access {   address-assignment   pool <i>pool-name</i>   address-pool <i>pool-name</i>   profile <i>profile-name</i> {     accounting (Access Profile) {       accounting-stop-on-access-deny;       accounting-stop-on-failure;       (authentication-order (ldap radius   none);       order (radius   none);     }     radius {       accounting-server [<i>server-addresses</i>];       authentication-server [<i>server-addresses</i>];     }   } } </pre> |
| <b>Hierarchy Level</b>          | [edit]                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p>                                                                                                                                                                                                                            |
| <b>Description</b>              | <p>Configure authentication, authorization, and accounting (AAA) services.</p> <p>The statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                       |
|                                 | <div>  <p><b>NOTE:</b> The [edit access] hierarchy is not available on QFabric systems.</p> </div>                                                                                                                                                                                                                                                                                |
| <b>Default</b>                  | Not enabled                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 67</a></li> </ul>                                                                                                                                                                                                                                                                                                                                    |

## accounting (Access Profile)

|                            |                                                                                                                                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> accounting {   accounting-stop-on-access-deny;   accounting-stop-on-failure;   order (radius   none); } </pre>                                                                                                                      |
| <b>Hierarchy Level</b>     | [edit access profile <i>profile-name</i> ]                                                                                                                                                                                                |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> |
| <b>Description</b>         | Configure the authentication order for authentication, authorization, and accounting (AAA) services.                                                                                                                                      |
| <b>Default</b>             | Not enabled                                                                                                                                                                                                                               |
| <b>Options</b>             | <p><b>none</b>—Use no authentication for specified subscribers.</p> <p><b>radius</b>—Use RADIUS authentication for specified subscribers.</p> <p>The remaining statements are explained separately.</p>                                   |



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

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25</a></li> <li>• <a href="#">Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 67</a></li> <li>• <a href="#">Understanding 802.1X and RADIUS Accounting on Switches on page 66</a></li> <li>• <a href="#">Configuring RADIUS Accounting</a></li> <li>• <a href="#">Understanding RADIUS Accounting on page 201</a></li> </ul> |

## accounting-options

---

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

```

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

```

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hierarchy Level</b>          | [edit]                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | Configure options for accounting statistics collection.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Understanding RADIUS Accounting on page 201</a></li> <li>• <a href="#">Understanding VSAs on page 219</a></li> <li>• <a href="#">Configuring RADIUS System Accounting on page 209</a></li> <li>• <i>Configuring Remote Template Accounts for User Authentication</i></li> <li>• <i>Configuring Local User Template Accounts for User Authentication</i></li> </ul> |

## accounting-server

---

|                            |                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>accounting-server[server-addresses];</code>                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>     | [edit access profile <i>profile-name</i> radius]                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b> | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                         |
| <b>Description</b>         | Configure the Remote Authentication Dial-In User Service (RADIUS) server for authentication. To configure multiple RADIUS servers, include multiple server addresses. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached. |
| <b>Default</b>             | Not enabled                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>             | <i>server-addresses</i> —One or more addresses of RADIUS authentication servers.                                                                                                                                                                                                                                                                   |



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

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show network-access aaa statistics authentication on page 367</a></li><li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25</a></li><li>• <a href="#">Understanding 802.1X and RADIUS Accounting on Switches on page 66</a></li><li>• <a href="#">Understanding RADIUS Accounting on page 201</a></li></ul> |

## accounting-stop-on-access-deny

|                            |                                                                                                                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | accounting-stop-on-access-deny;                                                                                                                                                                                            |
| <b>Hierarchy Level</b>     | [edit access profile <i>profile-name</i> accounting]                                                                                                                                                                       |
| <b>Release Information</b> | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>         | Configure the authentication order for authentication, authorization, and accounting (AAA) services to send an Acct-Stop message if the AAA server denies access to a supplicant.                                          |




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


|                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>                  | Not enabled                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25</a></li> <li>• <a href="#">Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 67</a></li> <li>• <a href="#">show network-access aaa statistics authentication on page 367</a></li> <li>• <a href="#">Configuring RADIUS Accounting</a></li> </ul> |

## accounting-stop-on-failure

---

|                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                              | accounting-stop-on-failure;                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>                                                                                                                                                     | [edit access profile <i>profile-name</i> accounting]                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>                                                                                                                                                 | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                                                                                  |
| <b>Description</b>                                                                                                                                                         | Configure authentication order for authentication, authorization, and accounting (AAA) services to send an Acct-Stop message if a supplicant fails AAA authorization, but the RADIUS server grants access. For example, a supplicant might fail AAA authentication because of an internal error such as a timeout.                                                                                                                                          |
| <div> <b>NOTE:</b> The [edit access] hierarchy is not available on QFabric systems.</div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Default</b>                                                                                                                                                             | Not enabled                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b>                                                                                                                                            | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>                                                                                                                                               | <ul style="list-style-type: none"><li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25</a></li><li>• <a href="#">Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 67</a></li><li>• <a href="#">Understanding 802.1X and RADIUS Accounting on Switches on page 66</a></li><li>• <a href="#">Configuring RADIUS Accounting</a></li><li>• <a href="#">Understanding RADIUS Accounting on page 201</a></li></ul> |

## advertisement-interval

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>advertisement-interval seconds;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit protocols lldp],<br>[edit routing-instances <i>routing-instance-name</i> protocols lldp]                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.6 for MX Series and T Series routers.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                                                                                                    |
| <b>Description</b>              | <p>For MX Series and T Series routers and EX Series switches, configure an interval for LLDP advertisement.</p> <p>For switches configured for Link Layer Discovery Protocol, configure the frequency at which LLDP advertisements are sent.</p> <p>The <b>advertisement-interval</b> value must be greater than or equal to four times the <b>transmit-delay</b> value, or an error will be returned when you attempt to commit the configuration.</p>                                                                                                           |
|                                 | <div>  <p><b>NOTE:</b> The default value of <b>transmit-delay</b> is 2 seconds. If you configure the <b>advertisement-interval</b> as less than 8 seconds and you do not configure a value for <b>transmit-delay</b>, the default value of <b>transmit-delay</b> is automatically changed to 1 second in order to satisfy the requirement that the <b>advertisement-interval</b> value must be greater than or equal to four times the <b>transmit-delay</b> value.</p> </div> |
| <b>Default</b>                  | Disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                  | <p><b>seconds</b>—Interval between LLDP advertisement.</p> <p><b>Default:</b> 30</p> <p><b>Range:</b> 5 through 32768</p>                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring LLDP</a></li> <li>• <a href="#">show lldp on page 353</a></li> <li>• <a href="#">Configuring LLDP (CLI Procedure) on page 104</a></li> <li>• <a href="#">Understanding 802.1X and LLDP and LLDP-MED on page 101</a></li> <li>• <a href="#">transmit-delay</a></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul>                                                                                                                                                                 |

## agent-address

---

|                                 |                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | agent-address outgoing-interface;                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit snmp trap-options]                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                          |
| <b>Description</b>              | Set the agent address of all SNMPv1 traps generated by this router or switch. Currently, the only option is <b>outgoing-interface</b> , which sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.                                                                                        |
| <b>Options</b>                  | <b>outgoing-interface</b> —Value of the agent address of all SNMPv1 traps generated by this router or switch. The <b>outgoing-interface</b> option sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.<br><b>Default:</b> Disabled (the agent address is not specified in SNMPv1 traps). |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Configuring the Agent Address for SNMP Traps</i></li></ul>                                                                                                                                                                                                                                  |

## archival

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

**Hierarchy Level** [edit system]

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

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

**Options** The remaining statements are explained separately.





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

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

**Related Documentation**

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

## archive-sites (Configuration File)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>archive-sites {     file://&lt;path&gt;/&lt;filename&gt;;     ftp://username@host:&lt;port&gt;url-path password password;     http://username@host:&lt;port&gt;url-path password password;     pasvftp://username@host:&lt;port&gt;url-path password password;     scp://username@host:&lt;port&gt;url-path password password; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>     | [edit system archival configuration]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b> | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>         | <p>Specify where to transfer the current configuration files. When specifying a URL in a Junos OS statement using an IPv6 host address, you must enclose the entire URL in quotation marks ( " ") and enclose the IPv6 host address in brackets ( [ ] ). For example, <b>"scp://username&lt;:password&gt;@[ipv6-host-address]&lt;:port&gt;/url-path"</b></p> <p>If you specify more than one archive site, the router or switch attempts to transfer the configuration files to the first archive site in the list, moving to the next only if the transfer fails.</p> <p>The destination filename is saved in the following format, where <i>n</i> corresponds to the number of the compressed configuration rollback file that has been archived:</p> <p><b>router-name_juniper.conf.n.gz_YYYYMMDD_HHMMSS.</b></p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> <b>NOTE:</b> The time included in the destination filename is always in Coordinated Universal Time (UTC) regardless of whether the time on the router or switch is configured as UTC or the local time zone. The default time zone on the router or switch is UTC.</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> <b>NOTE:</b> The [edit system archival] hierarchy is not available on QFabric systems.</p> </div> |
| <b>Options</b>             | <p>The prefix used in the configuration statement determines the form of transfer:</p> <p><b>file://</b> —transfer on a path to a named file</p> <p><b>ftp://</b> —transfer using active FTP server</p> <p><b>http://</b> —transfer using HTTP server</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

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

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

|                                 |                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site</i></li> <li>• <i>Junos OS Commit Model for Router or Switch Configuration</i></li> <li>• <a href="#">configuration on page 249</a></li> <li>• <a href="#">transfer-on-commit on page 328</a></li> </ul> |

## authentication-order

|                            |                                                                                                                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | authentication-order [none   password   radius];                                                                                                                                                                           |
| <b>Hierarchy Level</b>     | [edit <a href="#">access profile</a> profile-name],<br>[edit <a href="#">system</a> ]                                                                                                                                      |
| <b>Release Information</b> | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>         | Configure the order of authentication, authorization, and accounting (AAA) servers to use while sending authentication messages.                                                                                           |
| <b>Default</b>             | Not enabled                                                                                                                                                                                                                |
| <b>Options</b>             | <p><b>none</b>—No authentication for specified subscribers.</p> <p><b>password</b>—Password authentication.</p> <p><b>radius</b>—RADIUS authentication.</p>                                                                |



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

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

## authentication-server

---

|                                 |                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>authentication-server [server-addresses];</code>                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> radius]                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                            |
| <b>Description</b>              | Configure the RADIUS server for authentication. To configure multiple RADIUS servers, include multiple server addresses. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached. |
| <b>Options</b>                  | <b>server-addresses</b> —Configure one or more RADIUS server addresses.                                                                                                                                                                                                                               |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25</a></li><li>• <a href="#">show network-access aaa statistics authentication on page 367</a></li></ul>                                                                       |

## authenticator

**Syntax**

```
authenticator {
 authentication-profile-name access-profile-name;
 interface (all | [interface-names]) {
 disable;
 guest-vlan (vlan-id | vlan-name);
 lldp-med-bypass;
 mac-radius <restrict>;
 maximum-requests number;
 no-reauthentication;
 quiet-period seconds;
 reauthentication interval;
 retries number;
 server-fail (deny | permit | use-cache | vlan-id | vlan-name);
 server-reject-vlan (vlan-id | vlan-name) {
 eapol-block;
 block-interval block-interval;
 }
 server-timeout seconds;
 supplicant (single | single-secure | multiple);
 supplicant-timeout seconds;
 transmit-period seconds;
 }
 no-mac-table-binding;
 radius-options {
 use-vlan-id;
 use-vlan-name;
 }
 static mac-address {
 vlan-assignment vlan-identifier;
 }
}
```

**Hierarchy Level** [edit protocols [dot1x](#)]

**Release Information** Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

**Description** Configure an authenticator for 802.1X authentication.

The statements are explained separately.



**NOTE:** You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.

**Default** 802.1X authentication is disabled.


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

- Related Documentation**
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 22](#)
  - [Specifying RADIUS Server Connections on Switches \(CLI Procedure\) on page 24](#)
  - [Example: Configuring Static MAC Bypass of Authentication on a Switch on page 95](#)

---

## authorization

---

|                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                     | <code>authorization <i>authorization</i>;</code>                                                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>                                                                                                                                                            | <code>[edit snmp community <i>community-name</i>]</code>                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>                                                                                                                                                        | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                 |
| <b>Description</b>                                                                                                                                                                | Set the access authorization for SNMP <b>Get</b> , <b>GetBulk</b> , <b>GetNext</b> , and <b>Set</b> requests.                                                                                                                                                                                                                 |
| <b>Options</b>                                                                                                                                                                    | <i>authorization</i> —Access authorization level: <ul style="list-style-type: none"><li>• <b>read-only</b>—Enable <b>Get</b>, <b>GetNext</b>, and <b>GetBulk</b> requests.</li><li>• <b>read-write</b>—Enable all requests, including <b>Set</b> requests. You must configure a view to enable <b>Set</b> requests.</li></ul> |
| <div> <b>NOTE:</b> The read-write option is not supported on the QFX3000 QFabric system.</div> |                                                                                                                                                                                                                                                                                                                               |
| <b>Default:</b> read-only                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                               |
| <b>Required Privilege Level</b>                                                                                                                                                   | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                 |
| <b>Related Documentation</b>                                                                                                                                                      | <ul style="list-style-type: none"><li>• <a href="#">Configuring the SNMP Community String</a></li></ul>                                                                                                                                                                                                                       |

## block-interval

|                                 |                                                                                                                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>block-interval <i>block-interval</i>;</code>                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | <code>[edit protocols <b>dot1x authenticator interface</b> (all   [<i>interface-names</i>]) server-reject-vlan (<i>vlan-id</i>   <i>vlan-name</i>)],</code><br><code>[edit protocols dot1x authenticator interface (all   [<i>interface-names</i>]) server-reject-vlan]</code> |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                              |
| <b>Description</b>              | Specify the amount of time that the 802.1X interface ignores Extensible Authentication Protocol (EAP) start messages from the client when an EAPoL block has been enabled on the 802.1X interface.                                                                             |
| <b>Options</b>                  | <b><i>block-interval</i></b> —The number of seconds for the interval.<br><b>Range:</b> 120 through 65,535                                                                                                                                                                      |
| <b>Required Privilege Level</b> | <code>routing</code> —To view this statement in the configuration.<br><code>routing-control</code> —To add this statement to the configuration.                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">eapol-block on page 254</a></li> <li>• <a href="#">Example: Configuring Fallback Options on Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 69</a></li> </ul>                                     |

## categories

|                                 |                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>categories {<br/>    <i>category</i>;<br/>}</code>                                                                                                                                      |
| <b>Hierarchy Level</b>          | <code>[edit snmp trap-group <i>group-name</i>]</code>                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                 |
| <b>Description</b>              | Define the types of traps that are sent to the targets of the named trap group.                                                                                                               |
| <b>Default</b>                  | If you omit the <b>categories</b> statement, all trap types are included in trap notifications.                                                                                               |
| <b>Options</b>                  | <b><i>category</i></b> —Name of a trap type: <b>authentication</b> , <b>chassis</b> , <b>configuration</b> , <b>link</b> , <b>remote-operations</b> , <b>rmon-alarm</b> , or <b>startup</b> . |
| <b>Required Privilege Level</b> | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring SNMP Trap Groups</a></li> </ul>                                                                                              |

## client-list

---

|                                 |                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>client-list <i>client-list-name</i> {<br/>    <i>ip-addresses</i>;<br/>}</code>                                                          |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.  |
| <b>Description</b>              | Define a list of SNMP clients.                                                                                                                 |
| <b>Options</b>                  | <i>client-list-name</i> —Name of the client list.<br><br><i>ip-addresses</i> —IP addresses of the SNMP clients to be added to the client list, |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Adding a Group of Clients to an SNMP Community</i></li></ul>                                        |

## client-list-name

---

|                                 |                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>client-list-name <i>client-list-name</i>;</code>                                                                                        |
| <b>Hierarchy Level</b>          | [edit snmp community <i>community-name</i> ]                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Add a client list or prefix list to an SNMP community.                                                                                        |
| <b>Options</b>                  | <i>client-list-name</i> —Name of the client list or prefix list.                                                                              |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Adding a Group of Clients to an SNMP Community</i></li></ul>                                       |

## clients

|                                 |                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clients {<br><i>address</i> <restrict>;<br>}                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit snmp community <i>community-name</i> ]                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                              |
| <b>Description</b>              | Specify the IPv4 or IPv6 addresses of the SNMP client hosts that are authorized to use this community.                                                                                                                                                                                                     |
| <b>Default</b>                  | If you omit the <b>clients</b> statement, all SNMP clients using this community string are authorized to access the switch.                                                                                                                                                                                |
| <b>Options</b>                  | <b>address</b> —Address of an SNMP client that is authorized to access this switch. You must specify an address, not a hostname. To specify more than one client, include multiple <b>address</b> options.<br><br><b>restrict</b> —(Optional) Do not allow the specified SNMP client to access the switch. |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Configuring SNMP Communities</i></li> </ul>                                                                                                                                                                                                                    |

## commit-delay

|                                 |                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | commit-delay <i>seconds</i> ;                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit snmp nonvolatile]                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Configure the timer for the SNMP <b>Set</b> reply and start of the commit.                                                                    |
| <b>Options</b>                  | <b>seconds</b> —Delay between an affirmative SNMP <b>Set</b> reply and start of the commit operation.<br><b>Default:</b> 5 seconds            |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Configuring the Commit Delay Timer</i></li> </ul>                                                 |

## community (SNMP)

---

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

**Hierarchy Level**    [edit snmp]

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

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



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

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

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


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

The remaining statements are explained separately.

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

**Related Documentation**    • *Configuring the SNMP Community String*

## configuration

|                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                  | <pre>configuration {   transfer-interval interval;   transfer-on-commit;   archive-sites {     file://&lt;path&gt;/&lt;filename&gt;;     ftp://username@host:&lt;port&gt;url-path password password;     http://username@host:&lt;port&gt;url-path password password;     pasvftp://username@host:&lt;port&gt;url-path password password;     scp://username@host:&lt;port&gt;url-path password password;   } }</pre> |
| <b>Hierarchy Level</b>                                                                                                                                                                         | [edit system archival]                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>                                                                                                                                                                     | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>                                                                                                                    |
| <b>Description</b>                                                                                                                                                                             | Configure the router or switch to periodically transfer its currently active configuration (or after each commit).                                                                                                                                                                                                                                                                                                    |
| <div>  <p><b>NOTE:</b> The [edit system archival] hierarchy is not available on QFabric systems.</p> </div> |                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                                                                                                                                                                                 | The remaining statements are explained separately.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b>                                                                                                                                                                | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>                                                                                                                                                                   | <ul style="list-style-type: none"> <li>• <i>Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site</i></li> <li>• <i>archive</i></li> <li>• <a href="#">archive-sites on page 240</a></li> <li>• <a href="#">transfer-interval on page 327</a></li> <li>• <a href="#">transfer-on-commit on page 328</a></li> </ul>                                                          |

## connection-limit

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



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

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

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

## contact

|                                 |                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>contact <i>contact</i>;</code>                                                                                                          |
| <b>Hierarchy Level</b>          | <code>[edit snmp]</code>                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Define the value of the MIB II <b>sysContact</b> object, which is the contact person for the managed system.                                  |
| <b>Options</b>                  | <b>contact</b> —Name of the contact person. If the name includes spaces, enclose it in quotation marks (" ").                                 |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Configuring the System Contact on a Device Running Junos OS</i></li> </ul>                        |

## disable (802.1X)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>disable;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | <code>[edit protocols <b>dot1x authenticator</b> interface (all   [<i>interface-names</i>])]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Disable 802.1X authentication on a specified interface or all interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Default</b>                  | 802.1X authentication is disabled on all interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show dot1x on page 340</a></li> <li>• <a href="#">Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31</a></li> <li>• <a href="#">Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 61</a></li> <li>• <a href="#">Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch</a></li> <li>• <a href="#">Example: Configuring Static MAC Bypass of Authentication on a Switch on page 95</a></li> <li>• <a href="#">Configuring 802.1X Interface Settings (CLI Procedure) on page 22</a></li> <li>• <a href="#">Configuring 802.1X Authentication (J-Web Procedure)</a></li> </ul> |

## disable (LLDP)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | disable;                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">lldp</a> ],<br>[edit protocols <a href="#">interface lldp</a> ]                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                        |
| <b>Description</b>              | Disable the LLDP configuration on the switch or on one or more interfaces.                                                                                                                                                                                                                                                                        |
| <b>Default</b>                  | If you do not configure LLDP, it is disabled on the switch and on specific switch interfaces.                                                                                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show lldp on page 353</a></li><li>• <a href="#">Configuring LLDP (CLI Procedure) on page 104</a></li><li>• <a href="#">Understanding 802.1X and LLDP and LLDP-MED on page 101</a></li><li>• <a href="#">Configuring LLDP</a></li><li>• <a href="#">Understanding LLDP on page 5</a></li></ul> |

## dot1x

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> dot1x {   authenticator {     authentication-profile-name <i>access-profile-name</i>;     interface (all   [ <i>interface-names</i> ]) {       disable;       guest-vlan (<i>vlan-id</i>   <i>vlan-name</i>);       lldp-med-bypass;       mac-radius &lt;restrict&gt;;       maximum-requests <i>number</i>;       no-reauthentication;       quiet-period <i>seconds</i>;       reauthentication {         interval <i>seconds</i>;       }       retries <i>number</i>;       server-fail (deny   permit   use-cache   <i>vlan-id</i>   <i>vlan-name</i>);       server-reject-vlan (<i>vlan-id</i>   <i>vlan-name</i>) {         eapol-block;         block-interval <i>block-interval</i>;       }       server-timeout <i>seconds</i>;       supplicant (single   single-secure   multiple);       supplicant-timeout <i>seconds</i>;       transmit-period <i>seconds</i>;     }     no-mac-table-binding;     static <i>mac-address</i> {       interface <i>interface-names</i>;       vlan-assignment (<i>vlan-id</i>   <i>vlan-name</i>);     }   } } </pre> |
| <b>Hierarchy Level</b>          | [edit protocols]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | <p>Configure 802.1X authentication for Port-Based Network Access Control. 802.1X authentication is supported on interfaces that are members of private VLANs (PVLANS).</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Default</b>                  | 802.1X is disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show dot1x on page 340</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

- [Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31](#)
- [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 61](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
- [Example: Configuring Static MAC Bypass of Authentication on a Switch on page 95](#)
- [Example: Configuring MAC RADIUS Authentication on a Switch on page 82](#)
- [Configuring Server Fail Fallback \(CLI Procedure\) on page 30](#)

---

## eapol-block

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | eapol-block;                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">dot1x authenticator interface (802.1X)</a> (all   [ <i>interface-names</i> ]) server-reject-vlan],<br>[edit protocols dot1x authenticator interface (all   [ <i>interface-names</i> ]) server-reject-vlan ( <i>vlan-id</i>   <i>vlan-name</i> )]                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                                                                                          |
| <b>Description</b>              | Enable an EAPoL block that causes the 802.1X interface to ignore Extensible Authentication Protocol (EAP) start messages from the client, which are attempts to restart the authentication procedure. When the 802.1X interface ignores the EAP start messages from the client, the switch allows the existing session that was established through the server-reject VLAN to remain open. |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">block-interval on page 245</a></li><li>• <a href="#">Example: Configuring Fallback Options on Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 69</a></li></ul>                                                                                                                                                 |

## falling-threshold (Health Monitor)

---

|                                 |                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>falling-threshold <i>percentage</i>;</code>                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | <code>[edit snmp health-monitor]</code>                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                          |
| <b>Description</b>              | Set the lower threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored variable, you can be alerted whenever the value of the variable falls outside the allowable operational range. |
| <b>Options</b>                  | <b><i>percentage</i></b> —Lower threshold for the alarm entry.<br><b>Range:</b> 1 through 100<br><b>Default:</b> 70 percent of the maximum possible value                                                                                                              |
| <b>Required Privilege Level</b> | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">rising-threshold on page 304</a></li> <li>• <i>Configuring Health Monitoring</i></li> </ul>                                                                                                                       |

## filter-duplicates

---

|                                 |                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>filter-duplicates;</code>                                                                                                                                       |
| <b>Hierarchy Level</b>          | <code>[edit snmp]</code>                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                         |
| <b>Description</b>              | Filter duplicate <b>Get</b> , <b>GetNext</b> , or <b>GetBulk</b> SNMP requests.                                                                                       |
| <b>Required Privilege Level</b> | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Understanding the Implementation of SNMP on the QFabric System</i></li> <li>• <i>Example: Configuring SNMP</i></li> </ul> |

## full-name

---

|                                 |                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>full-name <i>complete-name</i>;</code>                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit system login user]                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Configure the complete name of a user.                                                                                                                                                                                                                                          |
| <b>Options</b>                  | <b><i>complete-name</i></b> —Full name of the user. If the name contains spaces, enclose it in quotation marks.                                                                                                                                                                 |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Configuring Junos OS User Accounts</i></li><li>• <i>user</i></li><li>• <a href="#">user on page 331</a></li></ul>                                                                                                                    |

## guest-vlan

---

|                                 |                                                                                                                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>guest-vlan (<i>vlan-id</i>   <i>vlan-name</i>);</code>                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit protocols <b>dot1x authenticator interface</b> (all   [ <i>interface-names</i> ])]                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                               |
| <b>Description</b>              | Specify the VLAN to which an interface is moved when no 802.1X supplicants are connected on the interface. The VLAN specified must already exist on the switch.                                                                                                                |
| <b>Default</b>                  | None                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <b><i>vlan-id</i></b> —VLAN tag identifier of the guest VLAN.<br><br><b><i>vlan-name</i></b> —Name of the guest VLAN.                                                                                                                                                          |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 61</a></li><li>• <a href="#">Understanding Guest VLANs for 802.1X on Switches on page 60</a></li></ul> |

---

## health-monitor

---

|                                 |                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | health-monitor {<br>falling-threshold <i>percentage</i> ;<br>interval <i>seconds</i> ;<br>rising-threshold <i>percentage</i> ;<br>}           |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Configure health monitoring.<br><br>The remaining statements are explained separately.                                                        |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Configuring Health Monitoring</i></li><li>• <i>Understanding Health Monitoring</i></li></ul>       |

## hold-multiplier

---

|                                 |                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>hold-multiplier <i>number</i>;</code>                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">lldp</a> ]                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for QFX Series.                                                                                                                            |
| <b>Description</b>              | Specify the multiplier used in combination with the <a href="#">advertisement-interval</a> value to determine the length of time LLDP information is held before it is discarded. The default value is 4 (or 120 seconds).                                                                                                                        |
| <b>Default</b>                  | Disabled.                                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                  | <b><i>number</i></b> —A number used as a multiplier.<br><b>Range:</b> 2 through 10<br><b>Default:</b> 4 (or 120 seconds)                                                                                                                                                                                                                          |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show lldp on page 353</a></li><li>• <a href="#">Configuring LLDP (CLI Procedure) on page 104</a></li><li>• <a href="#">Understanding 802.1X and LLDP and LLDP-MED on page 101</a></li><li>• <a href="#">Configuring LLDP</a></li><li>• <a href="#">Understanding LLDP on page 5</a></li></ul> |

## idle-timeout (Access)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>idle-timeout seconds;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>     | <code>[edit access group-profile <i>profile-name</i> ppp],</code><br><code>[edit access profile <i>profile-name</i> client <i>client-name</i> ppp]</code>                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                                                                                                           |
| <b>Description</b>         | Configure the idle timeout for a user. The router might consider a PPP session to be idle because of the following reasons: <ul style="list-style-type: none"> <li>• There is no ingress traffic on the PPP session.</li> <li>• There is no egress traffic.</li> <li>• There is neither ingress or egress traffic on the PPP session.</li> <li>• There is no ingress or egress PPP control traffic. This is applicable only if keepalives are enabled.</li> </ul> |
| <b>Options</b>             | <b>seconds</b> —Number of seconds a user can remain idle before the session is terminated.<br><b>Range:</b> 0 through 4,294,967,295 seconds<br><b>Default:</b> 0                                                                                                                                                                                                                                                                                                  |



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

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


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

## interface (802.1X)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> interface (all   [ <i>interface-names</i> ]) {   disable;   guest-vlan (<i>vlan-name</i>   <i>vlan-id</i>);   lldp-med-bypass;   mac-radius &lt;restrict&gt;;   maximum-requests <i>number</i>;   no-reauthentication;   quiet-period <i>seconds</i>;   reauthentication {     interval <i>seconds</i>;   }   retries <i>number</i>;   server-fail (deny   permit   use-cache   <i>vlan-id</i>   <i>vlan-name</i>);   server-reject-vlan (<i>vlan-id</i>   <i>vlan-name</i>) {     eapol-block;     block-interval <i>block-interval</i>;   }   server-timeout <i>seconds</i>;   supplicant (single   single-secure   multiple);   supplicant-timeout <i>seconds</i>;   transmit-period <i>seconds</i>; } </pre> |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">dot1x authenticator</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Configure 802.1X authentication for Port-Based Network Access Control for all interfaces or for specific interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <p><b>all</b>—Configure all interfaces for 802.1X authentication.</p> <p>[ <i>interface-names</i> ]— List of names of interfaces to configure for 802.1X authentication.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show dot1x on page 340</a></li> <li>• <a href="#">Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31</a></li> <li>• <a href="#">Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 61</a></li> <li>• <a href="#">Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch</a></li> <li>• <a href="#">Example: Configuring MAC RADIUS Authentication on a Switch on page 82</a></li> </ul>                                                                                                                             |

- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 22](#)
- *Configuring 802.1X Authentication (J-Web Procedure)*

## interface (LLDP)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>interface (all   <i>interface-name</i>) {     disable;     power-negotiation {         disable;     } }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">lldp</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Configure Link Layer Discovery Protocol (LLDP) on all interfaces or on a specific interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                                 | <div>  <p><b>NOTE:</b> On EX4300 switches, LLDP cannot be configured on the me0 or vme interface. Issuing the command <code>set protocols lldp interface me0</code> generates the following error message:</p> <pre>error: name: 'me0': Invalid interface error: statement creation failed: interface</pre> <p>Issuing the command <code>set protocols lldp interface vme</code> generates the following error message:</p> <pre>error: name: 'vme': Invalid interface error: statement creation failed: interface</pre> </div> |
| <b>Default</b>                  | None                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <p><b>all</b>—All interfaces on the switch.</p> <p><b><i>interface-name</i></b>—Name of a specific interface.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring LLDP (CLI Procedure) on page 104</a></li> <li>• <a href="#">Understanding 802.1X and LLDP and LLDP-MED on page 101</a></li> <li>• <a href="#">Configuring LLDP</a></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul>                                                                                                                                                                                                                                                                                                           |

## interface (Static MAC Bypass)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>interface [interface-names];</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit protocols <b>dot1x authenticator</b> authentication-profile-name <b>static mac-address</b> ],<br>[edit ethernet-switching-options authentication-whitelist <i>mac-address</i> ],<br>[edit switch-options authentication-whitelist <i>mac-address</i> ]                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement added to the <b>[edit ethernet-switching-options authentication-whitelist]</b> hierarchy in Junos OS Release 10.1 for EX Series switches.<br>Statement added to the <b>[edit switch-options authentication-whitelist]</b> hierarchy in Junos OS Release 13.2X50-D10 for EX Series switches (ELS).<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                       |
| <b>Description</b>              | Configure interfaces on which the specified MAC addresses are allowed to bypass RADIUS authentication and allowed to connect to the LAN without authentication.                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                  | <i>interface-names</i> —List of interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show dot1x static-mac-address on page 347</a></li> <li>• <a href="#">Example: Configuring Static MAC Bypass of Authentication on a Switch on page 95</a></li> <li>• <a href="#">Example: Setting Up Captive Portal Authentication on an EX Series Switch</a></li> <li>• <a href="#">Example: Setting Up Captive Portal Authentication on an EX Series Switch</a></li> <li>• <a href="#">Configuring Captive Portal Authentication (CLI Procedure)</a></li> </ul> |

## interval (Health Monitor)

---

|                                 |                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | interval <i>seconds</i> ;                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit snmp health-monitor]                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Configure the interval between sampling of the object being monitored by the health monitor.                                                  |
| <b>Options</b>                  | <b>seconds</b> —Time between samples, in seconds.<br><b>Range:</b> 1 through 2147483647 seconds<br><b>Default:</b> 300 seconds                |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Configuring Health Monitoring</i></li></ul>                                                        |

## lldp

```
Syntax lldp {
 advertisement-interval seconds;
 disable;
 hold-multiplier number;
 interface (all | [interface-name]) {
 disable;
 power-negotiation {
 disable;
 }
 }
 lldp-configuration-notification-interval seconds;
 management-address ip-management-address;
 netbios-snooping;
 no-tagging;
 ptopo-configuration-maximum-hold-time seconds;
 ptopo-configuration-trap-interval seconds;
 traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable>
 <no-stamp> <replace>;
 flag flag <disable>;
 }
 transmit-delay seconds;
}
```

**Hierarchy Level** [edit protocols]

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

**Description** Configure Link Layer Discovery Protocol (LLDP). The switch uses LLDP to advertise its identity and capabilities on a LAN, as well as to receive information about other network devices. LLDP is defined in the IEEE standard 802.1AB-2005.

The remaining statements are explained separately.



**NOTE:** The `transmit-delay` and `netbios-snooping` options are not available on QFabric systems.



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

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

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

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

---

**Default** LLDP is enabled.

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

**Related Documentation**

- [show lldp on page 353](#)
- [Configuring LLDP \(CLI Procedure\) on page 104](#)
- [Configuring LLDP](#)
- [Understanding LLDP on page 5](#)
- [Understanding 802.1X and LLDP and LLDP-MED on page 101](#)

## lldp-med (Ethernet Switching)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> lldp-med {   disable;   fast-start <i>number</i>;   interface (all   <i>interface-name</i>) {     disable;     location {       elin <i>number</i>;       civic-based {         what <i>number</i>;         country-code <i>code</i>;         ca-type {           <i>number</i> {             ca-value <i>value</i>;           }         }       }     }   } } </pre>                                                       |
| <b>Hierarchy Level</b>          | [edit protocols]                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.</p>                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | <p>Configure Link Layer Discovery Protocol—Media Endpoint Discovery. LLDP-MED is an extension of LLDP. The switch uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations for emergency services. LLDP-MED is defined in the standard ANSI/TIA-1057 by the Telecommunications Industry Association (TIA).</p> <p>The statements are explained separately.</p> |
| <b>Default</b>                  | Disabled.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show lldp on page 353</a></li> <li>• <a href="#">Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch</a></li> <li>• <a href="#">Configuring LLDP-MED (CLI Procedure) on page 107</a></li> </ul>                                                                                                                                                         |

## lldp-med-bypass

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | lldp-med-bypass;                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">dot1x authenticator interface</a> (all   <i>interface-name</i> )]                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                                                                                       |
| <b>Description</b>              | Bypass the 802.1X authentication procedure for connecting multiple LLDP-MED end devices. Automatically add the learned MAC addresses of the end devices to the switch's static MAC bypass list, and allow the devices to access the network. You can enable <b>lldp-med-bypass</b> only when the interface is also configured for 802.1X authentication of <i>multiple</i> supplicants. |
| <b>Default</b>                  | Disabled                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">supplicant on page 315</a></li><li>• <i>Understanding Authentication on Switches</i></li></ul>                                                                                                                                                                                                                                      |

## lldp-configuration-notification-interval

---

|                                 |                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | lldp-configuration-notification-interval <i>seconds</i> ;                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">lldp</a> ]                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.6 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Specify how often SNMP trap notifications are generated as a result of LLDP database changes. If the interval value is 0, trap notifications of database changes are disabled.                                             |
| <b>Default</b>                  | SNMP trap notifications of LLDP database changes are disabled.                                                                                                                                                             |
| <b>Options</b>                  | <b>seconds</b> —Interval between trap notifications about LLDP database changes.<br><b>Range:</b> 0 through 3600                                                                                                           |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show lldp on page 353</a></li></ul>                                                                                                                                    |

---

## location

---


|                                 |                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>location <i>location</i>;</code>                                                                                                        |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Define the value of the MIB II <b>sysLocation</b> object, which is the physical location of the managed system.                               |
| <b>Options</b>                  | <i>location</i> —Location of the local system. You must enclose the name within quotation marks (" ").                                        |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Configuring the System Location for a Device Running Junos OS</i></li></ul>                        |

## mac-radius

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>mac-radius &lt;flap-on-disconnect&gt; &lt;restrict&gt;;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">dot1x</a> authenticator interface <i>interface-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Option <b>flap-on-disconnect</b> introduced in Junos OS Release 9.4 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | <p>Configure MAC RADIUS authentication for specific interfaces. MAC RADIUS authentication allows LAN access to permitted MAC addresses. When a new MAC address appears on an interface, the switch consults the RADIUS server to check whether the MAC address is a permitted address. If the MAC address is configured on the RADIUS server, the device is allowed access to the LAN.</p> <p>If MAC RADIUS is configured, the switch first tries to get a response from the host for 802.1X authentication. If the host is unresponsive, the switch attempts to authenticate using MAC RADIUS.</p> <p>To restrict authentication to MAC RADIUS only, use the <b>restrict</b> option. In restrictive mode, all 802.1X packets are eliminated and the attached device on the interface is considered a nonresponsive host.</p> |
| <b>Options</b>                  | <p><b>flap-on-disconnect</b>—(Optional) When the RADIUS server sends a disconnect message to a supplicant, the switch resets the interface on which the supplicant is authenticated. If the interface is configured for multiple supplicant mode, the switch resets all the supplicants on the specified interface. This option takes effect only when the <b>restrict</b> option is also set.</p> <p><b>restrict</b>—(Optional) Restricts authentication to MAC RADIUS only. When <b>mac-radius restrict</b> is configured the switch drops all 802.1X packets. This option is useful when no other 802.1X authentication methods, such as guest VLAN, are needed on the interface, and eliminates the delay that occurs while the switch determines that a connected device is a non-802.1X-enabled host.</p>               |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show dot1x on page 340</a></li><li>• <a href="#">Example: Configuring MAC RADIUS Authentication on a Switch on page 82</a></li><li>• <a href="#">Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31</a></li><li>• <a href="#">Configuring MAC RADIUS Authentication (CLI Procedure) on page 77</a></li><li>• <a href="#">Configuring 802.1X Interface Settings (CLI Procedure) on page 22</a></li><li>• <a href="#">Understanding Authentication on Switches</a></li></ul>                                                                                                                                                                                                                                     |

## management-address

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <code>management-address <i>ip-management-address</i>;</code>                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                              | [edit protocols <a href="#">lldp</a> ]                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Statement introduced in Junos OS Release 9.5 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.                                                                                                                                                                        |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Specify the management address of the switch to be used in the LLDP Management type, length, and value (TLV). The Management Address TLV typically contains the IPv4 or IPv6 management address of the local system. Only out-of-band management addresses must be used for the management-address. Other remote managers can use this address to obtain information related to the local device. |
| <div>  <p><b>NOTE:</b> Ensure that the interface with the configured management address has LLDP enabled using the <code>set protocols lldp interface</code> command. If you configure a customized management address for LLDP on an interface that has LLDP disabled, the <code>show lldp local-information</code> command output will not display the correct interface information.</p> </div> |                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Default</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | The LLDP Management Address TLV uses the IP address of the switch's management Ethernet interface ( <b>me0</b> ), or the IP address of the virtual management Ethernet (VME) interface if the switch is a Virtual Chassis member.                                                                                                                                                                 |
| <b>Options</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <i>ip-management-address</i> —You can specify either an IPv4 or an IPv6 management address for the switch.                                                                                                                                                                                                                                                                                        |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                     | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• <a href="#">show lldp on page 353</a></li> <li>• <a href="#">Understanding 802.1X and LLDP and LLDP-MED on page 101</a></li> <li>• <a href="#">EX Series Switches Interfaces Overview</a></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul>                                                                                             |

## maximum-requests

---

|                                 |                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | maximum-requests <i>number</i> ;                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit protocols dot1x authenticator interface (all   [ <i>interface-names</i> ])]                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                 |
| <b>Description</b>              | For 802.1X authentication, configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out.                                         |
| <b>Default</b>                  | Two retransmission attempts                                                                                                                                                                                      |
| <b>Options</b>                  | <i>number</i> —Number of retransmission attempts.<br><b>Range:</b> 1 through 10<br><b>Default:</b> 2                                                                                                             |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring 802.1X Interface Settings (CLI Procedure) on page 22</a></li><li>• <a href="#">Configuring 802.1X Authentication (J-Web Procedure)</a></li></ul> |

## name

---

|                                 |                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | name <i>name</i> ;                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Set the system name from the command-line interface.                                                                                          |
| <b>Options</b>                  | <i>name</i> —System name override.                                                                                                            |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the System Name</a></li></ul>                                                 |

## nas-ip-address

---

|                                 |                                                                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>nas-ip-address ip-address;</code>                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | <code>[edit system]</code>                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.3.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Configure the NAS-IP address for outgoing RADIUS packets.                                                                                                                                                                                                                   |
| <b>Options</b>                  | <code>ip-address</code> —IP address of the network access server (NAS) that requests user authentication.                                                                                                                                                                   |
| <b>Required Privilege Level</b> | <code>system</code> —To view this statement in the configuration.<br><code>system-control</code> —To add this statement to the configuration.                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring RADIUS Authentication</a></li> <li>• <a href="#">Configuring RADIUS Authentication (QFX Series or OCX Series) on page 192</a></li> </ul>                                                                   |

## no-mac-table-binding (802.1X)

---

|                                 |                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>no-mac-table-binding;</code>                                                                                                                                 |
| <b>Hierarchy Level</b>          | <code>[edit protocols dot1x authenticator]</code>                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                  |
| <b>Description</b>              | For 802.1X authentication, disable the removal of the session from the authentication session table when the MAC address ages out of the Ethernet switching table. |
| <b>Default</b>                  | Not enabled                                                                                                                                                        |
| <b>Required Privilege Level</b> | <code>routing</code> —To view this statement in the configuration.<br><code>routing-control</code> —To add this statement to the configuration.                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Controlling Authentication Session Timeouts (CLI Procedure) on page 74</a></li> </ul>                         |

## nonvolatile

---

|                                 |                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>nonvolatile {<br/>    <a href="#">commit-delay</a> <i>seconds</i>;<br/>}</code>                                                         |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Configure options for SNMP <b>Set</b> requests.<br><br>The statement is explained separately.                                                 |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Configuring the Commit Delay Timer</i></li><li>• <i>commit-delay</i></li></ul>                     |

## no-reauthentication

---

|                                 |                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>no-reauthentication;</code>                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">dot1x authenticator interface (802.1X)</a> (all   [ <i>interface-names</i> ])]                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                  |
| <b>Description</b>              | For 802.1X authentication, disables reauthentication.                                                                                                                                                                                                             |
| <b>Default</b>                  | Not disabled                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring 802.1X Interface Settings (CLI Procedure) on page 22</a></li><li>• <i>Configuring 802.1X Authentication (J-Web Procedure)</i></li><li>• <i>Understanding Authentication on Switches</i></li></ul> |

---


## oid

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>oid <i>object-identifier</i> (exclude  include);</code>                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | <code>[edit snmp view <i>view-name</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Specify an object identifier (OID) used to represent a subtree of MIB objects.                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <b>exclude</b> —Exclude the subtree of MIB objects represented by the specified OID.<br><b>include</b> —Include the subtree of MIB objects represented by the specified OID.<br><b><i>object-identifier</i></b> —OID used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name. |
| <b>Required Privilege Level</b> | <b>snmp</b> —To view this statement in the configuration.<br><b>snmp-control</b> —To add this statement to the configuration.                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Configuring MIB Views</i></li></ul>                                                                                                                                                                                                                                                                                                                                                           |

## order

---

|                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                            | <code>order (radius   [ <i>accounting-order-data-list</i> ] );</code>                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>                                                                                                                                                                   | [edit access profile <i>profile-name</i> accounting]                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>                                                                                                                                                               | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.                                                                                              |
| <b>Description</b>                                                                                                                                                                       | Configure the order of authentication, authorization, and accounting (AAA) servers to use while sending accounting messages and updates.                                                                                                                                                                                |
| <b>Default</b>                                                                                                                                                                           | No order specified                                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                                                                                                                                                                           | <b>radius</b> —RADIUS accounting for specified subscribers.<br><br>[ <i>accounting-order-data-list</i> ]— Set of data listing the authentication order to be used, enclosed by brackets. This can be any combination of the authentication methods, up to and including a full list of the entire authentication order. |
| <hr/> <div> <b>NOTE:</b> The [edit access] hierarchy is not available on QFabric systems.</div> <hr/> |                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b>                                                                                                                                                          | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                         |
| <b>Related Documentation</b>                                                                                                                                                             | <ul style="list-style-type: none"><li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25</a></li><li>• <a href="#">Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 67</a></li><li>• <a href="#">Configuring RADIUS Accounting</a></li></ul>                               |

## port (RADIUS Server)


|                            |                                                                                                                                                                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>port <i>port-number</i>;</code>                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>     | [edit system radius-server <i>address</i> ],<br>[edit system accounting destination radius server <i>address</i> ]                                                                                                                                                              |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>         | Configure the port number on which to contact the RADIUS server.                                                                                                                                                                                                                |
| <b>Options</b>             | <i>number</i> —Port number on which to contact the RADIUS server.<br><b>Default:</b> 1812 (as specified in RFC 2865)                                                                                                                                                            |



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

|                                 |                                                                                                                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring RADIUS Authentication</a></li> <li>• <a href="#">Configuring RADIUS Authentication (QFX Series or OCX Series) on page 192</a></li> </ul> |

## profile

|                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                  | <pre> profile <i>profile-name</i> {     accounting (Access Profile) {         accounting-stop-on-access-deny;         accounting-stop-on-failure;         order ( radius   [ <i>accounting-order-data-list</i> ] );     }     authentication-order [<i>authentication-method</i>];     radius {         accounting-server [<i>server-addresses</i>];         authentication-server [<i>server-addresses</i>];     } } </pre> |
| <b>Hierarchy Level</b>                                                                                                                                                         | [edit access]                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>                                                                                                                                                     | <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>                                                                                                                                                                                    |
| <b>Description</b>                                                                                                                                                             | Configure an access profile. The access profile contains the entire authentication, authorization, and accounting (AAA) configuration that aids in handling AAA requests, including the authentication method and order, AAA server addresses, and AAA accounting.                                                                                                                                                           |
| <b>Default</b>                                                                                                                                                                 | Not enabled                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Options</b>                                                                                                                                                                 | <p><b><i>profile-name</i></b>—Profile name of up to 32 characters.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                             |
| <div>  <b>NOTE:</b> The [edit access] hierarchy is not available on QFabric systems. </div> |                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Required Privilege Level</b>                                                                                                                                                | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>                                                                                                                                                   | <ul style="list-style-type: none"> <li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25</a></li> <li>• <a href="#">Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 67</a></li> <li>• <a href="#">Configuring RADIUS Accounting</a></li> </ul>                                                                                                                                |

## protocols

```

Syntax protocols {
 bgp {
 disable;
 accept-remote-nexthop;
 advertise-external <conditional>;
 advertise-inactive;
 (advertise-peer-as | no-advertise-peer-as);
 authentication-algorithm (aes-128-cmac-96 | hmac-sha-1-96 | md5);
 authentication-key key;
 authentication-key-chain key-chain;
 bfd-liveness-detection {
 authentication {
 algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
 meticulous-keyed-sha-1 | simple-password);
 key-chain key-chain-name;
 loose-check;
 }
 detection-time {
 threshold milliseconds;
 }
 hold-down-interval milliseconds;
 minimum-interval milliseconds;
 minimum-receive-interval milliseconds;
 multiplier number;
 no-adaptation;
 session-mode (automatic | multihop | single-hop);
 transmit-interval {
 minimum-interval milliseconds;
 threshold milliseconds;
 }
 version (1 | automatic);
 }
 cluster cluster-identifier;
 damping;
 description text-description;
 export [policy-names];
 family family-name {
 ... the family subhierarchies appear after the main [edit protocols bgp] hierarchy ...
 }
 graceful-restart {
 disable;
 restart-time seconds;
 stale-routes-time seconds;
 }
 group group-name {
 ... the group subhierarchy appears after the main [edit protocols bgp] hierarchy ...
 }
 hold-time seconds;
 import [policy-names];
 include-mp-next-hop;
 keep (all | none);
 local-address address;
 }
}

```

```

local-as autonomous-system <loops number> <alias> <private>;
local-preference local-preference;
log-updown;
metric-out (metric | igp (delay-med-update | offset) | minimum-igp offset);
mtu-discovery;
multihop {
 no-nexthop-change;
 ttl ttl-value;
}
no-aggregator-id;
no-client-reflect;
out-delay seconds;
outbound-route-filter {
 bgp-orf-cisco-mode;
 prefix-based {
 accept {
 inet;
 inet6;
 }
 }
}
passive;
path-selection {
 always-compare-med;
 as-path-ignore;
 cisco-non-deterministic;
 external-router-id;
 med-plus-igp {
 igp-multiplier number;
 med-multiplier number;
 }
}
peer-as autonomous-system;
preference preference;
remove-private;
tcp-mss segment-size;
traceoptions {
 file filename <files number> <size maximum-file-size> <world-readable |
 no-world-readable>;
 flag flag <flag-modifier> <disable>;
}
}
dcbx {
 disable;
 interface (interface-name | all) {
 disable;
 application-map application-map-name;
 applications {
 no-auto-negotiation;
 }
 enhanced-transmission-selection {
 no-auto-negotiation;
 no-recommendation-tlv;
 recommendation-tlv {
 no-auto-negotiation;
 }
 }
 }
}

```

```

 }
 dcbx-version (auto-negotiate | ieee-dcbx | dcbx-version-1.01);
 priority-flow-control {
 no-auto-negotiation;
 }
}
}
iccp {
 authentication-key string;
 local-ip-addr local-ip-addr;
 peer ip-address {
 authentication-key string;
 backup-liveness-detection {
 backup-peer-ip ip-address;
 }
 liveness-detection {
 detection-time {
 threshold milliseconds;
 }
 minimum-interval milliseconds;
 minimum-receive-interval milliseconds;
 multiplier number;
 no-adaptation;
 transmit-interval {
 minimum-interval milliseconds;
 threshold milliseconds;
 }
 version (Liveness Detection) (1 | automatic);
 }
 local-ip-addr ipv4-address;
 session-establishment-hold-time seconds;
 }
 session-establishment-hold-time seconds;
 traceoptions {
 file <filename> <files number> <match regular-expression> <microsecond-stamp>
 <size size> <world-readable | no-world-readable>;
 flag flag;
 no-remote-trace;
 }
}
igmp-snooping {
 traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable> <match
 regex>;
 flag flag (detail | disable | receive | send);
 }
}
vlan vlan-name {
 disable;
}
interface interface-name {
 group-limit limit;
 multicast-router-interface;
 static {
 group ip-address;
 }
}
}

```

```

 robust-count number;
 }
}
isis {
 disable;
 export [policy-names];
 ignore-attached-bit;
 interface interface-name {
 bfd-liveness-detection {
 authentication {
 algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
 meticulous-keyed-sha-1 | simple-password);
 key-chain key-chain-name;
 loose-check;
 }
 detection-time {
 threshold milliseconds;
 }
 minimum-interval milliseconds;
 minimum-receive-interval milliseconds;
 multiplier number;
 no-adaptation;
 transmit-interval {
 minimum-interval milliseconds;
 threshold milliseconds;
 }
 }
 version (1 | automatic);
 }
 checksum;
 csnp-interval (seconds | disable);
 disable;
 hello-padding (adaptive | loose | strict);
 level (1 | 2) {
 disable;
 hello-authentication-key key;
 hello-authentication-type authentication;
 hello-interval seconds;
 hold-time seconds;
 ipv4-multicast-metric number;
 metric metric;
 passive;
 priority number;
 }
 lsp-interval milliseconds;
 mesh-group (value | blocked);
 no-ipv4-multicast;
 no-unicast-topology;
 passive;
 point-to-point;
}
level (1 | 2) {
 disable;
 authentication-key key;
 authentication-type authentication;
 external-preference preference;
 no-csnp-authentication;

```

```

 no-hello-authentication;
 no-psnp-authentication;
 preference preference;
 prefix-export-limit number;
 wide-metrics-only;
}
loose-authentication-check;
lsp-lifetime seconds;
max-areas number;
no-adjacency-holddown;
no-authentication-check;
no-ipv4-routing;
overload {
 advertise-high-metrics;
 timeout seconds;
}
reference-bandwidth reference-bandwidth;
rib-group {
 inet group-name;
}
topologies {
 ipv4-multicast;
}
traceoptions {
 file filename <files number> <size maximum-file-size> <world-readable |
 no-world-readable>;
 flag flag <flag-modifier> <disable>;
}
traffic-engineering {
 disable;
 family inet {
 shortcuts {
 multicast-rpf-routes:
 }
 }
}
}
lldp {
 disable;
 advertisement-interval seconds;
 hold-multiplier number;
 interface (LLDP) (all | interface-name) {
 disable;
 }
 traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable> <match
 regex>;
 flag flag (detail | disable | receive | send);
 }
}
mstp {
 disable;
 bpdu-timeout-action;
 bridge-priority priority;
 configuration-name (MSTP) name;
 forward-delay seconds;

```

```

hello-time seconds;
interface (all | interface-name) {
 disable;
 bpdu-timeout-action {
 block;
 alarm;
 }
 cost cost;
 edge;
 mode mode;
 no-root-port;
 priority priority;
}
max-age seconds;
max-hops hops;
msti msti-id {
 vlan (vlan-id | vlan-name);
 interface interface-name {
 disable;
 cost cost;
 edge;
 mode mode;
 priority priority;
 }
}
revision-level revision-level;
traceoptions {
 file filename <files number > <size size > <no-stamp | world-readable |
 no-world-readable>;
 flag flag;
}
}
ospf {
 disable;
 area area-id {
 area-range ip-prefix </prefix-length> <exact> <override-metric metric> <restrict>;
 context-identifier identifier
 interface interface-name {
 disable;
 authentication {
 md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
 simple-password key-string;
 }
 bandwidth-based-metrics {
 bandwidth value metric number;
 }
 bfd-liveness-detection {
 authentication {
 algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
 meticulous-keyed-sha-1 | simple-password);
 key-chain key-chain-name;
 loose-check;
 }
 detection-time {
 threshold milliseconds;
 }
 }
 }
 }
}

```

```

 full-neighbors-only;
 minimum-interval milliseconds;
 minimum-receive-interval milliseconds;
 multiplier number;
 no-adaptation;
 transmit-interval {
 minimum-interval milliseconds;
 threshold milliseconds;
 }
 version (1 | automatic);
}
dead-interval seconds;
dynamic-neighbors;
flood-reduction;
hello-interval seconds;
interface-type (nbma | p2mp | p2p);
metric metric;
neighbor address <eligible>;
no-eligible-backup;
no-interface-state-traps;
no-neighbor-down-notification;
passive {
 traffic-engineering {
 remote-node-id address;
 }
}
poll-interval seconds;
priority number;
retransmit-interval seconds;
secondary;
te-metric metric;
topology (name | default | ipv4-multicast) {
 disable;
 bandwidth-based-metrics {
 bandwidth value;
 metric number;
 }
 metric metric;
}
transit-delay seconds;
}
network-summary-export [policy-names];
network-summary-import [policy-names];
nssa {
 area-range ip-prefix </prefix-length> <exact> <override-metric metric> <restrict>;
 default-lsa {
 default-metric metric;
 metric-type type;
 type-7;
 }
}
(summaries | no-summaries);
}
stub <default-metric metric> <summaries | no-summaries>;
virtual-link neighbor-id router-id transit-area area-id {
 disable;
 authentication {

```

```

 md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
 simple-password key-string;
 }
 dead-interval seconds;
 demand-circuit;
 flood-reduction;
 hello-interval seconds;
 ipsec-sa sa-name;
 no-neighbor-down-notification;
 retransmit-interval seconds;
 topology (name | default | ipv4-multicast) {
 disable;
 metric metric;
 }
 transit-delay seconds;
}
}
database-protection {
 ignore-count number;
 ignore-time seconds;
 maximum-lsa number;
 reset-time seconds;
 warning-only;
 warning-threshold percent;
}
export [policy-names];
external-preference preference;
graceful-restart {
 disable;
 helper-disable <both | restart-signaling | standard>;
 no-strict-lsa-checking;
 notify-duration seconds;
 restart-duration seconds;
}
import [policy-names];
no-nssa-abr;
no-rfc-1583;
overload <timeout seconds>;
preference preference;
prefix-export-limit number;
reference-bandwidth reference-bandwidth;
rib-group group-name;
topology (default | ipv4-multicast | name) {
 overload;
 prefix-export-limit number;
 topology-id number;
}
}
traceoptions {
 file filename <files number> <size maximum-file-size> <world-readable |
 no-world-readable>;
 flag flag <flag-modifier> <disable>;
}
}
traffic-engineering {
 advertise-unnumbered-interfaces;
 credibility-protocol-preference;
 ignore-lsp-metrics;
}

```

```

 multicast-rpf-routes;
 no-topology;
 shortcuts <lsp-metric-into-summary>;
 }
}
pim {
 disable;
 assert-timeout seconds;
 dense-groups {
 addresses;
 }
 dr-election-on-p2p;
 export;
 family (inet | inet6) {
 disable;
 }
 graceful-restart {
 disable;
 restart-duration seconds;
 }
 import [policy-names];
 interface interface-name {
 accept-remote-source;
 disable;
 family (inet | inet6) {
 disable;
 }
 hello-interval seconds;
 mode (dense | sparse | sparse-dense);
 neighbor-policy [policy-names];
 override-interval milliseconds;
 priority number;
 propagation-delay milliseconds;
 reset-tracking-bit;
 version version;
 }
 join-load-balance;
 join-prune-timeout;
 nonstop-routing;
 override-interval milliseconds;
 propagation-delay milliseconds;
 reset-tracking-bit;
 rib-group group-name;
 rp {
 auto-rp {
 (announce | discovery | mapping);
 (mapping-agent-election | no-mapping-agent-election);
 }
 bootstrap {
 family (inet | inet6) {
 export [policy-names];
 import [policy-names];
 priority number;
 }
 }
 }
 bootstrap-import [policy-names];
}

```

```

bootstrap-export [policy-names];
bootstrap-priority number;
dr-register-policy [policy-names];
embedded-rp {
 group-ranges {
 destination-ip-prefix</prefix-length>;
 }
 maximum-rps limit;
}
local {
 family (inet | inet6) {
 address address;
 anycast-pim {
 disable;
 rp-set {
 address address <forward-msdp-sa>;
 }
 local-address address;
 }
 group-ranges {
 destination-ip-prefix</prefix-length>;
 }
 hold-time seconds;
 priority number;
 }
}
rp-register-policy [policy-names];
spt-threshold {
 infinity [policy-names];
}
static {
 address address {
 group-ranges {
 version version;
 destination-ip-prefix</prefix-length>;
 }
 }
}
}
rpf-selection {
 group group-address{
 source source-address{
 next-hop next-hop-address;
 }
 wildcard-source {
 next-hop next-hop-address;
 }
 }
 prefix-list prefix-list-addresses {
 source source-address {
 next-hop next-hop-address;
 }
 wildcard-source {
 next-hop next-hop-address;
 }
 }
}

```

```

traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable>;
 flag flag <flag-modifier> <disable>;
}
tunnel-devices [mt-fpc/pic/port];
}
rip {
 authentication-key password;
 authentication-type type;
 (check-zero | no-check-zero);
 group group-name {
 bfd-liveness-detection {
 authentication {
 algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
 meticulous-keyed-sha-1 | simple-password);
 key-chain key-chain-name;
 loose-check;
 }
 detection-time {
 threshold milliseconds;
 }
 minimum-interval milliseconds;
 minimum-receive-interval milliseconds;
 multiplier number;
 no-adaptation;
 transmit-interval {
 minimum-interval milliseconds;
 threshold milliseconds;
 }
 version (1 | automatic);
 }
 }
 export [policy-names];
 import [policy-names];
 metric-out metric;
 neighbor neighbor-name {
 any-sender;
 authentication-key password;
 authentication-type type;
 bfd-liveness-detection {
 ... same statements as at the [edit protocols rip group group-name
 bfd-liveness-detection] hierarchy level ...
 }
 (check-zero | no-check-zero);
 import [policy-names];
 message-size number;
 metric-in metric;
 receive (both | none | version-1 | version-2);
 route-timeout seconds;
 send (broadcast | multicast | none | version-1);
 update-interval seconds;
 }
 preference preference;
 route-timeout seconds;
 update-interval seconds;
}
holddown seconds;

```

```
import [policy-names];
message-size number;
metric-in metric;
receive (both | none | version-1 | version-2);
rib-group group-name;
route-timeout seconds;
send (broadcast | multicast | none | version-1);
traceoptions {
 file filename <files number> <size maximum-file-size> <world-readable |
 no-world-readable>;
 flag flag <flag-modifier> <disable>;
}
update-interval seconds;
}
rstp {
 disable;
 bpdu-block-on-edge;
 bridge-priority priority;
 forward-delay seconds;
 hello-time seconds;
 interface (all | interface-name) {
 disable;
 bpdu-timeout-action {
 alarm;
 block;
 }
 cost cost;
 edge;
 mode mode;
 no-root-port;
 priority priority;
 }
 max-age seconds;
}
traceoptions {
 file filename <files number> <size size> <no-stamp> <world-readable |
 no-world-readable>;
 flag flag;
}
}
stp {
 disable;
 bridge-priority priority;
 forward-delay seconds;
 hello-time seconds;
 interface (all | interface-name) {
 disable;
 bpdu-timeout-action {
 alarm;
 block;
 }
 cost cost;
 edge;
 mode mode;
 no-root-port;
 priority priority;
```

```

 }
 max-age seconds;
 }
 traceoptions {
 file filename <files number > <size size > <no-stamp | world-readable |
 no-world-readable>;
 flag flag;
 }
 uplink-failure-detection {
 group group-name {
 link-to-monitor interface-name;
 link-to-disable interface-name;
 }
 }
}
vstp {
 bpdu-block-on-edge;
 disable (Spanning Trees);
 force-version (Spanning Trees) stp;
 vlan (Spanning Trees) vlan-id {
 bridge-priority (Spanning Trees) priority;
 forward-delay (Spanning Trees) seconds;
 hello-time (Spanning Trees) seconds;
 interface (Spanning Trees) (all | interface-name) {
 bpdu-timeout-action (Spanning Trees) {
 block (Spanning Trees);
 log (Spanning Trees);
 }
 cost (Spanning Trees) cost;
 disable (Spanning Trees);
 edge (Spanning Trees);
 mode (Spanning Trees) mode;
 no-root-port (Spanning Trees);
 priority (Spanning Trees) priority;
 }
 max-age (Spanning Trees) seconds;
 traceoptions (Spanning Trees) {
 file filename <files number > <size size > <no-stamp | world-readable |
 no-world-readable>;
 flag flag;
 }
 }
}
}
}

```

|                                 |                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hierarchy Level</b>          | [edit]                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. |
| <b>Description</b>              | Configure protocols.<br><br>The remaining statements are explained separately.                                                                     |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                |

**Related Documentation**     • [Junos OS Routing Protocols Configuration Guide](#)

---

## protocol-version

---

|                                 |                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>protocol-version <i>version</i>;</code>                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit system services ssh]                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Specify the secure shell (SSH) protocol version.                                                                                                                                                                                                                           |
| <b>Default</b>                  | <b>v2</b> —SSH protocol version 2 is the default, introduced in Junos OS Release 11.4.                                                                                                                                                                                     |
| <b>Options</b>                  | <b><i>version</i></b> —SSH protocol version: <b>v1</b> , <b>v2</b> , or both.                                                                                                                                                                                              |
| <b>Required Privilege Level</b> | <b>admin</b> —To view this statement in the configuration.<br><b>admin-control</b> —To add this statement to the configuration.                                                                                                                                            |
| <b>Related Documentation</b>    | • <a href="#">Configuring SSH Service for Remote Access to the Router or Switch</a>                                                                                                                                                                                        |

## ptopo-configuration-maximum-hold-time

|                                 |                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>ptopo-configuration-maximum-hold-time <i>seconds</i>;</code>                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">lldp</a> ]                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.6 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.          |
| <b>Description</b>              | Configure how long to maintain the physical topology database entries. The physical topology identifies the devices on the network and their physical interconnections.                                                             |
| <b>Options</b>                  | <b><i>seconds</i></b> —Time to maintain physical topology database entries.<br><b>Default:</b> 300<br><b>Range:</b> 1 through 2147483647                                                                                            |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show lldp on page 353</a></li> <li>• <a href="#">Understanding 802.1X and LLDP and LLDP-MED on page 101</a></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul> |

## ptopo-configuration-trap-interval


|                                 |                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>ptopo-configuration-trap-interval <i>seconds</i>;</code>                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">lldp</a> ]                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.6 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Specify how often SNMP trap notifications are sent regarding changes in physical topology global statistics.                                                                                                               |
| <b>Default</b>                  | SNMP trap notifications of changes in physical topology global statistics are disabled.                                                                                                                                    |
| <b>Options</b>                  | <b><i>seconds</i></b> —Interval between SNMP trap notifications about physical topology global statistics.<br><b>Range:</b> 0 through 3600                                                                                 |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                        |

## quiet-period

---


|                                 |                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | quiet-period <i>seconds</i> ;                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit protocols <b>dot1x authenticator interface (802.1X)</b> (all   [ <i>interface-names</i> ])]                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                |
| <b>Description</b>              | For 802.1X authentication, configure the number of seconds the interface remains in the wait state following a failed authentication attempt by a supplicant before reattempting authentication.                                |
| <b>Default</b>                  | 60 seconds                                                                                                                                                                                                                      |
| <b>Options</b>                  | <b>seconds</b> —Number of seconds the interface remains in the wait state.<br><b>Range:</b> 0 through 65,535 seconds<br><b>Default:</b> 60 seconds                                                                              |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show network-access aaa statistics authentication on page 367</a></li><li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25</a></li></ul> |

## radius

|                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                 | <pre>radius {   accounting-server [server-addresses];   authentication-server [server-addresses]; }</pre>                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>                                                                                                                                                        | [edit access profile <i>profile-name</i> ]                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>                                                                                                                                                    | <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>                                                                                                                                                          |
| <b>Description</b>                                                                                                                                                            | <p>Configure the RADIUS servers for authentication and for accounting. To configure multiple RADIUS servers, include multiple <b>radius</b> statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.</p> <p>The statements are explained separately.</p>           |
| <div>  <b>NOTE:</b> The [edit access] hierarchy is not available on QFabric systems. </div> |                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b>                                                                                                                                               | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>                                                                                                                                                  | <ul style="list-style-type: none"> <li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25</a></li> <li>• <a href="#">Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 67</a></li> <li>• <a href="#">Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 40</a></li> <li>• <a href="#">Configuring RADIUS Accounting</a></li> </ul> |

## radius-options (edit system)

---


|                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                                                                                                                                                                                                | <pre>radius-options {<br/>  attributes {<br/>    nas-ip-address <i>ip-address</i>;<br/>  }<br/>  enhanced-accounting;<br/>  password-protocol <i>mschap-v2</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                   |
| Hierarchy Level                                                                                                                                                                                       | [edit system]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Release Information                                                                                                                                                                                   | <p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2.</p> <p>MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> |
| <hr/> <div> <b>NOTE:</b> The <code>radius-options</code> statement is not available on QFabric systems.</div> <hr/> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <p><b>enhanced-accounting</b> statement introduced in Junos OS Release 14.1.</p>                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Description                                                                                                                                                                                           | Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.                                                                                                                                                                                                                                                                                                                                                                                     |
| Options                                                                                                                                                                                               | <p><b>enhanced-accounting</b>—View the attribute values of a logged in user.</p> <p><b>nas-ip-address <i>ip-address</i></b>—IP address of the network access server (NAS) that requests user authentication.</p> <p><b>password-protocol <i>mschap-v2</i></b>—Protocol MS-CHAPv2, used for password authentication and password changing.</p>                                                                                                                                                                 |
| Required Privilege Level                                                                                                                                                                              | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                  |
| Related Documentation                                                                                                                                                                                 | <ul style="list-style-type: none"><li>• <i>Configuring MS-CHAPv2 for Password-Change Support</i></li><li>• <a href="#">Configuring RADIUS Authentication (QFX Series or OCX Series) on page 192</a></li><li>• <a href="#">Configuring RADIUS System Accounting on page 209</a></li><li>• <i>enhanced-accounting</i></li></ul>                                                                                                                                                                                 |

## radius-options (Protocols 802.1X)

|                                 |                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | radius-options {<br>use-vlan-id;<br>use-vlan-name;<br>}                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">dot1x authenticator</a> ]                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                        |
| <b>Description</b>              | Configure 802.1X authenticator so that the VLAN ID or VLAN name is included in the packet sent to the RADIUS server to request authentication.                                                                                                                                                                           |
| <b>Options</b>                  | <p><b>use-vlan-id</b>—Include the VLAN ID in the packet sent to the RADIUS server to request authentication.</p> <p><b>use-vlan-name</b>—Include the VLAN name in the packet sent to the RADIUS server to request authentication. The VLAN name is sent even if the 802.1X interface is configured with the VLAN ID.</p> |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring 802.1X Interface Settings (CLI Procedure) on page 22</a></li> <li>• <a href="#">Specifying RADIUS Server Connections on Switches (CLI Procedure) on page 24</a></li> <li>• <a href="#">authenticator on page 243</a></li> </ul>                         |

## radius-server

---

|                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                  | <pre>radius-server server-address {<br/>    accounting-port <i>port-number</i>;<br/>    port <i>number</i>;<br/>    retry <i>number</i>;<br/>    secret <i>password</i>;<br/>    source-address <i>source-address</i>;<br/>    timeout <i>seconds</i>;<br/>}</pre>                                                                                                                      |
| <b>Hierarchy Level</b>                                                                                                                                                                                         | [edit system]                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>                                                                                                                                                                                     | Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                                                                                      |
| <b>Description</b>                                                                                                                                                                                             | <p>Configure a RADIUS server for Point-to-Point Protocol (PPP).</p> <p>To configure multiple RADIUS servers, include multiple <b>radius-server</b> statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.</p>                                         |
| <b>Options</b>                                                                                                                                                                                                 | <p><b>server-address</b>—Address of the RADIUS authentication server.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                     |
| <div> <b>NOTE:</b> The <b>accounting-port</b> and <b>source-address</b> options are not available on QFabric systems.</div> |                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b>                                                                                                                                                                                | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>                                                                                                                                                                                   | <ul style="list-style-type: none"><li>• <a href="#">Configuring RADIUS Authentication (QFX Series or OCX Series) on page 192</a></li><li>• <a href="#">accounting-port</a></li><li>• <a href="#">port on page 277</a></li><li>• <a href="#">retry on page 303</a></li><li>• <a href="#">secret</a></li><li>• <a href="#">source-address</a></li><li>• <a href="#">timeout</a></li></ul> |

## rate-limit

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

## reauthentication

---

|                                 |                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>reauthentication <i>interval</i>;</code>                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">dot1x authenticator interface (802.1X)</a> (all   [ <i>interface-names</i> ])]                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.               |
| <b>Description</b>              | For 802.1X authentication, specify the number of seconds before an authentication session times out.                                                           |
| <b>Options</b>                  | <i>interval</i> —Sets the periodic reauthentication time interval in seconds.<br><b>Range:</b> 1 through 4,294,967,296 seconds<br><b>Default:</b> 3600 seconds |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring 802.1X Interface Settings (CLI Procedure) on page 22</a></li></ul>                             |

## remote-debug-permission

|                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | remote-debug-permission (qfabric-admin   qfabric-operator   qfabric-user);                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit system login user <i>username</i> authentication]<br>[edit system root-authentication]                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.3 for the QFX Series.                                                                                                                                                                                                                                     |
| <b>Description</b>              | (QFabric systems only) Configure authentication classes that permit or deny user access to individual components of the QFabric system.                                                                                                                                                                                                                                                |
| <b>Default</b>                  | qfabric-user                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <p><b>qfabric-admin</b>—Permits a user to log in to individual QFabric system components, view operations, and change component configurations.</p> <p><b>qfabric-operator</b>—Permits a user to log in to individual QFabric system components and view component operations.</p> <p><b>qfabric-user</b>—Prevents a user from logging in to individual QFabric system components.</p> |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Example: Configuring QFabric System Login Classes</i></li> <li>• <i>request component login</i></li> <li>• <i>Understanding QFabric System Login Classes</i></li> </ul>                                                                                                                                                                    |

## retries

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>retries <i>number</i>;</code>                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit protocols <code>dot1x authenticator interface (802.1X)</code> (all   [ <i>interface-names</i> ])]                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                                                               |
| <b>Description</b>              | For 802.1X authentication, configure the number of times the switch attempts to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt.                                                                                                                                     |
| <b>Options</b>                  | <i>number</i> —Number of retries.<br><b>Default:</b> 3 retries<br><b>Range:</b> 1 through 10                                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring 802.1X Interface Settings (CLI Procedure) on page 22</a></li><li>• <a href="#">Configuring 802.1X Authentication (J-Web Procedure)</a></li><li>• <a href="#">Example: Configuring Fallback Options on Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 69</a></li></ul> |

## retry

|                            |                                                                                                                                               |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>retry number;</code>                                                                                                                    |
| <b>Hierarchy Level</b>     | [edit system radius server <i>server-address</i> ],<br>[edit system accounting destination radius server <i>server-address</i> ]              |
| <b>Release Information</b> | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>         | Number of times the router or switch is allowed to try to contact a RADIUS authentication or accounting server.                               |
| <b>Options</b>             | <i>number</i> —Number of retries allowed for contacting a RADIUS server.<br><b>Range:</b> 1 through 10<br><b>Default:</b> 3                   |



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

|                                 |                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring RADIUS Authentication (QFX Series or OCX Series) on page 192</a></li> <li>• <a href="#">Configuring RADIUS Accounting</a></li> <li>• <a href="#">timeout</a></li> </ul> |

## rising-threshold (Health Monitor)

---

|                                 |                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>rising-threshold <i>percentage</i>;</code>                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | <code>[edit snmp health-monitor]</code>                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                        |
| <b>Description</b>              | Set the upper threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored object, you can be alerted whenever the value of the variable falls outside the allowable operational range. |
| <b>Options</b>                  | <b><i>percentage</i></b> —Upper threshold for the alarm entry.<br><b>Range:</b> 1 through 100<br><b>Default:</b> 80 percent of the maximum possible value                                                                                                            |
| <b>Required Privilege Level</b> | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Health Monitoring</a></li><li>• <a href="#">falling-threshold on page 255</a></li></ul>                                                                                                              |

## root-login

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | root-login (allow   deny   deny-password);                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit system services ssh]                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                  |
| <b>Description</b>              | Control user access through SSH.                                                                                                                                                                                                                                                                                                                                                 |
| <b>Default</b>                  | Allow user access through SSH.                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <p><b>allow</b>—Allow users to log in to the router or switch as root through SSH.</p> <p><b>deny</b>—Disable users from logging in to the router or switch as root through SSH.</p> <p><b>deny-password</b>—Allow users to log in to the router or switch as root through SSH when the authentication method (for example, RSA authentication) does not require a password.</p> |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><i>Configuring SSH Service for Remote Access to the Router or Switch</i></li> </ul>                                                                                                                                                                                                                                                       |

## server-fail

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>server-fail (deny   permit   use-cache   <i>vlan-id</i>   <i>vlan-name</i>);</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit protocols <b>dot1x authenticator interface (802.1X)</b> (all   [ <i>interface-names</i> ])]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | <p>For EX Series switches configured for 802.1X authentication, specify the server fail fallback action the switch takes when all RADIUS authentication servers are unreachable.</p> <p>When you specify the action <i>vlan-name</i> or <i>vlan-id</i>, the VLAN must already be configured on the switch.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Default</b>                  | Authentication is denied.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <p><b>deny</b>—Force fail the supplicant authentication. No traffic will flow through the interface.</p> <p><b>permit</b>—Force succeed the supplicant authentication. Traffic will flow through the interface as if it were successfully authenticated by the RADIUS server.</p> <p><b>use-cache</b>—Force succeed the supplicant authentication only if it was previously authenticated successfully. This action ensures that already authenticated supplicants are not affected.</p> <p><b>vlan-id</b>—Move supplicant on the interface to the VLAN specified by this numeric identifier. This action is allowed only if it is the first supplicant connecting to the interface. If an authenticated supplicant is already connected, then the supplicant is not moved to the VLAN and is not authenticated.</p> <p><b>vlan-name</b>—Move supplicant on the interface to the VLAN specified by this name. This action is allowed only if it is the first supplicant connecting to an interface. If an authenticated supplicant is already connected, then the supplicant is not moved to the VLAN and is not authenticated.</p> |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show dot1x on page 340</a></li><li>• <a href="#">Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to a Switch on page 54</a></li><li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25</a></li><li>• <a href="#">Configuring Server Fail Fallback (CLI Procedure) on page 30</a></li><li>• <a href="#">Understanding Server Fail Fallback and Authentication on Switches</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## server-timeout

---

|                                 |                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>server-timeout <i>seconds</i>;</code>                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">dot1x authenticator interface (802.1X)</a> (all   [ <i>interface-name</i> ])                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                  |
| <b>Description</b>              | For 802.1X authentication, configure the amount of time a port will wait for a reply when relaying a response from the supplicant to the authentication server before timing out and invoking the server-fail action.                                                                                             |
| <b>Default</b>                  | 30 seconds                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <b><i>seconds</i></b> —Number of seconds.<br><b>Range:</b> 1 through 60 seconds<br><b>Default:</b> 30 seconds                                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show dot1x on page 340</a></li> <li>• <a href="#">clear dot1x on page 336</a></li> <li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25</a></li> <li>• <a href="#">802.1X for Switches Overview on page 20</a></li> </ul> |

## services (Switches)

---

**Syntax**

```
services {
 service-deployment {
 servers address {
 port-number port-number;
 }
 source-address address;
 }
 ssh {
 connection-limit limit;
 protocol-version [v1 v2];
 rate-limit limit;
 root-login (allow | deny | deny-password);
 }
}
```

**Hierarchy Level** [edit system]

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

**Description** Configure the switch so that users on remote systems can access the local switch through SSH.

The remaining statements are explained separately.

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

## snmp

```

Syntax snmp {
 client-list client-list-name {
 ip-addresses;
 }
 community community-name {
 authorization authorization;
 client-list-name client-list-name;
 clients {
 address restrict;
 }
 logical-system logical-system-name {
 routing-instance routing-instance-name {
 clients {
 addresses;
 }
 }
 }
 routing-instance routing-instance-name {
 clients {
 addresses;
 }
 }
 view view-name;
 }
 contact contact;
 description description;
 filter-duplicates;
 filter-interfaces;
 health-monitor {
 falling-threshold integer;
 interval seconds;
 rising-threshold integer;
 }
 interface [interface-names];
 location location;
 name name;
 nonvolatile {
 commit-delay seconds;
 }
 rmon {
 alarm index {
 description description;
 falling-event-index index;
 falling-threshold integer;
 falling-threshold-interval seconds;
 interval seconds;
 request-type;
 rising-event-index index;
 rising-threshold integer;
 sample-type (absolute-value | delta-value);
 startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
 syslog-subtag syslog-subtag;
 }
 }
}

```

```

 variable oid-variable;
 }
 event index {
 community community-name;
 description description;
 type type;
 }
 history history-index {
 bucket-size number;
 interface interface-name;
 interval seconds;
 owner owner-name;
 }
}
traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable> <match
 regular-expression>;
 flag flag;
}
trap-group group-name {
 categories {
 category;
 }
 destination-port port-number;
 routing-instance routing-instance-name;
 targets {
 address;
 }
 version (all | v1 | v2);
}
trap-options {
 agent-address outgoing-interface;
 source-address address;
}
v3 {
 notify name {
 tag tag-name;
 type trap;
 }
 notify-filter profile-name {
 oid object-identifier (include | exclude);
 }
 snmp-community community-index {
 community-name community-name;
 security-name security-name;
 tag tag-name;
 }
 target-address target-address-name {
 address address;
 address-mask address-mask;
 logical-system logical-system;
 port port-number;
 retry-count number;
 routing-instance routing-instance-name;
 tag-list tag-list;
 target-parameters target-parameters-name;
 }
}

```

```

 timeout seconds;
 }
 target-parameters target-parameters-name {
 notify-filter profile-name;
 parameters {
 message-processing-model (v1 | v2c | V3);
 security-level (authentication | none | privacy);
 security-model (usm | v1 | v2c);
 security-name security-name;
 }
 }
 usm {
 local-engine {
 user username {
 authentication-sha {
 authentication-password authentication-password;
 }
 authentication-md5 {
 authentication-password authentication-password;
 }
 authentication-none;
 privacy-aes128 {
 privacy-password privacy-password;
 }
 privacy-des {
 privacy-password privacy-password;
 }
 privacy-3des {
 privacy-password privacy-password;
 }
 privacy-none;
 }
 }
 remote-engine engine-id {
 user username {
 authentication-sha {
 authentication-password authentication-password;
 }
 authentication-md5 {
 authentication-password authentication-password;
 }
 authentication-none;
 privacy-aes128 {
 privacy-password privacy-password;
 }
 privacy-des {
 privacy-password privacy-password;
 }
 privacy-3des {
 privacy-password privacy-password;
 }
 privacy-none {
 privacy-password privacy-password;
 }
 }
 }
 }
}

```

```

}
vacm {
 access {
 group group-name {
 (default-context-prefix | context-prefix context-prefix) {
 security-model (any | usm | v1 | v2c) {
 security-level (authentication | none | privacy) {
 notify-view view-name;
 read-view view-name;
 write-view view-name;
 }
 }
 }
 }
 }
}
security-to-group {
 security-model (usm | v1 | v2c) {
 security-name security-name {
 group group-name;
 }
 }
}
}
view view-name {
 oid object-identifier (include | exclude);
}
}

```

**Hierarchy Level** [edit]

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

**Description** Configure SNMP.

The remaining statements are explained separately.

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

**Related Documentation**

- *Understanding the Implementation of SNMP*
- *Configuring SNMP*

## ssh

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

## static (Protocols 802.1X)

---

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | <pre>static mac-address {<br/>    interface interface-names;<br/>    vlan-assignment (vlan-id  vlan-name );<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Hierarchy Level          | [edit protocols <a href="#">dot1x authenticator</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Release Information      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Description              | <p>Configure MAC addresses to exclude from 802.1X authentication. The static MAC list provides an authentication bypass mechanism for supplicants connecting to a port, permitting devices such as printers that are not 802.1X-enabled to be connected to the network on 802.1X-enabled ports.</p> <p>Using this 802.1X authentication-bypass mechanism, the supplicant connected to the MAC address is assumed to be successfully authenticated and the port is opened for it. No further authentication is done for the supplicant.</p> <p>You can optionally configure the VLAN that the supplicant is moved to or the interfaces on which the MAC address can gain access from.</p> |
| Options                  | <p><b>mac-address</b> —The MAC address of the device for which 802.1X authentication should be bypassed and the device permitted access to the port.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Required Privilege Level | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Related Documentation    | <ul style="list-style-type: none"><li>• <a href="#">show dot1x static-mac-address on page 347</a></li><li>• <a href="#">Example: Configuring Static MAC Bypass of Authentication on a Switch on page 95</a></li><li>• <a href="#">Configuring 802.1X Interface Settings (CLI Procedure) on page 22</a></li><li>• <a href="#">Configuring 802.1X Authentication (J-Web Procedure)</a></li><li>• <a href="#">Understanding Authentication on Switches</a></li></ul>                                                                                                                                                                                                                        |

## supplicant

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | supplicant (multiple   single   single-secure);                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit protocols <b>dot1x authenticator interface (802.1X)</b> (all   [ <i>interface-names</i> ])],<br>[edit services captive-portal interface (all   <i>interface-names</i> )]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement added to the [edit services captive-portal interface] hierarchy in Junos OS Release 10.1 for EX Series switches<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | Configure the MAC-based method used to authenticate clients for 802.1X or captive portal authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Default</b>                  | single                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                  | <p><b>single</b>—Authenticates only the first client that connects to an authenticator port. All other clients connecting to the authenticator port after the first are permitted free access to the port without further authentication. If the first authenticated client logs out, all other supplicants are locked out until a client authenticates again.</p> <p><b>single-secure</b>—Authenticates only one client to connect to an authenticator port. The host must be directly connected to the switch.</p> <p><b>multiple</b>—Authenticates multiple clients individually on one authenticator port. You can configure the number of clients per port. If you also configure a maximum number of devices that can be connected to a port through port security settings, the lower of the configured values is used to determine the maximum number of clients allowed per port.</p> |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31</a></li> <li>• <i>Example: Setting Up Captive Portal Authentication on an EX Series Switch</i></li> <li>• <i>Understanding Authentication on Switches</i></li> <li>• <i>Configuring Captive Portal Authentication (CLI Procedure)</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## supplicant-timeout

---

|                                 |                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>supplicant-timeout <i>seconds</i>;</code>                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">dot1x authenticator interface (802.1X)</a> (all   [ <i>interface-name</i> ])                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                           |
| <b>Description</b>              | For 802.1X authentication, configure how long the port waits for a response when relaying a request from the authentication server to the supplicant before resending the request.                                                                                                         |
| <b>Default</b>                  | 30 seconds                                                                                                                                                                                                                                                                                 |
| <b>Options</b>                  | <b><i>seconds</i></b> —Number of seconds.<br><b>Range:</b> 1 through 60 seconds<br><b>Default:</b> 30 seconds                                                                                                                                                                              |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">supplicant on page 315</a></li><li>• <a href="#">Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31</a></li><li>• <i>Understanding Authentication on Switches</i></li></ul> |

## system

```
Syntax system {
 accounting {
 events [login change-log interactive-commands];
 destination {
 radius {
 server {
 server-address {
 accounting-port port-number;
 retry number;
 secret password;
 source-address address;
 timeout seconds;
 }
 }
 }
 }
 tacplus {
 server {
 server-address {
 port port-number;
 secret password;
 single-connection;
 timeout seconds;
 }
 }
 }
 }
 archival {
 configuration {
 archive-sites {
 ftp://<username>:<password>@<host>:<port>/<url-path>;
 ftp://<username>:<password>@<host>:<port>/<url-path>;
 }
 transfer-interval interval;
 transfer-on-commit;
 }
 }
 arp {
 aging-timer minutes;
 interfaces;
 }
 authentication-order [authentication-methods];
 (compress-configuration-files | no-compress-configuration-files);
 default-address-selection;
 domain-name domain-name;
 domain-search [domain-list];
 host-name hostname;
 internet-options {
 icmpv4-rate-limit bucket-size bucket-size packet-rate packet-rate;
 source-port upper-limit <upper-limit>;
 }
 location {
```

```

altitude feet;
building name;
country-code code;
floor number;
hcoord horizontal-coordinate;
lata service-area;
latitude degrees;
longitude degrees;
npa-nxx number;
postal-code postal-code;
rack number;
vcoord vertical-coordinate;
}
login {
 announcementtext;
 class class-name {
 access-end;
 access-start;
 allow-configuration "regular-expression";
 allowed-days "regular-expression";
 deny-commands "regular-expression";
 deny-configuration "regular-expression";
 idle-timeout minutes;
 login-tip;
 permissions [permissions];
 }
 message text;
 password {
 change-type (set-transitions | character-set);
 format (md5 | sha1 | des);
 maximum-length length;
 minimum-changes number;
 minimum-length length;
 }
 retry-options {
 backoff-factor seconds;
 backoff-threshold number;
 minimum-time seconds;
 tries-before-disconnect number;
 }
}
user username {
 authentication {
 (encrypted-password "password" | plain-text-password);
 load-key-file URL;
 remote-debug-permission (qfabric-admin | qfabric-operator | qfabric-user);
 ssh-rsa "public-key";
 ssh-dsa "public-key";
 }
 uid uid-value;
 class class-name;
 full-name complete-name;
}
}
name-server {
 address;
}

```

```

no-multicast-echo;
no-redirects;
no-ping-record-route;
no-ping-time-stamp;
ntp {
 authentication-key number type type value password;
 serveraddress <key key-number> <version value> <prefer>;
}
ports {
 auxiliary {
 disable;
 insecure;
 type terminal-type;
 }
 console {
 disable;
 insecure;
 log-out-on-disconnect;
 type terminal-type;
 }
}
radius-server server-address {
 accounting-port port-number;
 port number;
 retry number;
 secret password;
 source-address source-address;
 timeout seconds;
}
radius-options {
 password-protocol mschap-v2;
}
attributes {
 nas-ip-address ip-address;
}
root-authentication {
 (encrypted-password "password" | plain-text-password);
 ssh-rsa "public-key";
 ssh-dsa "public-key";
}
(saved-core-context | no-saved-core-context);
saved-core-files saved-core-files;
services {
 finger {
 connection-limit limit;
 rate-limit limit;
 }
 flow-tap-dtcp {
 ssh {
 connection-limit limit;
 rate-limit limit;
 }
 }
}
ftp {
 connection-limit limit;
 rate-limit limit;
}

```

```
}
service-deployment {
 servers server-address {
 port port-number;
 }
 source-address source-address;
}
ssh {
 root-login (allow | deny | deny-password);
 protocol-version [v1 v2];
 connection-limit limit;
 rate-limit limit;
}
telnet {
 connection-limit limit;
 rate-limit limit;
}
web-management {
 http {
 interfaces [interface-names];
 port port;
 }
 https {
 interfaces [interface-names];
 local-certificate name;
 port port;
 }
 session {
 idle-timeout [minutes];
 session-limit [session-limit];
 }
}
xnm-clear-text {
 connection-limit limit;
 rate-limit limit;
}
xnm-ssl {
 connection-limit limit;
 local-certificate name;
 rate-limit limit;
}
}
static-host-mapping {
 hostname {
 alias [alias];
 inet [address];
 sysid system-identifier;
 }
}
syslog {
 archive {
 files number;
 size maximum-file-size;
 start-time "YYYY-MM-DD.hh:mm";
 transfer-interval minutes;
 (world-readable | no-world-readable);
 }
}
```

```

}
console {
 facility severity;
}
file filename {
 archive {
 files number;
 size maximum-file-size;
 start-time "YYYY-MM-DD.hh:mm";
 transfer-interval minutes;
 (world-readable | no-world-readable);
 }
 explicit-priority;
 facility severity;
 match "regular-expression";
 structured-data {
 brief;
 }
}
host (hostname | other-routing-engine | scc-master) {
 explicit-priority;
 facility-override facility;
 facility severity;
 log-prefix string;
 match "regular-expression";
}
source-address source-address;
time-format (millisecond | year | year millisecond);
user (username | *) {
 facility severity;
 match "regular-expression";
}
}
tacplus-options {
 service-name service-name;
 (no-cmd-attribute-value | exclude-cmd-attribute);
}
tacplus-server server-address {
 port
 secret password;
 single-connection;
 source-address source-address;
 timeout seconds;
}
time-zone (GMThour-offset | time-zone);
}
tracing {
 destination-override {
 syslog host;
 }
}
use-imported-time-zones;
}

```

Hierarchy Level [\[edit\]](#)

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

**Description** Configure system management properties.



**NOTE:** The `radius-server source-address` and `radius-options` statements are not available on the QFabric system.

---

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

## tacplus-options

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> tacplus-options {   (exclude-cmd-attribute   no-cmd-attribute-value);   enhanced-accounting;   service-name <i>service-name</i>;   timestamp-and-timezone; } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit system]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p><b>no-cmd-attribute-value</b> and <b>exclude-cmd-attribute</b> options introduced in Junos OS Release 9.3.</p> <p>Statement introduced in Junos OS Release 11.1 for QFX Series.</p> <p><b>timestamp-and-timezone</b> option introduced in Junos OS Release 12.2.</p> <p><b>enhanced-accounting</b> option introduced in Junos OS Release 14.1.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p>                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | Configure TACACS+ options for authentication and accounting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><b>enhanced-accounting</b>—View the attribute values of a logged in user.</p> <p><b>exclude-cmd-attribute</b>—Exclude the <b>cmd</b> attribute value completely from start and stop accounting records to enable logging of accounting records in the correct log file on a TACACS+ server.</p> <p><b>no-cmd-attribute-value</b>—Set the <b>cmd</b> attribute value to an empty string in the TACACS+ accounting start and stop requests to enable logging of accounting records in the correct log file on a TACACS+ server.</p> <p><b>service-name <i>service-name</i></b>—Name of the authentication service used when you configure multiple TACACS+ servers to use the same authentication service.</p> <p><b>Default:</b> junos-exec</p> <p><b>timestamp-and-timezone</b>—Include this statement if you want start time, stop time, and timezone attributes included in start/stop accounting records.</p> |
| <b>Required Privilege Level</b> | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Configuring TACACS+ Authentication</i></li> <li>• <i>Configuring TACACS+ System Accounting</i></li> <li>• <a href="#">Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 175</a></li> <li>• <i>enhanced-accounting</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## targets

---

|                                 |                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>targets {<br/>    address;<br/>}</code>                                                                                                 |
| <b>Hierarchy Level</b>          | <code>[edit snmp trap-group group-name]</code>                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Configure one or more systems to receive SNMP traps.                                                                                          |
| <b>Options</b>                  | <b>address</b> —IPv4 or IPv6 address of the system to receive traps. You must specify an address, not a hostname.                             |
| <b>Required Privilege Level</b> | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring SNMP Trap Groups</a></li></ul>                                                |

## transmit-period

---

|                                 |                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>transmit-period seconds;</code>                                                                                                                                                                |
| <b>Hierarchy Level</b>          | <code>[edit protocols dot1x authenticator interface (802.1X) (all   [interface-name])]</code>                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                     |
| <b>Description</b>              | For 802.1X authentication, how long the port waits before retransmitting the initial EAPOL PDUs to the supplicant.                                                                                   |
| <b>Default</b>                  | 30 seconds                                                                                                                                                                                           |
| <b>Options</b>                  | <b>seconds</b> —Number of seconds the port waits before retransmitting the initial EAPOL PDUs to the supplicant.<br><b>Range:</b> 1 through 65,535 seconds<br><b>Default:</b> 30 seconds             |
| <b>Required Privilege Level</b> | <code>routing</code> —To view this statement in the configuration.<br><code>routing-control</code> —To add this statement to the configuration.                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring 802.1X Interface Settings (CLI Procedure) on page 22</a></li><li>• <a href="#">802.1X for Switches Overview on page 20</a></li></ul> |

## traceoptions (LLDP)

|                            |                                                                                                                                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable   no-world-readable&gt; &lt;no-stamp&gt;     &lt;replace&gt;;     flag <i>flag</i> &lt;disable&gt;; } </pre>        |
| <b>Hierarchy Level</b>     | [edit protocols <a href="#">lldp</a> ]                                                                                                                                                                                                    |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> |
| <b>Description</b>         | Define tracing operations for the Link Layer Discovery Protocol (LLDP). You can trace messages under LLDP for LLDP and PTOPO MIBs.                                                                                                        |



**NOTE:** The traceoptions statement is not supported on the QFX3000 QFabric system.

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

- **vlan**—Trace VLAN update events.

**no-stamp**—(Optional) Do not timestamp the trace file.

**Default:** If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

**no-world-readable**—(Optional) Restrict file access to the user who created the file.

**replace**—(Optional) Replace an existing trace file if there is one rather than appending output to it.

**size size**—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **files** option.

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

**Range:** 10 KB through 1 GB

**Default:** 128 KB

**Default:** If you do not include this option, tracing output is appended to an existing trace file.

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



**NOTE:** The **traceoptions** statement is not supported on the QFX3000 QFabric system.

---

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

|                              |                                                                                                                                                                                                                                                                                                       |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Related Documentation</b> | <ul style="list-style-type: none"><li>• <a href="#">Configuring LLDP-MED (CLI Procedure) on page 107</a></li><li>• <a href="#">Understanding 802.1X and LLDP and LLDP-MED on page 101</a></li><li>• <a href="#">Configuring LLDP</a></li><li>• <a href="#">Understanding LLDP on page 5</a></li></ul> |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## transfer-interval (Configuration)

|                            |                                                                                                                                                                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>transfer-interval <i>interval</i>;</code>                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>     | [edit system archival configuration]                                                                                                                                                                                                                                            |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>         | Configure the router or switch to periodically transfer its currently active configuration to an archive site.                                                                                                                                                                  |
| <b>Options</b>             | <b>interval</b> —Interval at which to transfer the current configuration to an archive site.<br><b>Range:</b> 15 through 2880 minutes                                                                                                                                           |



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

|                                 |                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site</i></li> <li>• <i>archive</i></li> <li>• <a href="#">configuration on page 249</a></li> <li>• <a href="#">transfer-on-commit on page 328</a></li> </ul> |

## transfer-on-commit

---

|                            |                                                                                                                                                                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | transfer-on-commit;                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>     | [edit system archival configuration]                                                                                                                                                                                                                                            |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>         | Configure the router or switch to transfer its currently active configuration to an archive site each time you commit a candidate configuration.                                                                                                                                |



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



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

|                                 |                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site</i></li><li>• <i>archive</i></li><li>• <a href="#">configuration on page 249</a></li><li>• <a href="#">transfer-interval on page 327</a></li></ul> |

## trap-group

|                                 |                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> trap-group <i>group-name</i> {     categories {         <i>category</i>;     }     destination-port <i>port-number</i>;     routing-instance <i>instance</i>;     targets {         <i>address</i>;     }     version (all   v1   v2); } </pre>                                    |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p>                                                                |
| <b>Description</b>              | Create a named group of hosts to receive the specified trap notifications. The name of the trap group is embedded in SNMP trap notification packets as one variable binding (varbind) known as the community name. At least one trap group must be configured for SNMP traps to be sent. |
| <b>Options</b>                  | <p><b><i>group-name</i></b>—Name of the trap group. If the name includes spaces, enclose it in quotation marks (" ").</p> <p>The remaining statements are explained separately.</p>                                                                                                      |
| <b>Required Privilege Level</b> | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Configuring SNMP Trap Groups</i></li> </ul>                                                                                                                                                                                                  |

## trap-options

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>trap-options {<br/>    agent-address outgoing-interface;<br/>    source-address address;<br/>}</pre>                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                                                     |
| <b>Description</b>              | <p>Using SNMP trap options, you can set the source address of every SNMP trap packet sent by the router or switch to a single address, regardless of the outgoing interface. In addition, you can set the agent address of each SNMPv1 trap. For more information about the contents of SNMPv1 traps, see RFC 1157.</p> <p>The remaining statements are explained separately.</p> |
| <b>Default</b>                  | Disabled                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Configuring SNMP Trap Options</i></li></ul>                                                                                                                                                                                                                                                                                            |

## user (Access)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> user username {   authentication {     (encrypted-password "password"   plain-text-password);     load-key-file URL;     remote-debug-permission (qfabric-admin   qfabric-operator   qfabric-user);     ssh-dsa "public-key" &lt;from hostname&gt;;     ssh-rsa "public-key" &lt;from hostname&gt;;   }   class class-name;   full-name "complete-name";   uid uid-value; } </pre> |
| <b>Hierarchy Level</b>          | [edit system login]                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                                                                                                                                                                 |
| <b>Description</b>              | Configure access permission for individual users.                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | The remaining statements are explained separately.                                                                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Junos OS User Accounts on page 169</a></li> <li>• <i>class</i></li> </ul>                                                                                                                                                                                                                                               |

## version

---

|                                 |                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | version (all   v1   v2);                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit snmp trap-group <i>group-name</i> ]                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Specify the version number of SNMP traps.                                                                                                     |
| <b>Default</b>                  | all—Send an SNMPv1 and SNMPv2 trap for every trap condition.                                                                                  |
| <b>Options</b>                  | all—Send an SNMPv1 and SNMPv2 trap for every trap condition.<br><br>v1—Send SNMPv1 traps only.<br><br>v2—Send SNMPv2 traps only.              |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Configuring SNMP Trap Groups</i></li></ul>                                                         |

## vlan-assignment

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>vlan-assignment (vlan-id   vlan-name);</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | <p>[edit protocols <a href="#">dot1x authenticator</a> authentication-profile-name <a href="#">static (Protocols 802.1X)</a> <a href="#">mac-address</a>],</p> <p>[edit ethernet-switching-options authentication-whitelist],</p> <p>[edit switch-options authentication-whitelist]</p>                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement added to the [edit ethernet-switching-options authentication-whitelist] hierarchy in Junos OS Release 10.1 for EX Series switches.</p> <p>Statement added to the [edit switch-options authentication-whitelist] hierarchy in Junos OS Release 13.2X50-D10 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.</p>                                                                                                                            |
| <b>Description</b>              | Configure the VLAN that is associated with the list of MAC addresses that are excluded from RADIUS authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <i>vlan-id   vlan-name</i> —The name of the VLAN or the VLAN tag identifier to associate with the device. The VLAN already exists on the switch.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show dot1x static-mac-address on page 347</a></li> <li>• <a href="#">Example: Configuring Static MAC Bypass of Authentication on a Switch on page 95</a></li> <li>• <a href="#">Example: Setting Up Captive Portal Authentication on an EX Series Switch</a></li> <li>• <a href="#">Understanding Authentication on Switches</a></li> <li>• <a href="#">Example: Setting Up Captive Portal Authentication on an EX Series Switch</a></li> <li>• <a href="#">Configuring Captive Portal Authentication (CLI Procedure)</a></li> </ul> |

## voip

---

|                                 |                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>voip {<br/>  interface (all   [<i>interface-name</i>   access-ports]) {<br/>    vlan <i>vlan-name</i> ;<br/>    forwarding-class &lt;assured-forwarding   best-effort   expedited-forwarding  <br/>      network-control&gt;;<br/>  }<br/>}</pre>                                                                                           |
| <b>Hierarchy Level</b>          | [edit ethernet-switching-options],<br>[edit switch-options]                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                                                 |
| <b>Description</b>              | Configure voice over IP (VoIP) interfaces.<br><br>The remaining statements are explained separately.                                                                                                                                                                                                                                             |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch</i></li><li>• <i>Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication</i></li><li>• <i>Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support</i></li></ul> |

## CHAPTER 17

# Operational Commands

- `clear dot1x`
- `clear lldp neighbors`
- `clear lldp statistics`
- `show dot1x`
- `show dot1x authentication-failed-users`
- `show dot1x firewall`
- `show dot1x static-mac-address`
- `show ethernet-switching interfaces`
- `show lldp`
- `show lldp local-information`
- `show lldp neighbors`
- `show lldp statistics`
- `show network-access aaa statistics accounting`
- `show network-access aaa statistics authentication`
- `show network-access aaa statistics dynamic-requests`
- `show route instance`
- `show snmp statistics`
- `ssh`

## clear dot1x

**Syntax** `clear dot1x (firewall <counter-name> | interface <[interface-name]> | mac-address [mac-addresses] | statistics <interface interface-name>)`

**Release Information** Command introduced in Junos OS Release 9.0 for EX Series switches.  
**firewall** option added in Junos OS Release 9.5 for EX Series switches.  
 Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

**Description** Reset the authentication state of an interface or delete 802.1X statistics from the switch. When you reset an interface using the **interface** or **mac-address** options, reauthentication on the interface is also triggered. The switch sends out a multicast message on the interface to restart the authentication of all connected supplicants. If a MAC address is reset, then the switch sends out a unicast message to that specific MAC address to restart authentication.

If a supplicant is sending traffic when the **clear dot1x interface** command is issued, the authenticator immediately initiates reauthentication. This process happens quickly, and it might seem that reauthentication did not occur. To verify that reauthentication has happened, issue the **show dot1x interface detail** command. The values for **Reauthentication due** and **Reauthentication interval** will be about the same.



**CAUTION:** When you clear the learned MAC addresses from an interface using the **clear dot1x interface** command, all MAC addresses are cleared, including those in static MAC bypass list.

If you have enabled Media Access Control Security (MACsec) using static secure association key (SAK) security mode on an EX Series switch, the SAKs are rotated when the **clear dot1x** command is entered. The **clear dot1x** command has no impact on MACsec when MACsec is enabled using static connectivity association keys (CAK) or any other security mode.

**Options** **firewall <counter-name>**—Clear 802.1X firewall counter statistics. If the *counter-name* option is specified, clear 802.1X firewall statistics for that counter.

**interface <[interface-name]>**—Reset the authentication state of all the supplicants (also, clears all the authentication bypassed clients) connected to the specified interface (when the interface is an authenticator) or reset the authentication state for the interface itself (when the interface is a supplicant).

**mac-address [mac-addresses]**—Reset the authentication state of the specified MAC addresses.

**statistics <interface interface-name>**—Clear 802.1X statistics on all 802.1X-enabled interfaces. If the **interface** option is specified, clear 802.1X firewall statistics for that interface or interfaces.

**Required Privilege Level** view

**Related Documentation**

- [show dot1x on page 340](#)
- [Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31](#)
- [Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 40](#)

**List of Sample Output**

- [clear dot1x firewall on page 337](#)
- [clear dot1x interface \(Specific Interfaces\) on page 337](#)
- [clear dot1x mac-address \(Specific MAC Address\) on page 337](#)
- [clear dot1x statistics interface \(Specific Interface\) on page 337](#)

## Sample Output

**clear dot1x firewall**

```
user@switch> clear dot1x firewall c1
```

**clear dot1x interface (Specific Interfaces)**

```
user@switch> clear dot1x interface ge-1/0/0 ge-2/0/0 ge-2/0/0 ge5/0/0
```

**clear dot1x mac-address (Specific MAC Address)**

```
user@switch> clear dot1x mac-address 00:04:ae:cd:23:5f
```

**clear dot1x statistics interface (Specific Interface)**

```
user@switch> clear dot1x statistics interface ge-1/0/1
```

## clear lldp neighbors

---

|                                 |                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear lldp neighbors <interface <i>interface</i> >                                                                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.1 for the QFX Series.<br>Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.                                                |
| <b>Description</b>              | Clear the learned remote neighbor information on all or selected interfaces.                                                                                                                  |
| <b>Options</b>                  | <b>none</b> —Clear the remote neighbor information on all interfaces.<br><br><b>interface <i>interface</i></b> —(Optional) Clear the remote neighbor information from the selected interface. |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>show lldp</i></li><li>• <i>Configuring LLDP</i></li><li>• <a href="#">Understanding LLDP on page 5</a></li></ul>                                   |
| <b>List of Sample Output</b>    | <a href="#">clear lldp neighbors on page 338</a><br><a href="#">clear lldp neighbors interface on page 338</a>                                                                                |

### Sample Output

#### clear lldp neighbors

```
user@switch> clear lldp neighbors
```

#### clear lldp neighbors interface

```
user@switch> clear lldp neighbors interface ge-0/1/1.0
```

## clear lldp statistics

---

|                                 |                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>clear lldp statistics</code><br><code>&lt;interface <i>interface</i>&gt;</code>                                                                    |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.<br>Command introduced in Junos OS Release 11.1 for the QFX Series.           |
| <b>Description</b>              | Clear LLDP statistics on one or more interfaces.                                                                                                         |
| <b>Options</b>                  | <b>none</b> —Clears LLDP statistics on all interfaces.<br><br><b>interface <i>interface-names</i></b> —(Optional) Clear LLDP statistics on an interface. |
| <b>Required Privilege Level</b> | view                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring LLDP</a></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul>             |
| <b>List of Sample Output</b>    | <a href="#">clear lldp statistics on page 339</a><br><a href="#">clear lldp statistics interface on page 339</a>                                         |

### Sample Output

#### clear lldp statistics

```
user@switch> clear lldp statistics
```

#### clear lldp statistics interface

```
user@switch> clear lldp statistics interface ge-0/1/1.0
```

## show dot1x

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show dot1x</b><br><b>&lt;brief   detail&gt;</b><br><b>&lt;interface <i>interface-name</i>&gt;</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Display the current operational state of all ports with the list of connected users.<br><br>This command displays the list of connected supplicants received from the RADIUS authentication server regardless of the session state—that is, for both authenticated supplicants and for supplicants that attempted authentication.                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                  | <b>none</b> —Display information for all authenticator ports.<br><br><b>brief   detail</b> —(Optional) Display the specified level of output.<br><br><b>interface <i>interface-name</i></b> —Display information for the specified port with a list of connected supplicants.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dot1x on page 336</a></li> <li>• <a href="#">Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 31</a></li> <li>• <a href="#">Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to a Switch on page 54</a></li> <li>• <a href="#">Example: Configuring Fallback Options on Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 69</a></li> <li>• <a href="#">Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 40</a></li> <li>• <a href="#">Verifying 802.1X Authentication on page 74</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show dot1x interface brief on page 343</a><br><a href="#">show dot1x interface detail on page 343</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Output Fields</b>            | <a href="#">Table 36 on page 340</a> lists the output fields for the <b>show dot1x</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Table 36: show dot1x Output Fields**

| Field Name  | Field Description                                        | Level of Output |
|-------------|----------------------------------------------------------|-----------------|
| Interface   | Name of a port.                                          | All levels      |
| MAC address | The MAC address of the connected supplicant on the port. | All levels      |

Table 36: show dot1x Output Fields (*continued*)

| Field Name                  | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Level of Output      |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <b>Role</b>                 | The 802.1X authentication role of the interface. When 802.1X is enabled on an interface, the role is <b>Authenticator</b> . As <b>Authenticator</b> , the interface blocks LAN access until a supplicant is authenticated through 802.1X or MAC RADIUS authentication.                                                                                                                                                                                                                                                                                                                                                                | <b>brief, detail</b> |
| <b>State</b>                | <p>The state of the port:</p> <ul style="list-style-type: none"> <li>• <b>Authenticated</b>—The supplicant has been authenticated through the RADIUS server or has been permitted access through server fail fallback.</li> <li>• <b>Authenticating</b>—The supplicant is authenticating through the RADIUS server.</li> <li>• <b>Held</b>—An action has been triggered through server fail fallback during a RADIUS server timeout. A supplicant is denied access, permitted access through a specified VLAN, or maintains the authenticated state granted to it before the RADIUS server timeout occurred.</li> </ul>               | <b>brief</b>         |
| <b>User</b>                 | The user name of the connected supplicant                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>brief</b>         |
| <b>Administrative state</b> | <p>The administrative state of the port:</p> <ul style="list-style-type: none"> <li>• <b>auto</b>—Traffic is allowed through the port based on the authentication result. (Default)</li> <li>• <b>force-authorize</b>—All traffic flows through the port irrespective of the authentication result. This state is not allowed on an interface whose VLAN membership has been set to <b>dynamic</b>.</li> <li>• <b>force-unauthorize</b>—All traffic drops on the port irrespective of the authentication result. This state is not allowed on an interface whose VLAN membership has been set to <b>dynamic</b>.</li> </ul>           | <b>detail</b>        |
| <b>Supplicant</b>           | <p>The mode for the supplicant:</p> <ul style="list-style-type: none"> <li>• <b>single</b>—Authenticates only the first supplicant. All other supplicants who connect later to the port are allowed full access without any further authentication. They effectively “piggyback” on the first supplicant’s authentication.</li> <li>• <b>single-secure</b>—Allows only one supplicant to connect to the port. No other supplicant is allowed to connect until the first supplicant logs out.</li> <li>• <b>multiple</b>—Allows multiple supplicants to connect to the port. Each supplicant is authenticated individually.</li> </ul> | <b>detail</b>        |
| <b>Quiet period</b>         | The number of seconds the port remains in the wait state following a failed authentication exchange with the supplicant before reattempting the authentication. The default value is 60 seconds. The range is 0 through 65,535 seconds.                                                                                                                                                                                                                                                                                                                                                                                               | <b>detail</b>        |
| <b>Transmit period</b>      | The number of seconds the port waits before retransmitting the initial EAPOL PDUs to the supplicant. The default value is 30 seconds. The range is 1 through 65,535 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>detail</b>        |

Table 36: show dot1x Output Fields (*continued*)

| Field Name                                                  | Field Description                                                                                                                                                                                                                                                                                                                                                                                                       | Level of Output |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>MAC radius</b>                                           | MAC RADIUS authentication: <ul style="list-style-type: none"> <li>• <b>enabled</b>—The switch sends an EAPOL request to the connecting host to attempt 802.1X authentication and if the connecting host is unresponsive, the switch tries to authenticate using the MAC address.</li> <li>• <b>disabled</b>—The default. The switch will not attempt to authenticate the MAC address of the connecting host.</li> </ul> | <b>detail</b>   |
| <b>MAC radius restrict</b>                                  | The authentication method is restricted to MAC RADIUS only. 802.1X authentication is not enabled.                                                                                                                                                                                                                                                                                                                       | <b>detail</b>   |
| <b>Reauthentication</b>                                     | The reauthentication state: <ul style="list-style-type: none"> <li>• <b>disable</b>—Periodic reauthentication of the client is disabled.</li> <li>• <b>interval</b>—Sets the periodic reauthentication time interval. The default value is 3600 seconds. The range is 1 through 65,535 seconds.</li> </ul>                                                                                                              | <b>detail</b>   |
| <b>Supplicant timeout</b>                                   | The number of seconds the port waits for a response when relaying a request from the authentication server to the supplicant before resending the request. The default value is 30 seconds. The range is 1 through 60 seconds.                                                                                                                                                                                          | <b>detail</b>   |
| <b>Server timeout</b>                                       | The number of seconds the port waits for a reply when relaying a response from the supplicant to the authentication server before timing out. The default value is 30 seconds. The range is 1 through 60 seconds.                                                                                                                                                                                                       | <b>detail</b>   |
| <b>Maximum EAPOL requests</b>                               | The maximum number of retransmission times of an EAPOL request packet to the supplicant before the authentication session times out. The default value is 2. The range is 1 through 10.                                                                                                                                                                                                                                 | <b>detail</b>   |
| <b>Number of clients bypassed because of authentication</b> | The number of non-802.1X clients granted access to the LAN by means of static MAC bypass. The following fields are displayed: <ul style="list-style-type: none"> <li>• <b>Client</b>—MAC address of the client.</li> <li>• <b>vlan</b> —The name of the VLAN to which the client is connected.</li> </ul>                                                                                                               | <b>detail</b>   |
| <b>Guest VLAN member</b>                                    | The VLAN to which a supplicant is connected when the supplicant is authenticated using a guest VLAN. If a guest VLAN is not configured on the interface, this field displays <b>&lt;not configured&gt;</b> .                                                                                                                                                                                                            | <b>detail</b>   |
| <b>Number of connected supplicants</b>                      | The number of supplicants connected to a port.                                                                                                                                                                                                                                                                                                                                                                          | <b>detail</b>   |
| <b>Supplicant</b>                                           | The user name and MAC address of the connected supplicant.                                                                                                                                                                                                                                                                                                                                                              | <b>detail</b>   |

Table 36: show dot1x Output Fields (*continued*)

| Field Name              | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Level of Output |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Authentication method   | <p>The 802.1X authentication method used for a supplicant:</p> <ul style="list-style-type: none"> <li><b>Guest VLAN</b>—A supplicant is connected to the LAN through the guest VLAN.</li> <li><b>MAC Radius</b>—A nonresponsive host is authenticated based on its MAC address. The MAC address is configured as permitted on the RADIUS server, the RADIUS server lets the switch know that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected.</li> <li><b>Radius</b>—A supplicant is configured on the RADIUS server, the RADIUS server communicates this to the switch, and the switch opens LAN access on the interface to which the supplicant is connected.</li> <li><b>Server-fail deny</b>—If the RADIUS servers time out, all supplicants are denied access to the LAN, preventing traffic from flowing from the supplicant through the interface. This is the default.</li> <li><b>Server-fail permit</b>—When the RADIUS server is unavailable, a supplicant is still permitted access to the LAN as if the supplicant had been successfully authenticated by the RADIUS server.</li> <li><b>Server-fail use-cache</b>—If the RADIUS servers time out during reauthentication, previously authenticated supplicants are reauthenticated, but new supplicants are denied LAN access.</li> <li><b>Server-fail VLAN</b>—A supplicant is configured to be moved to a specified VLAN if the RADIUS server is unavailable to reauthenticate the supplicant. (The VLAN must already exist on the switch.)</li> </ul> | detail          |
| Authenticated VLAN      | The VLAN to which the supplicant is connected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | detail          |
| Dynamic filter          | User policy filter sent by the RADIUS server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | detail          |
| Session Reauth interval | The configured reauthentication interval.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | detail          |
| Reauthentication due in | The number of seconds in which reauthentication will occur again for the connected supplicant.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | detail          |

## Sample Output

### show dot1x interface brief

```

user@switch> show dot1x interface brief
802.1X Information:
Interface Role State MAC address User
ge-0/0/1 Authenticator Authenticated 00:a0:d2:18:1a:c8 user1
ge-0/0/2 Authenticator Connecting 00:a6:55:f2:94:ae user3
ge-0/0/3 Authenticator Held

```

### show dot1x interface detail

```

user@switch> show dot1x interface ge-0/0/16.0 detail

ge-0/0/16.0
Role: Authenticator
Administrative state: Auto

```

Supplicant mode: Single  
Number of retries: 3  
Quiet period: 60 seconds  
Transmit period: 30 seconds  
Mac Radius: Enabled  
Mac Radius Strict: Disabled  
Reauthentication: Enabled  
Configured Reauthentication interval: 40 seconds  
Supplicant timeout: 30 seconds  
Server timeout: 30 seconds  
Maximum EAPOL requests: 1  
Guest VLAN member: <not configured>  
Number of connected supplicants: 1  
    Supplicant: abc, 00:30:48:8C:66:BD  
        Operational state: Authenticated  
        Authentication method: Radius  
        Authenticated VLAN: v200  
        Reauthentication due in 17 seconds

## show dot1x authentication-failed-users

|                                 |                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show dot1x authentication-failed-users                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                       |
| <b>Description</b>              | Display supplicants (users) that have failed 802.1X authentication.                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dot1x on page 336</a></li> <li>• <a href="#">Example: Configuring Static MAC Bypass of Authentication on a Switch on page 95</a></li> <li>• <a href="#">Configuring 802.1X Interface Settings (CLI Procedure) on page 22</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show dot1x authentication-failed-users on page 345</a>                                                                                                                                                                                                                                 |
| <b>Output Fields</b>            | <a href="#">Table 37 on page 345</a> lists the output fields for the <b>show dot1x authentication-failed-users</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                |

**Table 37: show dot1x authentication-failed-users Output Fields**

| Field Name           | Field Description                                                                           | Level of Output |
|----------------------|---------------------------------------------------------------------------------------------|-----------------|
| <b>Interface</b>     | The MAC address configured to bypass 802.1X authentication.                                 | all             |
| <b>MAC address</b>   | The MAC address configured statically on the interface.                                     | all             |
| <b>User</b>          | The user that is configured on the RADIUS server and that has failed 802.1X authentication. | all             |
| <b>Failure Count</b> | The number of times that 802.1X authentication has failed on the interface.                 | all             |

## Sample Output

### show dot1x authentication-failed-users

```
user@switch> show dot1x authentication-failed-users
```

| Interface   | MAC address       | User         | Failure Count |
|-------------|-------------------|--------------|---------------|
| ge-0/0/17.0 | 00:37:00:00:00:00 | 003700000000 | 28            |
| ge-0/0/20.0 | 00:04:10:00:00:00 | 000410000000 | 32            |
| ge-0/0/18.0 | 00:00:03:00:0a:00 | 000003000a00 | 4             |
| ge-0/0/19.0 | 00:00:03:00:0b:00 | 000003000b00 | 18            |

## show dot1x firewall

---

|                                 |                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show dot1x firewall &lt;interface <i>interface-name</i>&gt;</code>                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.5 for EX Series switches.<br>Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                   |
| <b>Description</b>              | Displays information about the firewall filters for each user or nonresponsive host that is authenticated on each 802.1X-enabled interface that is configured for multiple supplicants. For example, if the firewall filter is configured with a term for counters, the command shows the count for each user. |
| <b>Options</b>                  | <b>none</b> —Display information for all interfaces.<br><br><b>interface <i>interface-names</i></b> —(Optional) Display information for the specified interface.                                                                                                                                               |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">clear dot1x on page 336</a></li><li>• <i>Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication</i></li></ul>                                                                            |
| <b>List of Sample Output</b>    | <a href="#">show dot1x firewall on page 346</a><br><a href="#">show dot1x firewall on page 346</a>                                                                                                                                                                                                             |
| <b>Output Fields</b>            | Output fields include any action modifier that is specified in firewall filters.                                                                                                                                                                                                                               |

### Sample Output

#### show dot1x firewall

(Showing counter action)

```
user@switch> show dot1x firewall
Filter: dot1x-filter-ge-0/0/3
Counters
 counter1_dot1x_ge-0/0/3_user1 342
 counter1_dot1x_ge-0/0/3_user2 857
```

#### show dot1x firewall

(Showing policer action)

```
user@switch> show dot1x firewall
Filter: dot1x_ge-0/0/0
Counters
 p1-t1 494946
```

## show dot1x static-mac-address

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show dot1x static-mac-address &lt;(interface [interface-name])&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Displays all the static MAC addresses that are configured to bypass 802.1X authentication on the switch.                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <b>none</b> —Display static MAC addresses for all interfaces.<br><br><b>interface interface-name</b> —(Optional) Display static MAC addresses for a specific interface.                                                                                                                                                                                                                                                                                                             |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dot1x on page 336</a></li> <li>• <a href="#">Example: Configuring Static MAC Bypass of Authentication on a Switch on page 95</a></li> <li>• <a href="#">Adding a Static MAC Address Entry to the Ethernet Switching Table (CLI Procedure)</a></li> <li>• <a href="#">Configuring 802.1X Interface Settings (CLI Procedure) on page 22</a></li> <li>• <a href="#">Understanding Authentication on Switches</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show dot1x static-mac-address on page 347</a><br><a href="#">show dot1x static-mac-address interface (Specific Interface) on page 348</a>                                                                                                                                                                                                                                                                                                                               |
| <b>Output Fields</b>            | <a href="#">Table 38 on page 347</a> lists the output fields for the <b>show dot1x static-mac-address</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                          |

**Table 38: show dot1x static-mac-address Output Fields**

| Field Name             | Field Description                                                                      | Level of Output |
|------------------------|----------------------------------------------------------------------------------------|-----------------|
| <b>MAC address</b>     | The MAC address of the device that is configured to bypass 802.1X authentication.      | <b>all</b>      |
| <b>VLAN-Assignment</b> | The name of the VLAN to which the device is assigned.                                  | <b>all</b>      |
| <b>Interface</b>       | The name of the interface on which authentication is bypassed for a given MAC address. | <b>all</b>      |

## Sample Output

### show dot1x static-mac-address

```
user@switch> show dot1x static-mac-address

MAC address VLAN-Assignment Interface
00:00:00:11:22:33
```

|                   |            |            |
|-------------------|------------|------------|
| 00:00:00:00:12:12 |            | ge-0/0/3.0 |
| 00:00:00:02:34:56 | facilities | ge-0/0/1.0 |

#### show dot1x static-mac-address interface (Specific Interface)

```
user@switch> show dot1x static-mac-address interface ge-0/0/0.1
```

| MAC address       | VLAN-Assignment | Interface  |
|-------------------|-----------------|------------|
| 00:00:00:12:24:12 | support         | ge-0/0/1.0 |
| 00:00:00:72:30:58 | support         | ge-0/0/1.0 |

## show ethernet-switching interfaces

|                                 |                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show ethernet-switching interfaces<br><brief   detail   summary><br><interface <i>interface-name</i> >                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.1 for the QFX Series.<br>Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.                                                                                                                                                                                                                             |
| <b>Description</b>              | Display information about switched Ethernet interfaces.                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <p><b>none</b>—(Optional) Display brief information for Ethernet-switching interfaces.</p> <p><b>brief   detail   summary</b>—(Optional) Display the specified level of output.</p> <p><b>interface <i>interface-name</i></b>—(Optional) Display Ethernet-switching information for a specific interface.</p>                                                              |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Troubleshooting Ethernet Switching</i> <i>Understanding Bridging and VLANs</i></li> <li>• <i>Example: Setting Up Basic Bridging and a VLAN on the QFX Series</i></li> <li>• <i>Example: Setting Up Bridging with Multiple VLANs</i></li> <li>• <i>Understanding FCoE</i></li> <li>• <i>Interfaces Overview</i></li> </ul>      |
| <b>List of Sample Output</b>    | <a href="#">show ethernet-switching interfaces on page 350</a><br><a href="#">show ethernet-switching interfaces summary on page 351</a><br><a href="#">show ethernet-switching interfaces brief on page 351</a><br><a href="#">show ethernet-switching interfaces detail on page 351</a><br><a href="#">show ethernet-switching interfaces interface-name on page 352</a> |
| <b>Output Fields</b>            | Table 39 on page 349 lists the output fields for the <b>show ethernet-switching interfaces</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                            |

**Table 39: show ethernet-switching interfaces Output Fields**

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

Table 39: show ethernet-switching interfaces Output Fields (*continued*)

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

## Sample Output

### show ethernet-switching interfaces

```
user@switch> show ethernet-switching interfaces
```

```

Interface State VLAN members Blocking
xe-0/0/0.0 up T1122 unblocked
xe-0/0/1.0 down default - MAC limit exceeded
xe-0/0/2.0 down default - MAC move limit exceeded
xe-0/0/3.0 down default - Storm control in effect
xe-0/0/4.0 down default unblocked
xe-0/0/5.0 down default unblocked
xe-0/0/6.0 down default unblocked
xe-0/0/7.0 down default unblocked
xe-0/0/8.0 down default unblocked
xe-0/0/9.0 up T111 unblocked
xe-0/0/10.0 down default unblocked
xe-0/0/11.0 down default unblocked
xe-0/0/12.0 down default unblocked
xe-0/0/13.0 down default unblocked
xe-0/0/14.0 down default unblocked
xe-0/0/15.0 down default unblocked
xe-0/0/16.0 down default unblocked
xe-0/0/17.0 down default unblocked
xe-0/0/18.0 down default unblocked
xe-0/0/19.0 up T111 unblocked
xe-0/1/0.0 down default unblocked
xe-0/1/1.0 down default unblocked
xe-0/1/2.0 down default unblocked
xe-0/1/3.0 down default unblocked

```

**show ethernet-switching interfaces summary**

```

user@switch> show ethernet-switching interfaces summary
xe-0/0/0.0
xe-0/0/1.0
xe-0/0/2.0
xe-0/0/3.0
xe-0/0/8.0
xe-0/0/10.0
xe-0/0/11.0

```

**show ethernet-switching interfaces brief**

```

user@switch> show ethernet-switching interfaces brief
Interface State VLAN members Blocking
xe-0/0/0.0 down default unblocked
xe-0/0/1.0 down employee-vlan unblocked
xe-0/0/2.0 down employee-vlan unblocked
xe-0/0/3.0 down employee-vlan unblocked
xe-0/0/8.0 down employee-vlan unblocked
xe-0/0/10.0 down default unblocked
xe-0/0/11.0 down employee-vlan unblocked

```

**show ethernet-switching interfaces detail**

```

user@switch> show ethernet-switching interfaces detail
Interface: xe-0/0/0.0 Index: 65
State: down
VLANs:
 default untagged unblocked

Interface: xe-0/0/1.0 Index: 66
State: down
VLANs:
 employee-vlan untagged unblocked

Interface: xe-0/0/2.0 Index: 67
State: down
VLANs:
 employee-vlan untagged unblocked

Interface: xe-0/0/3.0 Index: 68
State: down
VLANs:
 employee-vlan untagged unblocked

Interface: xe-0/0/8.0 Index: 69
State: down
VLANs:
 employee-vlan untagged unblocked

Interface: xe-0/0/10.0 Index: 70
State: down
VLANs:
 default untagged unblocked

Interface: xe-0/0/11.0 Index: 71
State: down
VLANs:
 employee-vlan tagged unblocked

```

**show ethernet-switching interfaces interface-name**

```
user@switch> show ethernet-switching interfaces xe-0/0/0.0
Interface State VLAN members Blocking
xe-0/0/0.0 down default unblocked
```

## show lldp

**Syntax** `show lldp`  
`<detail>`

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

**Description** Display information about Link Layer Discovery Protocol (LLDP) and Link Level Discovery Protocol—Media Endpoint Discovery (LLDP-MED) configuration and capabilities on the switch. LLDP and LLDP-MED are used to learn about and to distribute device information on network links.



**NOTE:** LLDP-MED is not available on the QFX Series.

**Options** **none**—Display LLDP information for all interfaces.  
**detail**—(Optional) Display detailed LLDP information for all interfaces.

**Required Privilege Level** view

**Related Documentation**

- [Configuring LLDP \(CLI Procedure\) on page 104](#)
- [Configuring LLDP-MED \(CLI Procedure\) on page 107](#)
- [Understanding 802.1X and LLDP and LLDP-MED on page 101](#)
- [Configuring LLDP](#)
- [Understanding LLDP on page 5](#)

**List of Sample Output** [show lldp \(EX3200 switches\) on page 356](#)  
[show lldp \(EX4300 switches\) on page 356](#)  
[show lldp detail \(EX4300 switches\) on page 357](#)

**Output Fields** [Table 40 on page 353](#) lists the output fields for the **show lldp** command. Output fields are listed in the approximate order in which they appear.

**Table 40: show lldp Output Fields**

| Field Name | Field Description                                                                                                                                                                                                                                                                                                 | Level of Output |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| LLDP       | LLDP operating state. The state can be <b>enabled</b> or <b>disabled</b> .<br><br><b>NOTE:</b> If a VLAN that has been configured for untagged packets on an interface also has Layer 2 protocol tunneling (L2PT) enabled for LLDP, the LLDP operating state for that interface is displayed as <b>disabled</b> . | All levels      |

Table 40: show lldp Output Fields (*continued*)

| Field Name                    | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                | Level of Output |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Advertisement interval</b> | Frequency, in seconds, at which LLDP advertisements are sent.<br><br>This value is set by the <a href="#">advertisement-interval</a> configuration statement.                                                                                                                                                                                                                                                                                                    | All levels      |
| <b>Transmit delay</b>         | Seconds of delay before advertisements are sent to neighbors following a change to a TLV (type, length, or value) element in the LLDP protocol or to the state of the local system, such as a change in hostname or management address. You can set this value to reduce the delay in notifying neighbors of a change in the local system.<br><br>This value is set by the <i>transmit-delay</i> configuration statement.                                        | All levels      |
| <b>Hold timer</b>             | On EX4300 switches, the hold timer shows the length of time LLDP information is held before it is discarded. The hold timer value is equal to the advertisement interval multiplied by the hold multiplier.<br><br>On all other switches, the hold timer shows the value of the hold multiplier.<br><br>The hold multiplier value is set by the <a href="#">hold-multiplier</a> configuration statement.                                                         | All levels      |
| <b>Notification interval</b>  | How often LLDP trap notifications are generated as a result of LLDP database changes. If the interval value is 0, LLDP trap notifications on database changes are disabled.<br><br>This value is set by the <i>lldp-configuration-notification-interval</i> configuration statement.                                                                                                                                                                             | All levels      |
| <b>Config Trap Interval</b>   | How often LLDP trap notifications are generated as a result of changes in topology—for example, when an endpoint connects or disconnects. If the interval value is 0, LLDP trap notifications on topology changes are disabled.<br><br>This value is set by the <a href="#">ptopo-configuration-trap-interval</a> configuration statement.                                                                                                                       | All levels      |
| <b>Connection Hold timer</b>  | Amount of time the system maintains dynamic topology entries.<br><br>This value is set by the <a href="#">ptopo-configuration-maximum-hold-time</a> configuration statement.                                                                                                                                                                                                                                                                                     | All levels      |
| <b>LLDP-MED</b>               | LLDP-MED operating state. The state can be <b>Enabled</b> or <b>Disabled</b> .                                                                                                                                                                                                                                                                                                                                                                                   | All levels      |
| <b>MED fast start count</b>   | Number of advertisements sent from a switch to a device, such as a VoIP telephone, when the device is first detected by the switch. These increased advertisements are temporary. After a device and a switch exchange information and can communicate, advertisements are reduced to one per second.<br><br>This value is set by using the <i>fast-start</i> configuration statement.<br><br><b>NOTE:</b> <i>fast-start</i> is not available on the QFX Series. | All levels      |
| <b>Interface</b>              | Name of the interface for which LLDP configuration information is being reported.                                                                                                                                                                                                                                                                                                                                                                                | All levels      |
| <b>Parent Interface</b>       | Name of the aggregated Ethernet interface, if any, to which the interface belongs.                                                                                                                                                                                                                                                                                                                                                                               | All levels      |

Table 40: show lldp Output Fields (*continued*)

| Field Name                       | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Level of Output |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>LLDP</b>                      | LLDP operating state. The state can be <b>Enabled</b> or <b>Disabled</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | All levels      |
| <b>Power Negotiation</b>         | LLDP power negotiation operating state. The state can be <b>Enabled</b> or <b>Disabled</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | All levels      |
| <b>Neighbor count</b>            | Total number of new LLDP neighbors detected since the last switch reboot.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>detail</b>   |
| <b>Interface</b>                 | Name of the interface that is advertising VLAN information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | All levels      |
| <b>Vlan-id</b>                   | VLAN tag associated with the interface sending LLDP frames. If the interface is not a member of a VLAN, the VLAN ID is advertised as 0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>detail</b>   |
| <b>Vlan-name</b>                 | VLAN name associated with the VLAN ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <b>detail</b>   |
| <b>LLDP basic TLVs supported</b> | Basic TLVs supported on the switch: <ul style="list-style-type: none"> <li>• <b>Chassis identifier</b>—TLV that advertises the MAC address associated with the local system.</li> <li>• <b>Port identifier</b>—TLV that advertises the port identification for the specified port in the local system.</li> <li>• <b>Port description</b>—Interface name for the port.</li> <li>• <b>System name</b>—TLV that advertises the user-configured name of the local system.</li> <li>• <b>System description</b>—TLV that advertises the system description containing information about the software and current image running on the system. This information is taken from the software and is not configurable.</li> <li>• <b>System capabilities</b>—TLV that advertises the primary functions performed by the system—for example, bridge or router.</li> <li>• <b>Management address</b>—TLV that advertises the IP management address of the local system.</li> </ul> | <b>detail</b>   |
| <b>Supported LLDP 802 TLVs</b>   | 802.3 TLVs supported on the switch: <ul style="list-style-type: none"> <li>• <b>MAC/PHY configuration status</b>—TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information is based on the physical interface structure and is not configurable.</li> <li>• <b>Power via MDI</b>—TLV that advertises MDI power support, PSE power pair, and power class information.</li> <li>• <b>Link aggregation</b>—TLV that advertises if the interface is aggregated and its aggregated interface ID.</li> <li>• <b>Maximum frame size</b>—TLV that advertises the maximum transmission unit (MTU) of the interface sending LLDP frames.</li> <li>• <b>Port VLAN tag</b>—TLV that advertises the VLAN tag configured on the interface.</li> <li>• <b>Port VLAN name</b>—TLV that advertises the VLAN name configured on the interface.</li> </ul>                                                     | <b>detail</b>   |

Table 40: show lldp Output Fields (*continued*)

| Field Name                     | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Level of Output |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Supported LLDP MED TLVs</b> | <p>LLDP-MED TLVs supported on the switch:</p> <ul style="list-style-type: none"> <li>• <b>LLDP MED capabilities</b>—TLV that advertises the primary function of the port. The capabilities values range from 0 through 15: <ul style="list-style-type: none"> <li>• 0—Capabilities</li> <li>• 1—Network Policy</li> <li>• 2—Location Identification</li> <li>• 3—Extended Power via MDI-PSE</li> <li>• 4—Inventory</li> <li>• 5–15—Reserved</li> </ul> </li> <li>• <b>Network policy</b>—TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types—such as voice or streaming video—802.1Q VLAN tagging, and 802.1p priority bits and DiffServ code points.</li> <li>• <b>Endpoint location</b>—TLV that advertises the physical location of the endpoint.</li> <li>• <b>Extended power Via MDI</b>—TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.</li> </ul> | <b>detail</b>   |

## Sample Output

### show lldp (EX3200 switches)

```

user@switch> show lldp
LLDP : Enabled
Advertisement interval : 30 seconds
Transmit delay : 2 seconds
Hold timer : 4 seconds
Notification interval : 0 Second(s)
Config Trap Interval : 0 seconds
Connection Hold timer : 300 seconds

LLDP MED : Disabled
MED fast start count : 3 Packets

```

|           |                  |         |          |                   |
|-----------|------------------|---------|----------|-------------------|
| Interface | Parent Interface | LLDP    | LLDP-MED | Power Negotiation |
| all       | -                | Enabled | Enabled  | Enabled           |

### show lldp (EX4300 switches)

```

user@switch> show lldp
LLDP : Enabled
Advertisement interval : 30 seconds
Transmit delay : 2 seconds
Hold timer : 120 seconds
Notification interval : 0 Second(s)
Config Trap Interval : 0 seconds
Connection Hold timer : 300 seconds

LLDP MED : Disabled
MED fast start count : 3 Packets

```

| Interface | Parent Interface | LLDP    | LLDP-MED | Power Negotiation |
|-----------|------------------|---------|----------|-------------------|
| all       | -                | Enabled | Enabled  | Enabled           |

### show lldp detail (EX4300 switches)

```

user@switch> show lldp detail
LLDP : Enabled
Advertisement interval : 30 seconds
Transmit delay : 2 seconds
Hold timer : 120 seconds
Notification interval : 0 Second(s)
Config Trap Interval : 0 seconds
Connection Hold timer : 300 seconds

LLDP MED : Disabled
MED fast start count : 3 Packets

```

| Interface      | Parent Interface | LLDP    | LLDP-MED | Power Negotiation |
|----------------|------------------|---------|----------|-------------------|
| Neighbor count |                  |         |          |                   |
| all            | -                | Enabled | Enabled  | Enabled           |
| 8              |                  |         |          |                   |

| Interface  | Parent Interface | Vlan-id | Vlan-name |
|------------|------------------|---------|-----------|
| xe-3/0/0.0 | ae31.0           | 100     | v100      |
| xe-3/0/0.0 | ae31.0           | 101     | v101      |
| xe-3/0/0.0 | ae31.0           | 4000    | v4000     |
| xe-3/0/1.0 | ae31.0           | 100     | v100      |
| xe-3/0/1.0 | ae31.0           | 101     | v101      |
| xe-3/0/1.0 | ae31.0           | 4000    | v4000     |
| xe-3/0/2.0 | ae31.0           | 100     | v100      |
| xe-3/0/2.0 | ae31.0           | 101     | v101      |
| xe-3/0/2.0 | ae31.0           | 4000    | v4000     |

#### LLDP basic TLVs supported:

Chassis identifier, Port identifier, Port description, System name, System description, System capabilities, Management address.

#### Supported LLDP 802 TLVs:

MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum frame size, Port VLAN tag, Port VLAN name.

#### Supported LLDP MED TLVs:

LLDP MED capabilities, Network policy, Endpoint location, Extended power Via MDI.

## show lldp local-information

|                                 |                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show lldp local-information                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 11.1 for the QFX Series.<br>Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.                                                                                                                                             |
| <b>Description</b>              | Display the information that the switch provides in Link Layer Discovery Protocol (LLDP) advertisements to its neighbors.                                                                                                                                                                                                                                        |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring LLDP (CLI Procedure) on page 104</a></li> <li>• <a href="#">Understanding 802.1X and LLDP and LLDP-MED on page 101</a></li> <li>• <a href="#">management-address on page 271</a></li> <li>• <a href="#">Configuring LLDP</a></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show lldp local-information (EX Series Switch) on page 359</a>                                                                                                                                                                                                                                                                                       |
| <b>Output Fields</b>            | <a href="#">Table 41 on page 358</a> lists the output fields for the <b>show lldp local-information</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                         |

**Table 41: show lldp local-information Output Fields**

| Field Name                            | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>LLDP Local Information details</b> | <p>Information about the local system (the switch):</p> <ul style="list-style-type: none"> <li>• <b>Chassis ID</b>—MAC address associated with the switch.</li> <li>• <b>System name</b>—User-configured name of the switch.</li> <li>• <b>System descr</b>—System description containing information about the switch model and the current software image running on the switch. This information is taken from the software and is not configurable.</li> </ul>                                                                                                                                                                                                                 |
| <b>System Capabilities</b>            | Capabilities (such as <b>bridge</b> or <b>router</b> ) that are supported or enabled on the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Management Information</b>         | <p>Details of the management information: <b>Port Name</b>, <b>Port Address</b> (such as 10.204.34.35), <b>Address Type</b> (such as ipv4 or ipv6), <b>Port ID</b> (SNMP interface index), <b>Port ID Subtype</b>, and <b>Port Subtype</b>.</p> <p>The <b>Port Subtype</b> displays:</p> <ul style="list-style-type: none"> <li>• <b>ifindex(2)</b>—IP address of the switch's management Ethernet interface (<b>me0</b>) or virtual management Ethernet (<b>VME</b>) interface address (for a virtual chassis) is used to manage the switch.</li> <li>• <b>unknown(1)</b>—IP management address has been configured with set <b>protocols lldp management-address</b>.</li> </ul> |

Table 41: show lldp local-information Output Fields (*continued*)

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

## Sample Output

### show lldp local-information (EX Series Switch)

```
user@switch> show lldp local-information
```

#### LLDP Local Information details

```
Chassis ID : 00:1d:b5:aa:b9:f0
System name : switch
System descr : Juniper Networks, Inc. ex8208 , version 10.4I0 [builder] Build
 date: 2010-11-17 12:38:30 UTC
```

#### System Capabilities

```
Supported : Bridge Router
Enabled : Bridge Router
```

#### Management Information

```
Port Name : -
Port Address : 10.93.54.6
Address Type : IPv4
Port ID : 34
Port ID Subtype : local(7)
Port Subtype : ifIndex(2)
```

| Interface name | Parent Interface | SNMP Index | Interface description | Status | Tunneling |
|----------------|------------------|------------|-----------------------|--------|-----------|
| me0.0          | -                | 34         | -                     | Down   | Disabled  |
| xe-3/0/0.0     | ae31.0           | 769        | xe-3/0/0.0            | Up     | Disabled  |
| xe-3/0/1.0     | ae31.0           | 770        | xe-3/0/1.0            | Up     | Disabled  |
| xe-3/0/2.0     | ae31.0           | 771        | xe-3/0/2.0            | Up     | Disabled  |
| xe-3/0/3.0     | ae31.0           | 772        | xe-3/0/3.0            | Up     | Disabled  |
| xe-3/0/4.0     | ae31.0           | 577        | xe-3/0/4.0            | Up     | Disabled  |
| xe-3/0/5.0     | ae31.0           | 578        | xe-3/0/5.0            | Up     | Disabled  |
| xe-3/0/6.0     | ae31.0           | 579        | xe-3/0/6.0            | Up     | Disabled  |
| xe-3/0/7.0     | ae31.0           | 581        | xe-3/0/7.0            | Up     | Disabled  |

## show lldp neighbors

**Syntax** <show lldp *neighbors*>  
<interface *interface-ids*>

**Release Information** Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description** Display learned information about Link Layer Discovery Protocol (LLDP) on all neighboring interfaces or on selected interfaces.

**Options** **none**—Display learned LLDP information on all neighboring interfaces and devices.

**interface *interface-ids***—(Optional) Display learned LLDP information on the selected interfaces or devices.



**NOTE:** When a port with DCBX enabled begins to exchange type, length, and value (TLV) entries, optional LLDP TLVs on that port are not advertised to neighbors in order to interoperate with a wider variety of converged network adapters (CNAs). As a result, information for those ports will not be listed in the output for this command.

**Required Privilege Level** view

**Related Documentation**

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

**List of Sample Output** [show lldp neighbors on page 362](#)  
[show lldp neighbors interface on page 363](#)

**Output Fields** [Table 42 on page 360](#) lists the output fields for the **show lldp neighbors** command. Output fields are listed in the approximate order in which they appear.

**Table 42: show lldp neighbors Output Fields**

| Field Name       | Field Description                                                                                        |
|------------------|----------------------------------------------------------------------------------------------------------|
| Local Interface  | List of local interfaces for which neighbor information is available.                                    |
| Parent Interface | List of aggregated Ethernet interfaces, if any, to which the local interfaces belong.                    |
| Chassis ID       | List of chassis identifiers for neighbors.                                                               |
| Port info        | List of port information gathered from neighbors. This could be the port identifier or port description. |
| System name      | List of system names gathered from neighbors.                                                            |

Table 42: show lldp neighbors Output Fields (*continued*)

| Field Name                       | Field Description                                                                                                                                                                                                                                                     |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>LLDP Neighbor Information</b> | Information about both the local system (the switch) and a neighbor system on the interface (appears when the <b>interface</b> option is used).                                                                                                                       |
| <b>Local Information</b>         | Information about the local system (appears when the <b>interface</b> option is used).                                                                                                                                                                                |
| <b>Index</b>                     | Local interface index (appears when the <b>interface</b> option is used).                                                                                                                                                                                             |
| <b>Time to live</b>              | Number of seconds for which this information is valid (appears when the <b>interface</b> option is used).                                                                                                                                                             |
| <b>Time mark</b>                 | Date and timestamp of information (appears when the <b>interface</b> option is used).                                                                                                                                                                                 |
| <b>Local Interface</b>           | Name of the local physical interface (appears when the <b>interface</b> option is used).                                                                                                                                                                              |
| <b>Parent Interface</b>          | Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the <b>interface</b> option is used).                                                                                                                                 |
| <b>Local Port ID</b>             | Local interface SNMP index (appears when the <b>interface</b> option is used).                                                                                                                                                                                        |
| <b>Ageout Count</b>              | Number of times the complete set of information advertised by the neighbor has been deleted from LLDP neighbor information maintained by the local system because the information timeliness interval has expired (appears when the <b>interface</b> option is used). |
| <b>Neighbor Information</b>      | Information about a neighbor system on the interface (appears when the <b>interface</b> option is used).                                                                                                                                                              |
| <b>Chassis type</b>              | Type of chassis identifier supplied, such as <b>MAC address</b> (appears when the <b>interface</b> option is used).                                                                                                                                                   |
| <b>Chassis ID</b>                | Chassis identifier of the chassis type listed (appears when the <b>interface</b> option is used).                                                                                                                                                                     |
| <b>Port type</b>                 | Type of port identifier supplied, such as <b>locally assigned</b> (appears when the <b>interface</b> option is used).                                                                                                                                                 |
| <b>Port ID</b>                   | Port identifier of the port type listed (appears when the <b>interface</b> option is used).                                                                                                                                                                           |
| <b>Port description</b>          | Port description (appears when the <b>interface</b> option is used).                                                                                                                                                                                                  |
| <b>System name</b>               | Name supplied by the system on the interface (appears when the <b>interface</b> option is used).                                                                                                                                                                      |
| <b>System Description</b>        | Description supplied by the system on the interface (appears when the <b>interface</b> option is used).                                                                                                                                                               |

Table 42: show lldp neighbors Output Fields (*continued*)

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

## Sample Output

### show lldp neighbors

```
user@switch> show lldp neighbors
```

| Local Interface | Parent Interface | Chassis Id        | Port info  | System Name |
|-----------------|------------------|-------------------|------------|-------------|
| xe-3/0/4.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/0/0.0 | newyork31   |
| xe-3/0/5.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/0/1.0 | newyork31   |
| xe-3/0/6.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/0/2.0 | newyork31   |
| xe-3/0/7.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/0/3.0 | newyork31   |
| xe-3/0/0.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/1/0.0 | newyork31   |
| xe-3/0/1.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/1/1.0 | newyork31   |
| xe-3/0/2.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/1/2.0 | newyork31   |
| xe-3/0/3.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/1/3.0 | newyork31   |

### show lldp neighbors interface

```
user@switch> show lldp neighbors interface ge-0/0/2
```

#### LLDP Neighbor Information:

##### Local Information:

```
Index: 1 Time to live: 240 Time mark: Wed Dec 1 10:23:24 2010 Age: 29 secs
Local Interface : ge-0/0/2.0
Parent Interface : -
Local Port ID : 507
Ageout Count : 0
```

##### Neighbour Information:

```
Chassis type : Mac address
Chassis ID : 00:1f:12:38:7f:c0
Port type : Locally assigned
Port ID : 507
Port description : ge-0/0/2.0
System name : bng-148p5-dev
```

```
System Description : Juniper Networks, Inc. ex4200-48p , version 10.4IO Build
date: 2010-11-30 09:32:17 UTC
```

##### System capabilities

```
Supported : Bridge Router
Enabled : Bridge Router
```

##### Management Info

```
Type : IPv4
Address : 10.204.96.235
Port ID : 34
Subtype : 1
Interface Subtype : ifIndex(2)
OID : 1.3.6.1.2.1.31.1.1.1.1.34
```

```
Media endpoint class: Network Connectivity
```

##### Organization Info

```
OUI : 0.12.f
Subtype : 1
Index : 1
Info : 22A8360000
```

##### Organization Info

```
OUI : 0.12.f
Subtype : 2
Index : 2
Info : 030100
```

## show lldp statistics

|                                 |                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show lldp statistics</code><br><code>&lt;interface <i>interface-ids</i>&gt;</code>                                                                                          |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.1 for the QFX Series.<br>Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.                                    |
| <b>Description</b>              | Display LLDP statistics on all or selected interfaces.                                                                                                                            |
| <b>Options</b>                  | <b>none</b> —Display LLDP statistics on all interfaces and devices.<br><br><b>interface <i>interface-ids</i></b> —(Optional) Display LLDP statistics on the selected devices.     |
| <b>Required Privilege Level</b> | view                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring LLDP</a></li> <li>• <a href="#">Understanding LLDP on page 5</a></li> </ul>                                      |
| <b>List of Sample Output</b>    | <a href="#">show lldp statistics on page 364</a>                                                                                                                                  |
| <b>Output Fields</b>            | <a href="#">Table 43 on page 364</a> lists the output fields for the <b>show lldp statistics</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 43: show lldp statistics Output Fields**

| Field Name            | Field Description                                                | Level of Output |
|-----------------------|------------------------------------------------------------------|-----------------|
| <b>Interface</b>      | Name of an interface.                                            | All levels      |
| <b>Received</b>       | Total number of LLDP frames received on an interface.            | All levels      |
| <b>Unknown-TLVs</b>   | Number of unrecognized LLDP TLVs received on an interface.       | All levels      |
| <b>With Errors</b>    | Number of LLDP frames received that contain errors.              | All levels      |
| <b>Discarded TLVs</b> | Number of LLDP TLVs received and then discarded on an interface. | All levels      |
| <b>Transmitted</b>    | Total number of LLDP frames transmitted on an interface.         | All levels      |
| <b>Untransmitted</b>  | Total number of LLDP frames not transmitted on an interface.     | All levels      |

## Sample Output

### show lldp statistics

```
user@switch> show lldp statistics
```

```
Interface Received Unknown TLVs With Errors Discarded TLVs Transmitted
Untransmitted
```

|            |      |   |   |   |      |   |
|------------|------|---|---|---|------|---|
| me0.0      | 0    | 0 | 0 | 0 | 8003 | 0 |
| ge-0/0/0.0 | 8002 | 0 | 0 | 0 | 8003 | 0 |
| ge-0/0/1.0 | 8002 | 0 | 0 | 0 | 8003 | 0 |

## show network-access aaa statistics accounting

|                                 |                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show network-access aaa statistics accounting</b>                                                                                                                                                                    |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 11.1 for QFX Series switches.                                                                              |
| <b>Description</b>              | Display authentication, authorization, and accounting (AAA) accounting statistics.                                                                                                                                      |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">accounting-server on page 234</a></li> <li>• <a href="#">accounting-stop-on-access-deny on page 235</a></li> <li>• <i>Configuring RADIUS Accounting</i></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show network-access aaa statistics accounting on page 366</a>                                                                                                                                               |
| <b>Output Fields</b>            | <a href="#">Table 44 on page 366</a> lists the output fields for the <b>show network-access aaa statistics accounting</b> command. Output fields are listed in the approximate order in which they appear.              |

**Table 44: show network-access aaa statistics accounting Output Fields**

| Field Name                   | Field Description                                                                                       |
|------------------------------|---------------------------------------------------------------------------------------------------------|
| Requests received            | The number of accounting-request packets sent from a switch to a RADIUS accounting server.              |
| Accounting Response failures | The number of accounting-response failure packets sent from the RADIUS accounting server to the switch. |
| Accounting Response Success  | The number of accounting-response success packets sent from the RADIUS accounting server to the switch. |
| Requests timedout            | The number of requests-timedout packets sent from the RADIUS accounting server to the switch.           |

## Sample Output

### show network-access aaa statistics accounting

```

user@switch> show network-access aaa statistics accounting
Accounting module statistics
 Requests received: 1
 Accounting Response failures: 0
 Accounting Response Success: 1
 Requests timedout: 0

```

## show network-access aaa statistics authentication

|                                 |                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show network-access aaa statistics authentication</b>                                                                                                                                               |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 11.1 for QFX Series switches.                                                             |
| <b>Description</b>              | Display authentication, authorization, and accounting (AAA) authentication statistics.                                                                                                                 |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">authentication-server on page 242</a></li> <li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show network-access aaa statistics authentication on page 367</a><br><a href="#">show network-access aaa statistics authentication (in QFX Series Switches) on page 367</a>                |
| <b>Output Fields</b>            | Table 45 on page 367 lists the output fields for the <b>show network-access aaa statistics authentication</b> command. Output fields are listed in the approximate order in which they appear.         |

**Table 45: show network-access aaa statistics authentication Output Fields**

| Field Name               | Field Description                                                   |
|--------------------------|---------------------------------------------------------------------|
| <b>Requests received</b> | The number of authentication requests received by the switch.       |
| <b>Accepts</b>           | The number of authentication accepts received by the RADIUS server. |
| <b>Rejects</b>           | The number authentication rejects sent by the RADIUS server.        |
| <b>Challenges</b>        | The number of authentication challenges sent by the RADIUS server.  |

## Sample Output

### show network-access aaa statistics authentication

```

user@switch> show network-access aaa statistics authentication
Authentication module statistics
Requests received: 2
Accepts: 1
Rejects: 0
Challenges: 1

```

### show network-access aaa statistics authentication (in QFX Series Switches)

```

user@lf0> show network-access aaa statistics authentication
Authentication module statistics
Requests received: 2
Accepts: 1

```

Rejects: 0  
Challenges: 1

## show network-access aaa statistics dynamic-requests

|                                 |                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show network-access aaa statistics dynamic-requests;</b>                                                                                                                                                      |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 11.1 for QFX Series switches.                                                                       |
| <b>Description</b>              | Display authentication, authorization, and accounting (AAA) authentication statistics for disconnects.                                                                                                           |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">authentication-server on page 242</a></li> <li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to a Switch on page 25</a></li> </ul>           |
| <b>List of Sample Output</b>    | <a href="#">show network-access aaa statistics authentication on page 369</a>                                                                                                                                    |
| <b>Output Fields</b>            | <a href="#">Table 46 on page 369</a> lists the output fields for the <b>show network-access aaa statistics dynamic-requests</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 46: show network-access aaa statistics dynamic-requests Output Fields**

| Field Name                      | Field Description                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------|
| <b>Requests received</b>        | The number of dynamic requests received by the RADIUS server.                                  |
| <b>Processed successfully</b>   | The number of dynamic requests successfully processed by the RADIUS server.                    |
| <b>Errors during processing</b> | The number of errors that occurred while the RADIUS server was processing the dynamic request. |
| <b>Silently dropped</b>         | The number of silently dropped requests.                                                       |

## Sample Output

### show network-access aaa statistics authentication

```

user@switch> show network-access aaa statistics dynamic-requests
Dynamic-requests module statistics
 Requests received: 0
 Processed successfully: 0
 Errors during processing: 0
 Silently dropped: 0

```

## show route instance

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show route instance<br><brief   detail   summary><br><instance-name><br><operational>                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.3 for the QFX Series.<br>Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | (QFabric systems only) Display routing instance information.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                  | <p><b>none</b>—(Same as <b>brief</b>) Display standard information about all routing instances.</p> <p><b>brief   detail   summary</b>—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to <b>brief</b>. (These options are not available with the <b>operational</b> keyword.)</p> <p><b>instance-name</b>—(Optional) Display information for a specified routing instance.</p> <p><b>operational</b>—(Optional) Display operational routing instances.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>List of Sample Output</b>    | <a href="#">show route instance on page 371</a><br><a href="#">show route instance detail on page 371</a><br><a href="#">show route instance operational on page 372</a><br><a href="#">show route instance summary on page 372</a>                                                                                                                                                                                                                                                                                        |
| <b>Output Fields</b>            | Table 47 on page 370 lists the output fields for the <b>show route instance</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                           |

Table 47: show route instance Output Fields

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

Table 47: show route instance Output Fields (*continued*)

| Field Name             | Field Description                               | Level of Output           |
|------------------------|-------------------------------------------------|---------------------------|
| Primary RIB            | Primary table for this routing instance.        | <b>brief none summary</b> |
| Active/holddown/hidden | Number of active, hold-down, and hidden routes. | All levels                |

## Sample Output

### show route instance

```

user@switch> show route instance
Instance Type
Primary RIB
master forwarding
inet.0 4/0/1

__juniper_private1__ forwarding
__juniper_private1__.inet.0 1/0/3

__juniper_private2__ forwarding
__juniper_private2__.inet.0 0/0/1

__juniper_private3__ forwarding
__juniper_private3__.inet.0 1/0/2

__juniper_private4__ forwarding
__juniper_private4__.inet.0 4/0/2

__master.anon__ forwarding

r1 virtual-router

r2 virtual-router

```

### show route instance detail

```

user@switch> show route instance detail
master:
 Router ID: 3.3.3.7
 Type: forwarding State: Active
 Tables:
 inet.0 : 5 routes (4 active, 0 holddown, 1 hidden)

__juniper_private1__:
 Router ID: 0.0.0.0
 Type: forwarding State: Active
 Interfaces:
 lo0.16385
 bme0.0
 Tables:
 __juniper_private1__.inet.0: 6 routes (1 active, 0 holddown, 3 hidden)

__juniper_private2__:
 Router ID: 0.0.0.0
 Type: forwarding State: Active
 Interfaces:
 lo0.16384

```

```

Tables:
 __juniper_private2__.inet.0: 1 routes (0 active, 0 holddown, 1 hidden)

__juniper_private3__:
Router ID: 0.0.0.0
Type: forwarding State: Active
Interfaces:
 bme0.1
Tables:
 __juniper_private3__.inet.0: 4 routes (1 active, 0 holddown, 2 hidden)

__juniper_private4__:
Router ID: 0.0.0.0
Type: forwarding State: Active
Interfaces:
 bme0.2
Tables:
 __juniper_private4__.inet.0: 8 routes (4 active, 0 holddown, 2 hidden)

__master.anon__:
Router ID: 0.0.0.0
Type: forwarding State: Active

r1:
Router ID: 0.0.0.0
Type: virtual-router State: Active
Interfaces:
 xe-0/0/0.0

r2:
Router ID: 0.0.0.0
Type: virtual-router State: Active
Interfaces:
 xe-0/0/3.0

```

### show route instance operational

```

user@switch> show route instance operational
Operational Routing Instances:

__juniper_private1__
__juniper_private2__
__juniper_private3__
__juniper_private4__
r1---qfabric
r2---qfabric
master

```

### show route instance summary

```

user@switch> show route instance summary

```

| Instance             | Type       | Primary RIB                 | Active/holddown/hidden |
|----------------------|------------|-----------------------------|------------------------|
| master               | forwarding | inet.0                      | 4/0/1                  |
| __juniper_private1__ | forwarding | __juniper_private1__.inet.0 | 1/0/3                  |
| __juniper_private2__ | forwarding | __juniper_private2__.inet.0 | 0/0/1                  |

```
__juniper_private3__ forwarding
__juniper_private3__.inet.0 1/0/2

__juniper_private4__ forwarding
__juniper_private4__.inet.0 4/0/2

__master.anon__ forwarding

r1 virtual-router
r2 virtual-router
```

## show snmp statistics

|                                 |                                                                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show snmp statistics                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | <p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> |
| <b>Description</b>              | Display statistics about Simple Network Management Protocol (SNMP) packets sent and received by the router or switch.                                                                                                                                                                 |
| <b>Options</b>                  | This command has no options.                                                                                                                                                                                                                                                          |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><i>clear snmp statistics</i></li> </ul>                                                                                                                                                                                                        |
| <b>List of Sample Output</b>    | <a href="#">show snmp statistics on page 377</a>                                                                                                                                                                                                                                      |
| <b>Output Fields</b>            | <p><a href="#">Table 48 on page 374</a> describes the output fields for the <b>show snmp statistics</b> command.</p> <p>Output fields are listed in the approximate order in which they appear.</p>                                                                                   |

**Table 48: show snmp statistics Output Fields**

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

Table 48: show snmp statistics Output Fields (*continued*)

| Field Name        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Input (continued) | <ul style="list-style-type: none"> <li>• <b>General errors—(snmpInGenErrs)</b> Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <b>genErr</b>.</li> <li>• <b>Total requests varbinds—(snmpInTotalReqVars)</b> Total number of MIB objects retrieved successfully by the SNMP entity as a result of receiving valid SNMP <b>GetRequest</b> and <b>GetNext</b> PDUs.</li> <li>• <b>Total set varbinds—(snmpInSetVars)</b> Total number of MIB objects modified successfully by the SNMP entity as a result of receiving valid SNMP <b>SetRequest</b> PDUs.</li> <li>• <b>Get requests—(snmpInGetRequests)</b> Total number of SNMP <b>GetRequest</b> PDUs that have been accepted and processed by the SNMP entity.</li> <li>• <b>Get nexts—(snmpInGetNexts)</b> Total number of SNMP <b>GetNext</b> PDUs that have been accepted and processed by the SNMP entity.</li> <li>• <b>Set requests—(snmpInSetRequests)</b> Total number of SNMP <b>SetRequest</b> PDUs that have been accepted and processed by the SNMP entity.</li> <li>• <b>Get responses—(snmpInGetResponses)</b> Total number of SNMP <b>GetResponse</b> PDUs that have been accepted and processed by the SNMP entity.</li> <li>• <b>Traps—(snmpInTraps)</b> Total number of SNMP traps generated by the SNMP entity.</li> <li>• <b>Silent drops—(snmpSilentDrops)</b> Total number of <b>GetRequest</b>, <b>GetNextRequest</b>, <b>GetBulkRequest</b>, <b>SetRequests</b>, and <b>InformRequest</b> PDUs delivered to the SNMP entity that were silently dropped because the size of a reply containing an alternate response PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the requests.</li> <li>• <b>Proxy drops—(snmpProxyDrops)</b> Total number of <b>GetRequest</b>, <b>GetNextRequest</b>, <b>GetBulkRequest</b>, <b>SetRequests</b>, and <b>InformRequest</b> PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in such a way (other than a timeout) that no response PDU could be returned.</li> <li>• <b>Commit pending drops</b>—Number of SNMP packets for <b>Set</b> requests dropped because of a previous pending SNMP <b>Set</b> request on the committed configuration.</li> <li>• <b>Throttle drops</b>—Number of SNMP packets for any requests dropped reaching the throttle limit.</li> </ul> |

Table 48: show snmp statistics Output Fields (*continued*)

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

Table 48: show snmp statistics Output Fields (*continued*)

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

## Sample Output

### show snmp statistics

```

user@host> show snmp statistics
SNMP statistics:
 Input:
 Packets: 246213, Bad versions: 12, Bad community names: 12,
 Bad community uses: 0, ASN parse errors: 96,
 Too big: 0, No such names: 0, Bad values: 0,
 Read onlys: 0, General errors: 0,
 Total request varbinds: 227084, Total set varbinds: 67,
 Get requests: 44942, Get nexts: 190371, Set requests: 10712,
 Get responses: 0, Traps: 0,
 Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
 Throttle drops: 0,
 V3 Input:
 Unknown security models: 0, Invalid messages: 0
 Unknown pdu handlers: 0, Unavailable contexts: 0
 Unknown contexts: 0, Unsupported security levels: 1
 Not in time windows: 0, Unknown user names: 0
 Unknown engine ids: 44, Wrong digests: 23, Decryption errors: 0
 Output:
 Packets: 246093, Too big: 0, No such names: 31561,
 Bad values: 0, General errors: 2,
 Get requests: 0, Get nexts: 0, Set requests: 0,
 Get responses: 246025, Traps: 0

```

## ssh

**List of Syntax** [Syntax on page 378](#)  
[Syntax \(EX Series Switch and the QFX Series\) on page 378](#)

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

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

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

**Description** Use the SSH program to open a connection between a local router or switch and a remote system and execute commands on the remote system. You can issue the **ssh** command from the Junos OS CLI to log in to a remote system or from a remote system to log in to the local router or switch. When executing this command, you include one or more CLI commands by enclosing them in quotation marks and separating the commands with semicolons:

```
ssh address 'cli-command1 ; cli-command2 '
```

**Options** **host**—Name or address of the remote system.

**bypass-routing**—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

**inet | inet6**—(Optional) Create an IPv4 or IPv6 connection, respectively.

**interface interface-name**—(Optional) Interface name for the SSH session. (This option does not work when **default-address-selection** is configured at the **[edit system]** hierarchy level, because this configuration uses the loopback interface as the source address for all locally generated IP packets.)

**logical-system logical-system-name**—(Optional) Name of a particular logical system for the SSH attempt.

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

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

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

**Additional Information** To configure an SSH (version 1) key for your user account, include the **authentication ssh-rsa** statement at the **[edit system login user *user-name*]** hierarchy level. To configure an SSH (version 2) key for your user account, include the **authentication dsa-rsa** statement at the **[edit system login user *user-name*]** hierarchy level.

You can limit the number of times a user can attempt to enter a password while logging in through SSH. To specify the number of times a user can attempt to enter a password to log in through SSH, include the **retry-options** statement at the **[edit system login]** hierarchy level. For details, see the .

**Required Privilege Level** network

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

**List of Sample Output** [ssh on page 379](#)

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

## Sample Output

ssh

```
user@switch> ssh cree
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes

Host ?cree' added to the list of known hosts.
boojun@cree's password:
Last login: Sun Jun 21 10:43:42 1998 from junos-router
% ...
```

