



Access Control and Authentication Feature Guide for EX2300, EX3400, and EX4300 Switches

Release

14.1x53 (THIS IS A !5.1 page, with BAD release: saving
into 13.2X51)



Modified: 2017-01-10

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.

Access Control and Authentication Feature Guide for EX2300, EX3400, and EX4300 Switches
Release 14.1x53 (THIS IS A !5.1 page, with BAD release: saving into 13.2X51)
Copyright © 2016, 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	xiii
	Documentation and Release Notes	xiii
	Supported Platforms	xiii
	Using the Examples in This Manual	xiii
	Merging a Full Example	xiv
	Merging a Snippet	xiv
	Documentation Conventions	xv
	Documentation Feedback	xvii
	Requesting Technical Support	xvii
	Self-Help Online Tools and Resources	xvii
	Opening a Case with JTAC	xviii
Chapter 1	Understanding Access Control and Authentication	19
	Understanding Authentication on EX Series Switches	19
	Sample Authentication Topology	19
	802.1X Authentication	20
	MAC RADIUS Authentication	22
	Captive Portal Authentication	22
	Static MAC Bypass of Authentication	23
	Fallback of Authentication Methods	24
	Authentication Process Flow for EX Series Switches	25
	Understanding Authentication Session Timeout	27
	Understanding Server Fail Fallback and Authentication on EX Series Switches	28
Chapter 2	Configuring 802.1X Authentication to Control Network Access	29
	802.1X for EX Series Switches Overview	30
	How 802.1X Authentication Works	30
	802.1X Features Overview	30
	Configuring 802.1X Interface Settings (CLI Procedure)	32
	Specifying RADIUS Server Connections on an EX Series Switch (CLI Procedure)	34
	Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch	35
	Configuring Flexible Authentication Order	39

	Configuring RADIUS Server Fail Fallback (CLI Procedure)	42
	Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant	
	Configurations on an EX Series Switch	44
	Understanding Dynamic Filters Based on RADIUS Attributes	49
	Juniper-Switching-Filter VSA Match Conditions and Actions	50
	Filtering 802.1X Supplicants by Using RADIUS Server Attributes	52
	Configuring Firewall Filters on the RADIUS Server	52
	Applying a Locally Configured Firewall Filter from the RADIUS Server	55
	Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by	
	Using RADIUS Server Attributes on an EX Series Switch	56
	Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled	
	for 802.1X or MAC RADIUS Authentication	62
	Example: Configuring 802.1X Authentication Options When the RADIUS Server	
	Is Unavailable to an EX Series Switch	67
	Understanding Guest VLANs for 802.1X on EX Series Switches	73
	Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access	
	to Corporate Visitors on an EX Series Switch	73
	Understanding 802.1X and RADIUS Accounting on EX Series Switches	78
	RADIUS Accounting Process	78
	Supported RADIUS Attributes	79
	Understanding RADIUS-Initiated Changes to an Authorized User Session	80
	Disconnect Messages	80
	Change of Authorization Messages	81
	Error-Cause Codes	81
	Configuring 802.1X RADIUS Accounting (CLI Procedure)	83
	Understanding Dynamic VLAN Assignment Using RADIUS Attributes	84
	Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS	
	Authentication and Odyssey Access Clients	85
	Controlling Authentication Session Timeouts (CLI Procedure)	90
	Verifying 802.1X Authentication	91
	Monitoring 802.1X Authentication	92
Chapter 3	Configuring MAC RADIUS Authentication to Control Network Access	95
	Configuring MAC RADIUS Authentication (CLI Procedure)	96
	Specifying RADIUS Server Connections on an EX Series Switch (CLI	
	Procedure)	97
	Configuring RADIUS Server Fail Fallback (CLI Procedure)	98
	Example: Configuring MAC RADIUS Authentication on an EX Series Switch	100
	Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled	
	for 802.1X or MAC RADIUS Authentication	106
	Controlling Authentication Session Timeouts (CLI Procedure)	112
Chapter 4	Configuring Captive Portal Authentication to Control Network Access	113
	Configuring Captive Portal Authentication (CLI Procedure)	113
	Configuring Secure Access for Captive Portal	114
	Enabling an Interface for Captive Portal	114
	Configuring Bypass of Captive Portal Authentication	114
	Designing a Captive Portal Authentication Login Page on an EX Series	
	Switch	115
	Example: Setting Up Captive Portal Authentication on an EX Series Switch	117

Chapter 5	Configuring Central Web Authentication to Control Network Access	123
	Understanding Central Web Authentication	123
	Central Web Authentication Process	123
	Dynamic Firewall Filters for Central Web Authentication	125
	Redirect URL for Central Web Authentication	125
	Configuring Central Web Authentication	125
	Configuring Dynamic Firewall Filters for Central Web Authentication	126
	Configuring the Redirect URL for Central Web Authentication	127
	Guidelines for Configuring Central Web Authentication	128
Chapter 6	Bypassing 802.1X and MAC RADIUS Authentication to Allow Trusted Hosts to Access the Network	129
	Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication (CLI Procedure)	129
	Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch	130
Chapter 7	Configuring Device Discovery Using LLDP and LLDP-MED	135
	Understanding LLDP and LLDP-MED on EX Series Switches	135
	Configuring LLDP (CLI Procedure)	138
	Enabling LLDP on Interfaces	138
	Adjusting LLDP Advertisement Settings	139
	Adjusting SNMP Notification Settings of LLDP Changes	139
	Specifying a Management Address for the LLDP Management TLV	140
	Configuring LLDP Power Negotiation	140
	Configuring LLDP-MED (CLI Procedure)	141
	Enabling LLDP-MED on Interfaces	141
	Configuring Location Information Advertised by the Switch	142
	Configuring a Fast Start for LLDP-MED	142
Chapter 8	Configuring VoIP	143
	Understanding 802.1X and VoIP on EX Series Switches	143
	Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch	145
	Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication	154
Chapter 9	Configuration Statements	161
	[edit access] Configuration Statement Hierarchy on EX Series Switches	163
	Supported Statements in the [edit access] Hierarchy Level	163
	Unsupported Statements in the [edit access] Hierarchy Level	168
	[edit protocols dot1x] Configuration Statement Hierarchy on EX Series Switches	169
	Supported Statements in the [edit protocols dot1x] Hierarchy Level	169
	Unsupported Statements in the [edit protocols dot1x] Hierarchy Level	170
	accounting	172
	accounting (Access Profile)	173
	accounting-order	174
	accounting-port	175
	address-assignment (Address-Assignment Pools)	176

address-protection	178
authorization-order	179
authentication-order (Access Profile)	180
authentication-order (Authenticator)	181
authentication-protocol	183
authentication-whitelist	184
authenticator	185
client-accounting-algorithm	186
client-authentication-algorithm	187
coa-dynamic-variable-validation	188
destination (Accounting)	189
destination-host (Gx-Plus)	190
destination-realm (Gx-Plus)	190
diameter-instance (Gx-Plus)	191
domain (Domain Map)	192
domain-name-server (Routing Instances and Access Profiles)	193
domain-name-server-inet (Routing Instances and Access Profiles)	194
domain-name-server-inet6 (Routing Instances and Access Profiles)	195
ethernet-port-type-virtual	195
global (Gx-Plus)	196
gx-plus (Gx-Plus)	196
ignore	197
include-ipv6 (Gx-Plus)	198
interface (Static MAC Bypass)	199
interface (VoIP)	200
interface-description-format	201
juniper-dsl-attributes	202
lldp	203
lldp-med (Ethernet Switching)	205
mau-type	206
max-outstanding-requests (Gx-Plus)	207
nas-identifier	207
nas-port-extended-format	208
nas-port-id-delimiter (Subscriber Management)	209
nas-port-id-format (Subscriber Management)	210
nas-port-type (Subscriber Management)	212
options	214
partition (Gx-Plus)	215
port	216
provisioning-order	217
radius (Access Profile)	218
radius (System)	220
radius-options (Protocols 802.1X)	221
radius-options (Access)	222
radius-server (System)	223
redirect-url	224
retry	225
revert-interval	226
routing-instance	226

	secret	227
	send-acct-status-on-config-change (Access Profile)	227
	server (RADIUS Accounting)	228
	server-fail-voip	229
	service (Service Accounting)	230
	source-address	231
	timeout (RADIUS)	232
	vlan (VoIP)	233
	vlan-assignment	234
	vlan-nas-port-stacked-format	235
	voip	235
	wait-for-acct-on-ack (Access Profile)	236
Chapter 10	Command Summaries	237
	clear captive-portal	238
	clear dot1x	240
	clear lldp neighbors	242
	clear lldp statistics	243
	show captive-portal authentication-failed-users	244
	show captive-portal firewall	246
	show captive-portal interface	248
	show dot1x	251
	show dot1x authentication-failed-users	256
	show dot1x firewall	257
	show dot1x static-mac-address	258
	show lldp	260
	show lldp local-information	265
	show lldp neighbors	267
	show lldp remote-global-statistics	273
	show lldp statistics	275
	show network-access aaa statistics accounting	277
	show network-access aaa statistics authentication	278
	show network-access aaa statistics dynamic-requests	280

List of Figures

Chapter 1	Understanding Access Control and Authentication	19
	Figure 1: Example Authentication Topology	20
	Figure 2: Authentication Process Flow for an EX Series Switch	26
Chapter 2	Configuring 802.1X Authentication to Control Network Access	29
	Figure 3: Topology for Configuration	37
	Figure 4: Topology for Configuring Supplicant Modes	45
	Figure 5: Topology for Firewall Filter and RADIUS Server Attributes Configuration	58
	Figure 6: Conceptual Model: Dynamic Filter Updated for Each New User	64
	Figure 7: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server	65
	Figure 8: Topology for Configuring 802.1X Options	69
	Figure 9: Topology for Guest VLAN Example	75
	Figure 10: EX Series Switch Connecting OAC to RADIUS Server Using EAP-TTLS Authentication	87
Chapter 3	Configuring MAC RADIUS Authentication to Control Network Access	95
	Figure 11: Topology for MAC RADIUS Authentication Configuration	102
	Figure 12: Conceptual Model: Dynamic Filter Updated for Each New User	108
	Figure 13: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server	109
Chapter 4	Configuring Captive Portal Authentication to Control Network Access	113
	Figure 14: Example of a Captive Portal Login Page	115
Chapter 5	Configuring Central Web Authentication to Control Network Access	123
	Figure 15: Central Web Authentication Process	124
Chapter 6	Bypassing 802.1X and MAC RADIUS Authentication to Allow Trusted Hosts to Access the Network	129
	Figure 16: Topology for Static MAC Bypass of Authentication Configuration	131
Chapter 8	Configuring VoIP	143
	Figure 17: VoIP Multiple Supplicant Topology	144
	Figure 18: VoIP Single Supplicant Topology	145
	Figure 19: VoIP Topology	148

List of Tables

	About the Documentation	xiii
	Table 1: Notice Icons	xv
	Table 2: Text and Syntax Conventions	xv
Chapter 2	Configuring 802.1X Authentication to Control Network Access	29
	Table 3: Components of the Topology	37
	Table 4: Components of the Supplicant Mode Configuration Topology	45
	Table 5: Match Conditions	50
	Table 6: Actions for VSAs	51
	Table 7: Components of the Firewall Filter and RADIUS Server Attributes Topology	58
	Table 8: Components of the Topology	69
	Table 9: Components of the Guest VLAN Topology	75
	Table 10: RADIUS Accounting Request Attributes	79
	Table 11: Error-Cause Codes (RADIUS Attribute 101)	81
	Table 12: Components of the OAC Deployment	87
Chapter 3	Configuring MAC RADIUS Authentication to Control Network Access	95
	Table 13: Components of the MAC RADIUS Authentication Configuration Topology	102
Chapter 4	Configuring Captive Portal Authentication to Control Network Access . . .	113
	Table 14: Configurable Elements of a Captive Portal Login Page	116
Chapter 6	Bypassing 802.1X and MAC RADIUS Authentication to Allow Trusted Hosts to Access the Network	129
	Table 15: Components of the Static MAC Bypass of Authentication Configuration Topology	131
Chapter 8	Configuring VoIP	143
	Table 16: Components of the VoIP Configuration Topology	148
Chapter 9	Configuration Statements	161
	Table 17: Unsupported [edit access] Configuration Statements on EX Series Switches	168
Chapter 10	Command Summaries	237
	Table 18: clear captive-portal interface Output Fields	238
	Table 19: show captive-portal authentication-failed-users Output Fields	244
	Table 20: show captive-portal interface Output Fields	248
	Table 21: show dot1x Output Fields	251
	Table 22: show dot1x authentication-failed-users Output Fields	256
	Table 23: show dot1x static-mac-address Output Fields	258

Table 24: show lldp Output Fields	260
Table 25: show lldp local-information Output Fields	265
Table 26: show lldp neighbors Output Fields	267
Table 27: show lldp remote-global-statistics Output Fields	273
Table 28: show lldp statistics Output Fields	275
Table 29: show network-access aaa statistics accounting Output Fields	277
Table 30: show network-access aaa statistics authentication Output Fields . . .	278
Table 31: show network-access aaa statistics dynamic-requests Output Fields	280

About the Documentation

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

Documentation and Release Notes

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

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

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

Supported Platforms

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

- EX Series

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

```
system {
  scripts {
    commit {
      file ex-script.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 [CLI Explorer](#).

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

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

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

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<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 address; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<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 of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

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

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

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

Opening a Case with JTAC

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

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

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

CHAPTER 1

Understanding Access Control and Authentication

- [Understanding Authentication on EX Series Switches on page 19](#)
- [Authentication Process Flow for EX Series Switches on page 25](#)
- [Understanding Authentication Session Timeout on page 27](#)
- [Understanding Server Fail Fallback and Authentication on EX Series Switches on page 28](#)

Understanding Authentication on EX Series Switches

You can control access to your network through a Juniper Networks EX Series Ethernet Switch by using authentication methods such as 802.1X, MAC RADIUS, or captive portal. Authentication prevents unauthenticated devices and users from gaining access to your LAN. For 802.1X and MAC RADIUS authentication, end devices must be authenticated before they receive an IP address from a Dynamic Host Configuration Protocol (DHCP) server. For captive portal authentication, the switch allows the end devices to acquire an IP address in order to redirect them to a login page for authentication.

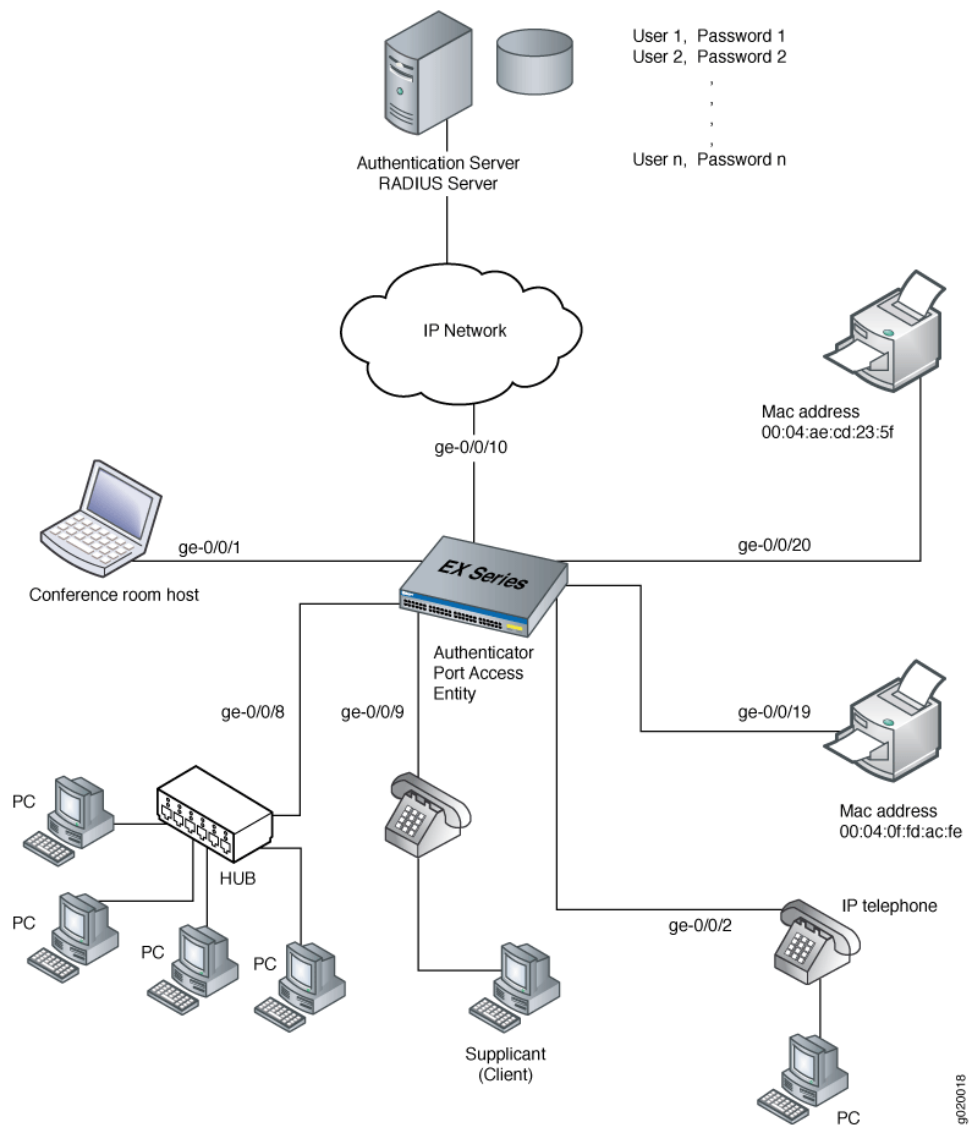
This topic covers:

- [Sample Authentication Topology on page 19](#)
- [802.1X Authentication on page 20](#)
- [MAC RADIUS Authentication on page 22](#)
- [Captive Portal Authentication on page 22](#)
- [Static MAC Bypass of Authentication on page 23](#)
- [Fallback of Authentication Methods on page 24](#)

Sample Authentication Topology

[Figure 1 on page 20](#) illustrates a basic deployment topology for authentication on an EX Series switch:

Figure 1: Example Authentication Topology



The topology contains an EX Series access switch connected to the authentication server on port ge-0/0/10. Interface ge-0/0/1 connects to the conference room host. Interface ge-0/0/8 is connected to four desktop PCs through a hub. Interfaces ge-0/0/9 and ge-0/0/2 are connected to IP phones with an integrated hub to connect the phone and desktop PC to a single port. Interfaces ge-0/0/19 and ge-0/0/20 are connected to printers.

802.1X Authentication

802.1X is an IEEE standard for port-based network access control (PNAC). It provides an authentication mechanism for devices seeking to access a LAN. The 802.1X authentication feature on an EX Series switch is based upon the IEEE 802.1X standard *Port-Based Network Access Control*.

The communication protocol between the end device and the switch is Extensible Authentication Protocol over LAN (EAPoL). EAPoL is a version of EAP designed to work with Ethernet networks. The communication protocol between the authentication server and the switch is RADIUS.

During the authentication process, the switch completes multiple message exchanges between the end device and the authentication server. While 802.1X authentication is in process, only 802.1X traffic and control traffic can transit the network. Other traffic, such as DHCP traffic and HTTP traffic, is blocked at the data link layer.



NOTE: You can configure both the maximum number of times an EAPoL request packet is retransmitted and the timeout period between attempts. For information, see [“Configuring 802.1X Interface Settings \(CLI Procedure\)” on page 32](#).

An 802.1X authentication configuration for a LAN contains three basic components:

- *Supplicant* (also called end device)—Supplicant is the IEEE term for an end device that requests to join the network. The end device can be responsive or nonresponsive. A responsive end device is 802.1X-enabled and provides authentication credentials—specifically, a username and password for EAP MD5 or a username and client certificates for Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), and Protected EAP (PEAP).

You can configure a server-reject VLAN to provide limited LAN access for responsive 802.1X-enabled end devices that sent incorrect credentials. A server-reject VLAN can provide a remedial connection, typically only to the Internet, for these devices. See [“Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients” on page 85](#) for additional information.



NOTE: If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is dropped.

A nonresponsive end device is one that is not 802.1X-enabled. It can be authenticated through MAC RADIUS authentication.

- *Authenticator port access entity*—The IEEE term for the authenticator. The EX Series switch is the authenticator, and it controls access by blocking all traffic to and from end devices until they are authenticated.
- *Authentication server*—The authentication server contains the backend database that makes authentication decisions. It contains credential information for each end device that is authenticated to connect to the network. The authenticator forwards credentials supplied by the end device to the authentication server. If the credentials forwarded by the authenticator match the credentials in the authentication server database, access is granted. If the credentials forwarded do not match, access is denied. The EX Series switches support RADIUS authentication servers.



NOTE: You cannot configure 802.1X authentication on redundant trunk groups (RTGs). For more information about RTGs, see *Understanding Redundant Trunk Links*.

MAC RADIUS Authentication

You can configure MAC RADIUS authentication on interfaces that are connected to end devices that are not 802.1X-enabled and for which you want to allow to access the LAN.

The authentication protocols supported for MAC RADIUS authentication on EX Series switches are EAP-MD5, which is the default, and Password Authentication Protocol (PAP).

If both 802.1X-enabled end devices and end devices that are not 802.1X-enabled connect to an interface, you can configure both 802.1X and MAC RADIUS authentication methods on the interface. In this case, the switch first attempts to authenticate the end device by using 802.1X, and if that method fails, it attempts to authenticate the end device by using MAC RADIUS authentication.

If you know that only end devices that are not 802.1X-enabled connect on that interface, you can eliminate the delay that occurs for the switch to determine that the end device is not 802.1X-enabled by configuring the **mac-radius restrict** option. When this option is configured, 802.1X authentication is bypassed. The switch does not attempt to authenticate the end device through 802.1X authentication but instead immediately sends a request to the RADIUS server for authentication of the MAC address of the end device. If the MAC address of that end device is configured as a valid MAC address on the RADIUS server, the switch opens LAN access to the end device on the interface to which it is connected.

The **mac-radius-restrict** option is useful when no other 802.1X authentication methods, such as guest VLAN, are needed on the interface. If you configure **mac-radius-restrict** on an interface, the switch drops all 802.1X packets.

Captive Portal Authentication

Captive portal authentication (hereafter referred to as captive portal) enables you to authenticate users on EX Series switches by redirecting Web browser requests to a login page that requires users to input a valid username and password before they can access the network. Captive portal controls network access by requiring users to provide information that is authenticated against a RADIUS server database by using EAP-MD5. You can also use captive portal to display an acceptable-use policy to users before they access your network.

Juniper Networks Junos operating system (Junos OS) for EX Series switches provides a template that enables you to easily design and modify the look of the captive portal login page. You enable specific interfaces for captive portal. The first time an end device connected to a captive portal interface attempts to access a webpage, the switch presents the captive portal login page. After the device is successfully authenticated, it is allowed access to the network and to continue to the original page requested.



NOTE: If HTTPS is enabled, HTTP requests are redirected to an HTTPS connection for the captive portal authentication process. After authentication, the end device is returned to the HTTP connection.

If there are end devices that are not HTTP-enabled connected to the captive portal interface, you can allow them to bypass captive portal authentication by adding their MAC addresses to an authentication whitelist.

When a user is authenticated by the RADIUS server, any per-user policies (attributes) associated with that user are also sent to the switch.

Captive portal on EX Series switches has the following limitations:

- Captive portal does not support dynamic assignment of VLANs downloaded from the RADIUS server.
- If the user remains idle for more than about 5 minutes and there is no traffic passed, the user must log back in to the captive portal.

Static MAC Bypass of Authentication

You can allow end devices to access the LAN without authentication on a RADIUS server by including their MAC addresses in the static MAC bypass list (also known as the exclusion list).

You might choose to include a device in the bypass list to:

- Allow non-802.1X-enabled devices access to the LAN.
- Eliminate the delay that occurs for the switch to determine that a connected device is a non-802.1X-enabled host.

When you configure static MAC on the switch, the MAC address of the end device is first checked in a local database (a user-configured list of MAC addresses). If a match is found, the end device is successfully authenticated and the interface is opened up for it. No further authentication is done for that end device. If a match is not found and 802.1X authentication is enabled on the switch, the switch attempts to authenticate the end device through the RADIUS server.

For each MAC address, you can also configure the VLAN to which the end device is moved or the interfaces on which the host connects.



CAUTION: When you clear the learned MAC addresses from an interface, using the `clear dot1x interface` command, all MAC addresses are cleared, including those in the static MAC bypass list.

Fallback of Authentication Methods

You can configure 802.1X, MAC RADIUS, and captive portal authentication on a single interface to enable fallback to another method if authentication by one method fails. The authentication methods can be configured in any combination, except that you cannot configure both MAC RADIUS and captive portal on an interface without also configuring 802.1X. By default, an EX Series switch uses the following order of authentication methods:

1. 802.1X authentication—If 802.1X is configured on the interface, the switch sends EAPoL requests to the end device and attempts to authenticate the end device through 802.1X authentication. If the end device does not respond to the EAP requests, the switch checks whether MAC RADIUS authentication is configured on the interface.
2. MAC RADIUS authentication—If MAC RADIUS authentication is configured on the interface, the switch sends the MAC RADIUS address of the end device to the authentication server. If MAC RADIUS authentication is not configured, the switch checks whether captive portal is configured on the interface.
3. Captive portal authentication—If captive portal is configured on the interface, the switch attempts to authenticate the end device by using this method after the other authentication methods configured on the interface have failed.

For an illustration of the default process flow when multiple authentication methods are configured on an interface, see [“Authentication Process Flow for EX Series Switches” on page 25](#).

You can override the default order for fallback of authentication methods by configuring the **authentication-order** statement to specify that the switch use either 802.1X authentication or MAC RADIUS authentication first. Captive portal must always be last in the order of authentication methods. For more information, see [“Configuring Flexible Authentication Order” on page 39](#).



NOTE: Starting with Junos OS Release 15.1R3, if an interface is configured in multiple-suplicant mode, end devices connecting through the interface can be authenticated using different methods in parallel. Therefore, if an end device on the interface was authenticated after fall back to captive portal, then additional end devices can still be authenticated using 802.1X or MAC RADIUS authentication.

Related Documentation

- [802.1X for EX Series Switches Overview on page 30](#)
- [Authentication Process Flow for EX Series Switches on page 25](#)
- [Example: Setting Up 802.1X for Single-Suplicant or Multiple-Suplicant Configurations on an EX Series Switch on page 44](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)
- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 96](#)

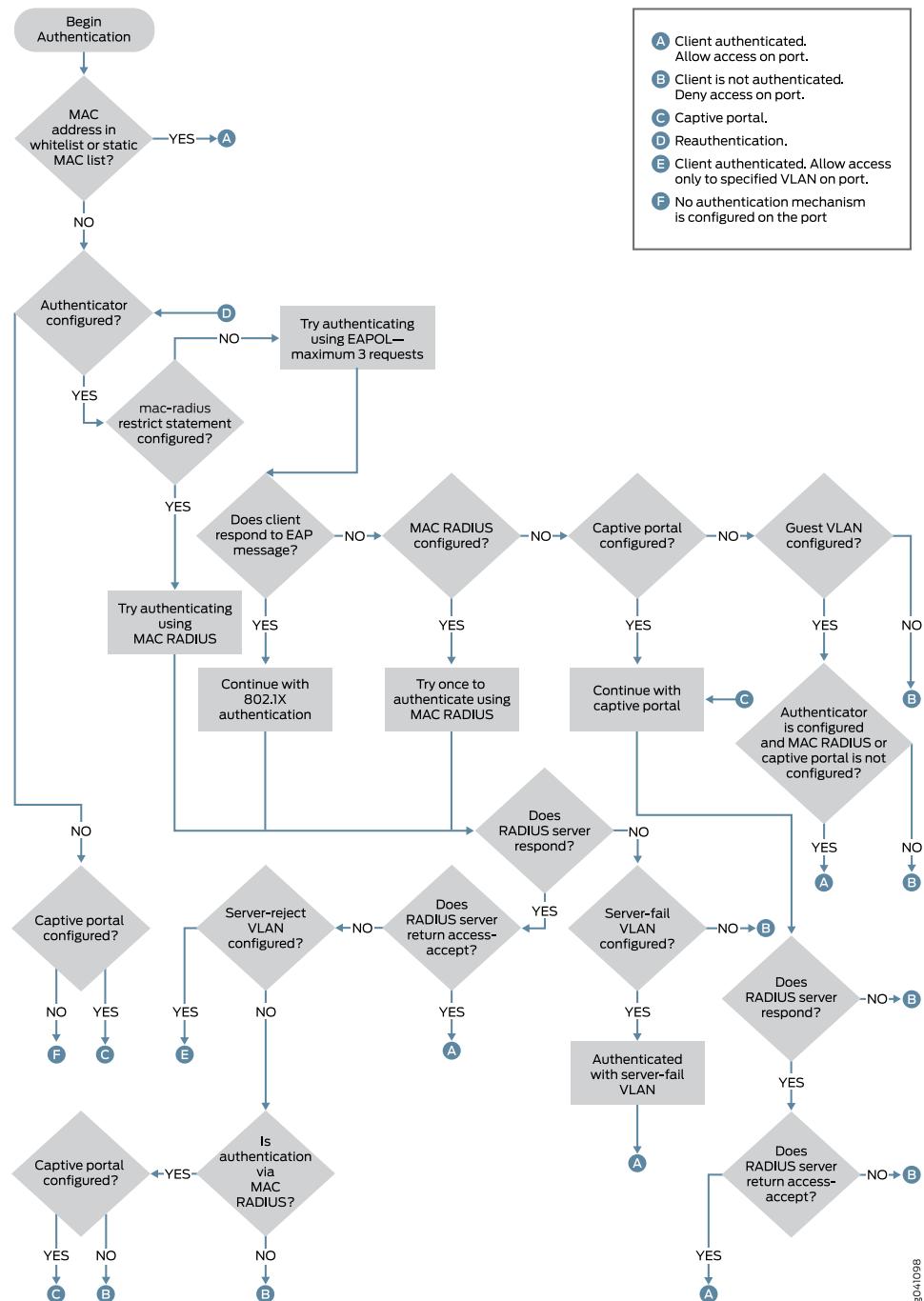
- *Configuring Captive Portal Authentication (CLI Procedure)*
- [Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication \(CLI Procedure\) on page 129](#)
- [Controlling Authentication Session Timeouts \(CLI Procedure\) on page 90](#)

Authentication Process Flow for EX Series Switches

You can control access to your network through an EX Series switch by using several different authentication methods—including 802.1X, MAC RADIUS, or captive portal.

[Figure 2 on page 26](#) illustrates the authentication process:

Figure 2: Authentication Process Flow for an EX Series Switch

**Related Documentation**

- [Understanding Authentication on EX Series Switches on page 19](#)
- [Understanding Server Fail Fallback and Authentication on EX Series Switches on page 28](#)

- [Understanding Guest VLANs for 802.1X on EX Series Switches on page 73](#)
- [Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 84](#)
- *Example: Setting Up Captive Portal Authentication on an EX Series Switch*

Understanding Authentication Session Timeout

You can specify authentication session timeout values for captive portal authentication sessions and 802.1X and MAC RADIUS authentication sessions.

For captive portal authentication sessions, the duration of the session depends on the value configured for the **session-expiry** statement. The remainder of this topic pertains only to 802.1X and MAC RADIUS authentication sessions.

For 802.1X and MAC RADIUS authentication sessions, the duration of the session before timeout depends on the interval value of the **reauthentication** statement. The authentication session might also end when the MAC table aging time expires because, unless you configure it not to, the session is removed from the authentication session table when the MAC address is removed from the Ethernet switching table.

Information about each 802.1X and MAC RADIUS authentication session—including the associated interfaces and VLANs for each MAC address that is authenticated by 802.1X authentication or MAC RADIUS authentication—is stored in the authentication session table. The authentication session table is tied to the Ethernet switching table (also called the MAC table). Each time the switch detects traffic from a MAC address, it updates the timestamp for that network node in the Ethernet switching table. A timer on the switch periodically checks the timestamp and if its value exceeds the user-configured **mac-table-aging-time** value, the switch removes the MAC address from the Ethernet switching table. When a MAC address ages out of the Ethernet switching table, the entry for that MAC address is also removed from the authentication database, with the result that the session ends.

You can control variables affecting timeout of authentication sessions in the following ways:

- Set the authentication session timeout on all interfaces or on selected interfaces using the **reauthentication** statement.
- Disassociate the authentication session table from the Ethernet switching table by using the **no-mac-table-binding** statement. This setting prevents the termination of the authentication session when the associated MAC address ages out of the Ethernet switching table.

Related Documentation

- [Understanding Authentication on EX Series Switches on page 19](#)
- [Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 44](#)
- [Controlling Authentication Session Timeouts \(CLI Procedure\) on page 90](#)
- [Configuring MAC Table Aging \(CLI Procedure\)](#)

Understanding Server Fail Fallback and Authentication on EX Series Switches

Juniper Networks Ethernet Switches use authentication to implement access control in an enterprise network. If 802.1X, MAC RADIUS, or captive portal authentication is configured on the switch, end devices are evaluated at the initial connection by an authentication (RADIUS) server. If the end device is configured on the authentication server, the device is granted access to the LAN and the EX Series switch opens the interface to permit access.

Server fail fallback enables you to specify how end devices connected to the switch are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message. Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by an end device's first attempt at authentication through the RADIUS server.

Server fail fallback enables you to specify one of four actions to be taken for end devices awaiting authentication when the server is timed out. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN. The VLAN must already be configured on the switch. The configured VLAN name overrides any attributes sent by the server.

- *Permit* authentication, allowing traffic to flow from the end device through the interface as if the end device were successfully authenticated by the RADIUS server.
- *Deny* authentication, preventing traffic from flowing from the end device through the interface. This is the default.
- *Move* the end device to a specified VLAN if the switch receives a RADIUS access-reject message. The configured VLAN name overrides any attributes sent by the server. (The VLAN must already exist on the switch.)
- *Sustain* authenticated end devices that already have LAN access and *deny* unauthenticated end devices. If the RADIUS servers time out during reauthentication, previously authenticated end devices are reauthenticated and new users are denied LAN access.

Related Documentation

- [802.1X for EX Series Switches Overview on page 30](#)
- [Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 67](#)
- [Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 44](#)
- [Configuring RADIUS Server Fail Fallback \(CLI Procedure\) on page 42](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)

CHAPTER 2

Configuring 802.1X Authentication to Control Network Access

- [802.1X for EX Series Switches Overview on page 30](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)
- [Specifying RADIUS Server Connections on an EX Series Switch \(CLI Procedure\) on page 34](#)
- [Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 35](#)
- [Configuring Flexible Authentication Order on page 39](#)
- [Configuring RADIUS Server Fail Fallback \(CLI Procedure\) on page 42](#)
- [Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 44](#)
- [Understanding Dynamic Filters Based on RADIUS Attributes on page 49](#)
- [Juniper-Switching-Filter VSA Match Conditions and Actions on page 50](#)
- [Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 52](#)
- [Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch on page 56](#)
- [Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on page 62](#)
- [Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 67](#)
- [Understanding Guest VLANs for 802.1X on EX Series Switches on page 73](#)
- [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 73](#)
- [Understanding 802.1X and RADIUS Accounting on EX Series Switches on page 78](#)
- [Understanding RADIUS-Initiated Changes to an Authorized User Session on page 80](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 83](#)
- [Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 84](#)
- [Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 85](#)
- [Controlling Authentication Session Timeouts \(CLI Procedure\) on page 90](#)

- [Verifying 802.1X Authentication on page 91](#)
- [Monitoring 802.1X Authentication on page 92](#)

802.1X for EX Series Switches Overview

How 802.1X Authentication Works

802.1X authentication works by using an authenticator port access entity (the switch) to block ingress traffic from a supplicant (end device) at the port until the supplicant's credentials are presented and match on the authentication server (a RADIUS server). When authenticated, the switch stops blocking traffic and opens the port to the supplicant.

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

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

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

- Whether or not the end device is 802.1X-enabled.
- Whether or not MAC RADIUS authentication is configured on the switch interfaces to which the hosts are connected.
- Whether the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message. See [“Configuring RADIUS Server Fail Fallback \(CLI Procedure\)” on page 42](#).

802.1X Features Overview

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

- **Guest VLAN**—Provides limited access to a LAN, typically only to the Internet, for nonresponsive end devices that are not 802.1X-enabled when MAC RADIUS authentication is not configured on the switch interfaces to which the hosts are connected. Also, a guest VLAN can be used to provide limited access to a LAN for guest users. Typically, the guest VLAN provides access only to the Internet and to other guests' end devices.
- **Server-reject VLAN**—Provides limited access to a LAN, typically only to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong

credentials. If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is not allowed.

- **Server-fail VLAN**—Provides limited access to a LAN, typically only to the Internet, for 802.1X end devices during a RADIUS server timeout.
- **Dynamic VLAN**—Enables an end device, after authentication, to be a member of a VLAN dynamically.
- **Private VLAN**—Enables configuration of 802.1X authentication on interfaces that are members of private VLANs (PVLANS).
- **Dynamic changes to a user session**—Enables the switch administrator to terminate an already authenticated session. This feature is based on support of the RADIUS Disconnect Message defined in RFC 3576.
- **VoIP VLAN**—Supports IP telephones. The implementation of a voice VLAN on an IP telephone is vendor-specific. If the phone is 802.1X-enabled, it is authenticated as any other supplicant is. If the phone is not 802.1X-enabled, but has another 802.1X-compatible device connected to its data port, that device is authenticated, and then VoIP traffic can flow to and from the phone (provided that the interface is configured in single supplicant mode and not in single-secure supplicant mode).



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

- **RADIUS accounting**—Sends accounting information to the RADIUS accounting server. Accounting information is sent to the server whenever a subscriber logs in or logs out and whenever a subscriber activates or deactivates a subscription.
- **RADIUS server attributes for 802.1X**—The **Juniper-Switching-Filter** is a vendor-specific attribute (VSA) that can be configured on the RADIUS server to further define a supplicant's access during the 802.1X authentication process. Centrally configuring attributes on the authentication server obviates the need to configure these same attributes in the form of firewall filters on every switch in the LAN to which the supplicant might connect to the LAN. This feature is based on RLI 4583, AAA RADIUS BRAS VSA Support.

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

- **Static MAC bypass**—Provides a bypass mechanism to authenticate devices that are not 802.1X-enabled (such as printers). Static MAC bypass connects these devices to 802.1X-enabled ports, bypassing 802.1X authentication.
- **MAC RADIUS authentication**—Provides a means to permit hosts that are not 802.1X-enabled to access the LAN. MAC-RADIUS simulates the supplicant functionality of the client device, using the MAC address of the client as username and password.

Related Documentation

- [Understanding Authentication on EX Series Switches on page 19](#)
- [Understanding 802.1X and VoIP on EX Series Switches on page 143](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 135](#)

- [Understanding 802.1X and RADIUS Accounting on EX Series Switches on page 78](#)
- [Understanding Guest VLANs for 802.1X on EX Series Switches on page 73](#)
- [Understanding Dynamic Filters Based on RADIUS Attributes on page 49](#)
- [Understanding Server Fail Fallback and Authentication on EX Series Switches on page 28](#)

Configuring 802.1X Interface Settings (CLI Procedure)

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



NOTE:

- You can also specify an 802.1X exclusion list to specify supplicants that can bypass authentication and be automatically connected to the LAN. See [“Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication \(CLI Procedure\)” on page 129](#).
 - 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 trunk ports.
-

Before you begin, specify the RADIUS server or servers to be used as the authentication server. See [“Specifying RADIUS Server Connections on an EX Series Switch \(CLI Procedure\)” on page 34](#).

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 attempts 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 on page 92](#)
- [Verifying 802.1X Authentication on page 91](#)
- [Configuring LLDP \(CLI Procedure\) on page 138](#)
- [Understanding Authentication on EX Series Switches on page 19](#)

Specifying RADIUS Server Connections on an EX Series Switch (CLI Procedure)

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

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

To configure a RADIUS server on the switch:

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

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



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

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

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

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

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

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

```
[edit access profile profile-name]
user@switch# set radius authentication-server server-address server-address
```

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

```
[edit]
```

```
user@switch# set protocols dot1x authenticator authentication-profile-name
access-profile-name
```

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

Related Documentation

- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 96](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 83](#)

Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch

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

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

- [Requirements on page 35](#)
- [Overview and Topology on page 36](#)
- [Configuration on page 38](#)
- [Verification on page 39](#)

Requirements

This example uses the following software and hardware components:

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

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

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*. 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 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 3 on page 37 shows one EX4200 switch that is connected to the devices listed in Table 3 on page 37.

Figure 3: Topology for Configuration

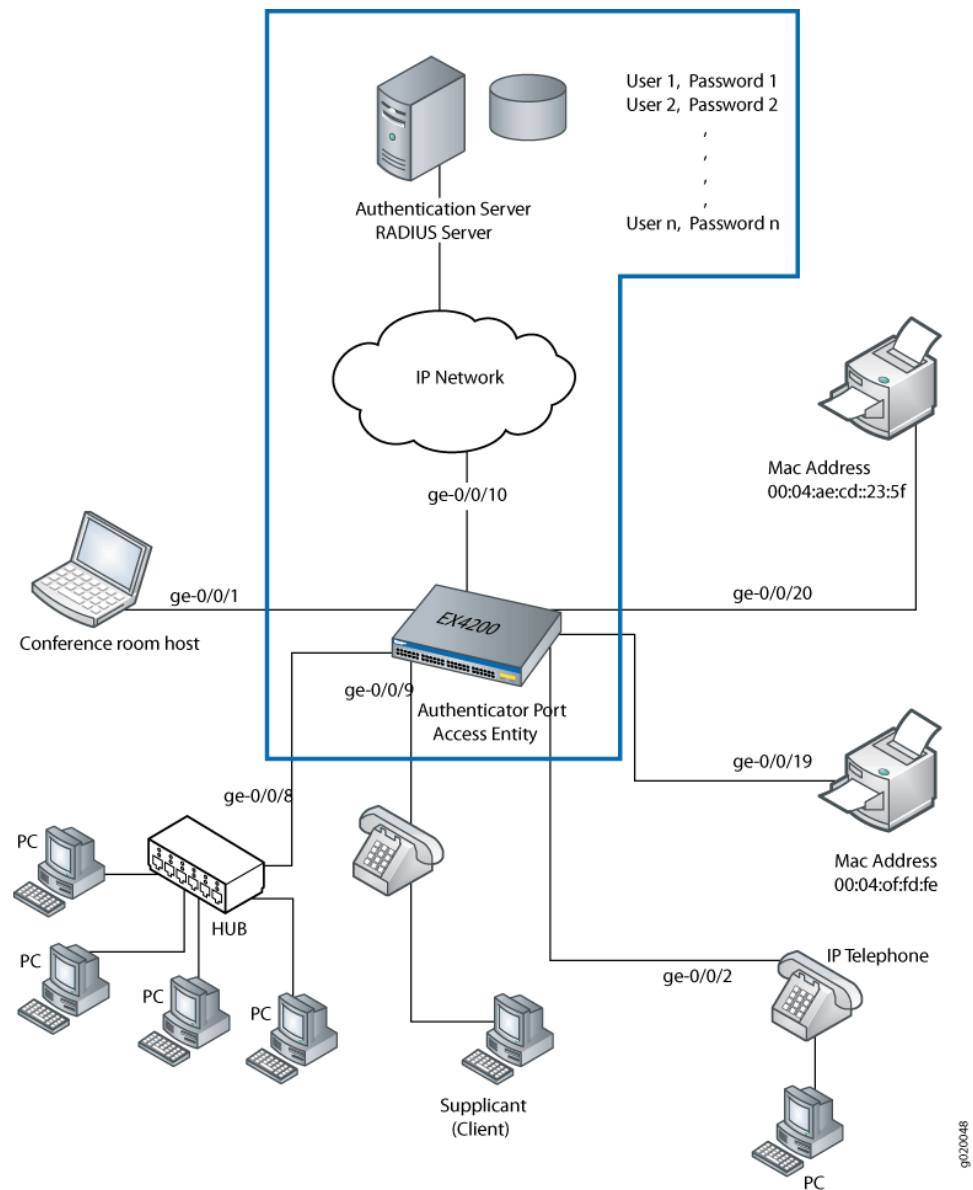


Table 3: Components of the Topology

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

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



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

Configuration

CLI Quick Configuration

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

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

Step-by-Step Procedure

To connect the RADIUS server to the switch:

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


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


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


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

Results Display the results of the configuration:

```
user@switch> show configuration access
radius-server {
  10.0.0.100
  port 1812;
  secret "$ABC123"; ## SECRET-DATA
}
profile profile1{
  authentication-order radius;
  radius {
    authentication-server 10.0.0.100 10.0.0.200;
  }
}
```

Verification

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

- [Verify That the Switch and RADIUS Server Are Properly Connected on page 39](#)

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-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 44 • Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 73 • Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch • Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 83 • Filtering 802.1X Suplicants by Using RADIUS Server Attributes on page 52

Configuring Flexible Authentication Order

You can use the flexible authentication order feature to specify the order of authentication methods that the switch uses when attempting to authenticate a client. If multiple authentication methods are configured on a single interface, when one authentication method fails, the switch falls back to another method.

By default, the switch attempts to authenticate a client by using 802.1X authentication first. If 802.1X authentication fails because there is no response from the client, and MAC RADIUS authentication is configured on the interface, the switch will attempt authentication using MAC RADIUS. If MAC RADIUS fails, and captive portal is configured on the interface, the switch attempts authentication using captive portal.

With a flexible authentication order, the sequence of authentication method used can be changed based on the type of clients connected to the interface. You can configure the **authentication-order** statement to specify whether 802.1X authentication or MAC RADIUS authentication must be the first authentication method tried. Captive portal is always the last authentication method tried.

If MAC RADIUS authentication is configured as the first authentication method in the order, then on receiving data from any client, the switch attempts to authenticate the client by using MAC RADIUS authentication. If MAC RADIUS authentication fails, then the switch uses 802.1X authentication to authenticate the client. If 802.1X authentication fails, and captive portal is configured on the interface, the switch attempts authentication using captive portal.



NOTE: If 802.1X authentication and MAC RADIUS authentication fail, and captive portal is not configured on the interface, the client is denied access to the LAN unless a server fail fallback method is configured. See [“Configuring RADIUS Server Fail Fallback \(CLI Procedure\)” on page 42](#) for more information.

Different authentication methods can be used in parallel on an interface that is configured in multiple-suplicant mode. Therefore, if an end device is authenticated on the interface by using captive portal, another end device connected to that interface can still be authenticated using 802.1X or MAC RADIUS authentication.

Before you configure the flexible authentication order on an interface, make sure that the authentication methods are configured on that interface. The switch does not attempt authentication using a method that is not configured on the interface, even if that method is included in the authentication order; the switch ignores that method and attempts the next method in the authentication order that is enabled on that interface.

Use the following guidelines when configuring the **authentication-order** statement:

- The authentication order must include at least two methods of authentication.
- 802.1X authentication must be one of the methods included in the authentication order.
- If captive portal is included in the authentication order, it must be the last method in the order.
- If **mac-radius-restrict** is configured on an interface then the authentication order cannot be configured on that interface.

To configure a flexible authentication order, use one of the following valid combinations:



NOTE: The authentication order can be configured globally using the `interface all` option as well as locally using the individual interface name. If the authentication order is configured both for an individual interface and for all interfaces, the local configuration for that interface overrides the global configuration.

- To configure 802.1X authentication as the first authentication method, followed by MAC RADIUS authentication, and then captive portal:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name authentication-order
[dot1x mac-radius captive-portal]
```

- To configure 802.1X authentication as the first authentication method, followed by captive portal:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name authentication-order
[dot1x captive-portal]
```

- To configure 802.1X authentication as the first authentication method, followed by MAC RADIUS authentication:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name authentication-order
[dot1x mac-radius]
```

- To configure MAC RADIUS authentication as the first authentication method, followed by 802.1X, followed by captive portal:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name authentication-order
[mac-radius dot1x captive-portal]
```

After you configure the authentication order, you must use the **insert** command to make any modifications to the authentication order. Using the **set** command does not change the configured order.

To change the authentication order after initial configuration:

```
[edit]
user@switch# insert protocols dot1x authenticator interface interface-name authentication-order
authentication-method before authentication-method
```

For example, to change the order from `[mac-radius dot1x captive portal]` to `[dot1x mac-radius captive portal]`:

```
[edit]
user@switch# insert protocols dot1x authenticator interface interface-name authentication-order
dot1x before mac-radius
```

Related Documentation

- [Understanding Authentication on EX Series Switches on page 19](#)
- [Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 100](#)

Configuring RADIUS Server Fail Fallback (CLI Procedure)

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

When you set up 802.1X or MAC RADIUS authentication on the switch, you specify a primary authentication server and one or more backup authentication servers. If the primary authentication server cannot be reached by the switch and the secondary authentication servers are also unreachable, a RADIUS server timeout occurs. If this happens, because it is the authentication server that grants or denies access to the end devices awaiting authentication, the switch does not receive access instructions for end devices attempting access to the LAN, and normal authentication cannot be completed.

You can configure the server fail fallback feature to specify an action that the switch applies to end devices when the authentication servers are unavailable. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN.

You can also configure the server reject fallback feature for end devices that receive a RADIUS access-reject message from the authentication server. The server reject fallback feature provides limited access to a LAN, typically only to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials.

Server fail fallback is supported for voice traffic starting in Release 14.1X53-D40 and Release 15.1R4. To configure server fail fallback actions for VoIP clients sending voice traffic, use the **server-fail-voip** statement. For all data traffic, use the **server-fail** statement. The switch determines the fallback method to use based on the type of traffic sent by the client. Untagged data frames are subject to the action configured with **server-fail**, even if they are sent by a VoIP client. Tagged VoIP VLAN frames are subject to the action configured with **server-fail-voip**. If **server-fail-voip** is not configured, the voice traffic is dropped.



NOTE: Server reject fallback is not supported for VoIP VLAN tagged traffic. If a VoIP client starts authentication by sending untagged data traffic to a VLAN while server reject fallback is in effect, the VoIP client is allowed to access the fallback VLAN. If the same client subsequently sends tagged voice traffic, the voice traffic is dropped.

If a VoIP client starts authentication by sending tagged voice traffic while server reject fallback is in effect, the VoIP client is denied access to the fallback VLAN.

You can use the following procedure to configure server fail actions for data clients. To configure server fail fallback for VoIP clients sending voice traffic, use the **server-fail-voip** statement in place of the **server-fail** statement.

To configure server fail fallback actions:

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

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

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

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

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

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

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

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

You can configure an interface that receives a RADIUS access-reject message from the authentication server to move end devices attempting LAN access on the interface to a server-reject VLAN, a specified VLAN already configured on the switch.

To configure a server reject fallback VLAN:

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

Release History Table

Release	Description
14.1X53-D40	Server fail fallback is supported for voice traffic starting in Release 14.1X53-D40 and Release 15.1R4.

Related Documentation

- [Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 67](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)
- [Monitoring 802.1X Authentication on page 92](#)
- [Understanding Server Fail Fallback and Authentication on EX Series Switches on page 28](#)

Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch

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

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

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

- [Requirements on page 44](#)
- [Overview and Topology on page 45](#)
- [Configuration of 802.1X to Support Multiple Supplicant Modes on page 46](#)
- [Verification on page 47](#)

Requirements

This example uses the following software and hardware components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from 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*. 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 4 on page 45](#), 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.

Figure 4: Topology for Configuring Supplicant Modes

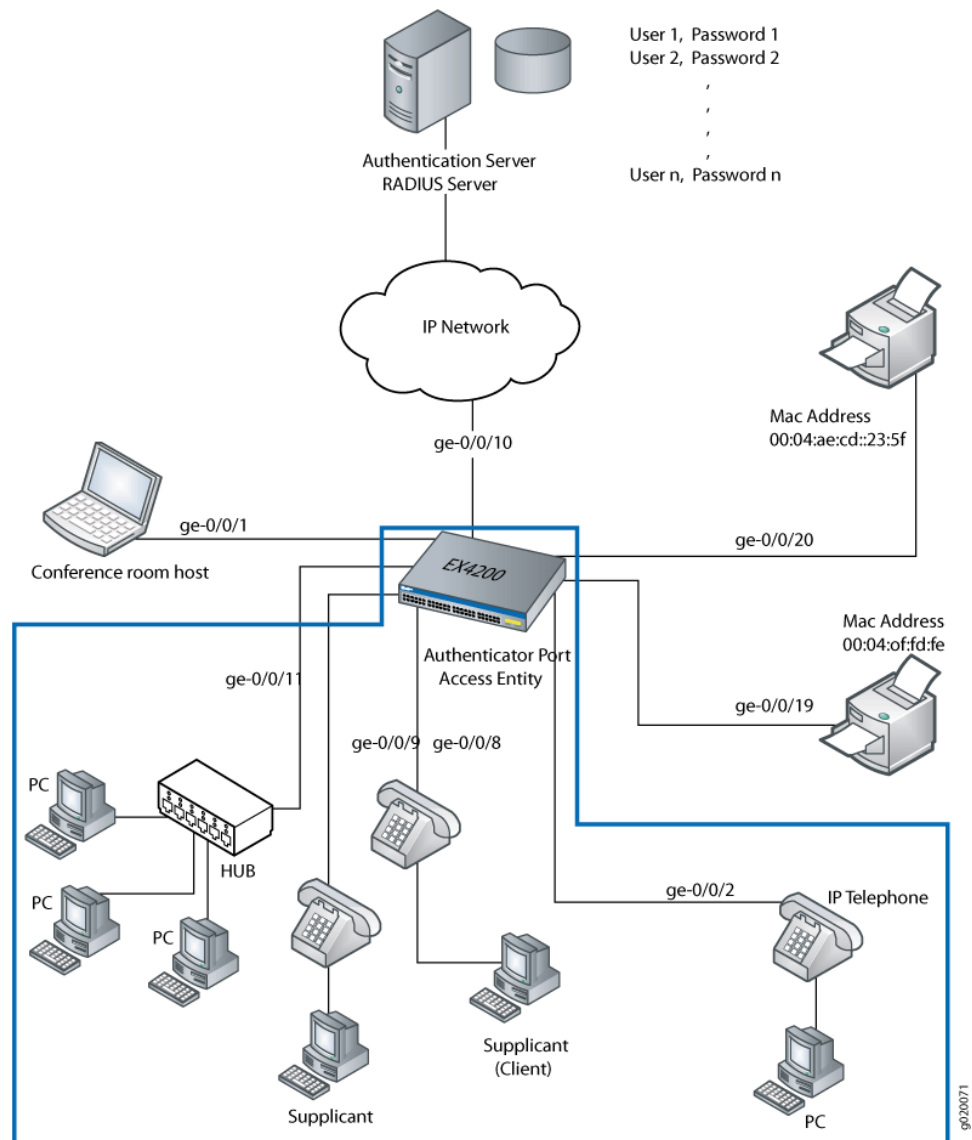


Table 4: Components of the Supplicant Mode Configuration Topology

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)

Table 4: Components of the Supplicant Mode Configuration Topology (*continued*)

Property	Settings
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 47](#)

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 90](#)
- [Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 35](#)
- [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 73](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 83](#)
- [Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 52](#)
- [Understanding Authentication on EX Series Switches on page 19](#)

Understanding Dynamic Filters Based on RADIUS Attributes

You can use RADIUS server attributes to implement port firewall filters on a RADIUS authentication server. These filters can be dynamically applied to supplicants that request authentication through that server. RADIUS server attributes are clear-text fields encapsulated in Access-Accept messages sent from the authentication server to the switch when a supplicant connected to the switch is successfully authenticated. The switch, acting as the authenticator, uses the information in the RADIUS attributes to apply the related filters to the supplicant. Dynamic filters can be applied to multiple ports on the same switch, or to multiple switches that use the same authentication server, providing centralized access control for the network.

You can define firewall filters directly on the RADIUS server by using the `Juniper-Switching-Filter` attribute, which is a RADIUS attribute specific to Juniper Networks, also known as a vendor-specific attribute (VSA). VSAs are described in RFC 2138, *Remote Authentication Dial In User Service* (RADIUS). The `Juniper-Switching-Filter` VSA is listed under attribute ID number 48 in the Juniper dictionary on the RADIUS server, with the vendor ID set to the Juniper Networks ID number 2636. Using this attribute, you define filters on the authentication server, which are applied on all switches that authenticate supplicants through that server. This method eliminates the need to configure the same filters on multiple switches.

Alternatively, you can apply a port firewall filter to multiple ports on the same switch by using the `Filter-ID` attribute, which is RADIUS attribute ID number 11. To use the `Filter-ID` attribute, you must first configure a filter on the switch, and then add the filter name to user policies on the RADIUS server as the value of the `Filter-ID` attribute. When a supplicant defined in one of those policies is authenticated by the RADIUS server, the filter is applied to the switch port that has been authenticated for the supplicant. Use this method when the firewall filter has complex conditions, or if you want to use different conditions for the same filter on different switches. The filter named in the `Filter-ID` attribute must be configured locally on the switch at the `[edit firewall family ethernet-switching filter]` hierarchy level.

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

Related Documentation

- [Understanding Authentication on EX Series Switches on page 19](#)
- [Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch on page 56](#)
- [Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 52](#)
- [Configuring Firewall Filters \(CLI Procedure\)](#)
- [Juniper-Switching-Filter VSA Match Conditions and Actions on page 50](#)

Juniper-Switching-Filter VSA Match Conditions and Actions

Switching devices support the configuration of RADIUS server attributes specific to Juniper Networks, which are known as vendor-specific attributes (VSAs). The Juniper-Switching-Filter VSA works in conjunction with 802.1X authentication to centrally control access of supplicants to the network. You can use this VSA to configure filters on the RADIUS server, which are sent to the switch and applied to users that have been authenticated using 802.1X authentication.

The Juniper-Switching-Filter VSA can contain one or more filter terms. Filter terms are configured using one or more *match conditions* with a resulting *action*. Match conditions are the criteria that a packet must meet for a configured action to be applied on it. The action is the action that the switch takes if a packet meets the criteria in the match conditions. The action that the switch can take is either accept or deny a packet.

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

- Both **match** and **action** statements are mandatory.
- If no match condition is specified, any packet is considered a match by default.
- If no action is specified, the default action is to deny the packet.
- Any or all options can be included in each **match** and **action** statement.
- The AND operation is performed on fields that are of a different type, which are separated by commas. Fields of the same type cannot be repeated.
- For the **forwarding-class** option to be applied, the forwarding class must be configured on the switch. If the forwarding class is not configured on the switch, this option is ignored.

[Table 5 on page 50](#) describes the match conditions that you can specify when you configure a VSA attribute as a firewall filter by using the **match** command on the RADIUS server. The string that defines a match condition is called a *match statement*.

Table 5: Match Conditions

Option	Description
<code>destination-mac mac-address</code>	Destination media access control (MAC) address of the packet.

Table 5: Match Conditions (*continued*)

Option	Description
<code>source-vlan <i>source-vlan</i></code>	Name of the source VLAN.
<code>source-dot1q-tag <i>tag</i></code>	Tag value in the 802.1Q header, in the range 0 through 4095.
<code>destination-ip <i>ip-address</i></code>	Address of the final destination node.
<code>ip-protocol <i>protocol-id</i></code>	IPv4 protocol value. In place of the numeric value, you can specify one of the following text synonyms: ah , egp (8), esp (50), gre (47), icmp (1), igmp (2), ipip (4), ipv6 (41), ospf (89), pim (103), rsvp (46), tcp (6), or udp (17)
<code>source-port <i>port</i></code>	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 .
<code>destination-port <i>port</i></code>	TCP or UDP destination port field. Normally, you specify this match statement in conjunction with the ip-protocol match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify one of the following text synonyms (the port numbers are also listed): afs (1483), bgp (179), biff (512), bootpc (68), bootps (67), cvspserver (2401), cmd (514), dhcp (67), domain (53), eklogin (2105), ekshell (2106), exec (512), finger (79), ftp (21), ftp-data (20), http (80), https (443), ident (113), imap (143), kerberos-sec (88), klogin (543), kpasswd (761), krb-prop (754), krbupdate (760), kshell (544), ldap (389), login (513), mobileip-agent (434), mobilip-mn (435), msdp (639), netbios-dgm (138), netbios-ns (137), netbios-ssn (139), nfsd (2049), nntp (119), ntalk (518), ntp (123), pop3 (110), pptp (1723), printer (515), radacct (1813), radius (1812), rip (520), rkinit (2108), smtp (25), snmp (161), snmptrap (162), snpp (444), socks (1080), ssh (22), sunrpc (111), syslog (514), telnet (23), tacacs-ds (65), talk (517), tftp (69), timed (525), who (513), xdmcp (177), zephyr-clt (2103), zephyr-hm (2104)

When you define one or more terms that specify the filtering criteria, you also define the action to take if the packet matches all criteria. [Table 6 on page 51](#) shows the actions that you can specify in a term.

Table 6: Actions for VSAs

Option	Description
<code>(allow deny)</code>	Accept a packet or discard a packet silently without sending an Internet Control Message Protocol (ICMP) message.
<code>forwarding-class <i>class-of-service</i></code>	(Optional) Classify the packet in one of the following forwarding classes: <ul style="list-style-type: none"> • assured-forwarding • best-effort • expedited-forwarding • network-control

Table 6: Actions for VSAs (*continued*)

Option	Description
loss-priority (low medium high)	(Optional) Set the packet loss priority (PLP) to low , medium , or high . Specify both the forwarding class and the loss priority.
Related Documentation <ul style="list-style-type: none"> • Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 52 • Understanding Dynamic Filters Based on RADIUS Attributes on page 49 • Understanding Vendor-Specific Attributes (VSAs) 	

Filtering 802.1X Supplicants by Using RADIUS Server Attributes

There are two ways to configure the a RADIUS server with port firewall filters (Layer 2 firewall filters):

- Include one or more filter terms in the Juniper-Switching-Filter attribute. The Juniper-Switching-Filter attribute is a vendor-specific attribute (VSA) listed under attribute ID number 48 in the Juniper dictionary on the RADIUS server. Use this VSA to configure simple filter conditions for 802.1X authenticated users. Nothing needs to be configured on the switch; all of the configuration is on the RADIUS server.
- Configure a local firewall filter on each switch and apply that firewall filter to users authenticated through the RADIUS server. Use this method for more complex filters. Use this method for more complex filters. The firewall filter must be configured on each switch.



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

This topic includes the following tasks:

1. [Configuring Firewall Filters on the RADIUS Server on page 52](#)
2. [Applying a Locally Configured Firewall Filter from the RADIUS Server on page 55](#)

Configuring Firewall Filters on the RADIUS Server

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



NOTE: This procedure describes using FreeRADIUS software to configure the Juniper-Switching-Filter VSA. For specific information about configuring your server, consult the AAA documentation included with your server.

To configure the Juniper-Switching-Filter attribute, enter one or more filter terms by using the CLI for the RADIUS server. Each filter term consists of match conditions with a corresponding action. Enter the filter terms enclosed within quotation marks (" ") by using the following syntax:

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

More than one match condition can be included in a filter term. When multiple conditions are specified in a filter term, they must all be fulfilled for the packet to match the filter term. For example, the following filter term requires a packet to match *both* the destination IP address and the destination MAC address to meet the term criteria:

```
Juniper-Switching-Filter = "match destination-ip 10.10.10.8 destination-mac
00:00:00:01:02:03 action allow"
```

Multiple filter terms should be separated with commas—for example:

```
Juniper-Switching-Filter = "match destination-mac 00:00:00:01:02:03 action allow,
match destination-port 80 destination-mac 00:aa:bb:cc:dd:ee action allow"
```

See [“Juniper-Switching-Filter VSA Match Conditions and Actions”](#) on page 50 for definitions of match conditions and actions.

To configure match conditions on the RADIUS server:

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

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

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

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

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

```
[root@freeradius]#
```

```
cd /usr/local/etc/raddb
vi users
```

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

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

- To deny access based on a destination IP address:

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

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

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

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

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

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

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



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

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

Applying a Locally Configured Firewall Filter from the RADIUS Server

You can apply a port firewall filter (Layer 2 firewall filter) to user policies centrally from the RADIUS server. The RADIUS server can then specify the firewall filters that are to be applied to each user that requests authentication, reducing the need to configure the same firewall filter on multiple switches. Use this method when the firewall filter contains a large number of conditions or you want to use different conditions for the same filter on different switches. The firewall filters must be configured on each switch.

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

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



NOTE: If port firewall filters are also configured locally for the interface, then the firewall filters configured by using VSAs take precedence if they conflict with the locally configured port firewall filters. If there is no conflict, they are merged.

1. Create the firewall filter on the local switch. See *Configuring Firewall Filters (CLI Procedure)* for more information on configuring a port firewall filter.
2. On the RADIUS server, open the **users** file to display the local user profiles of the end devices to which you want to apply the filter:

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

3. Apply the filter to each user profile by adding the Filter-ID attribute with the filter name as the attribute value:

Filter-Id =filter-name

For example, the user profile below for **supplicant1** includes the Filter-ID attribute with the filter name **filter1**:

```
[root@freeradius]# cat /usr/local/etc/raddb/users  
  
supplicant1 Auth-Type := EAP, User-Password == "supplicant1"  
    Tunnel-Type = VLAN,  
    Tunnel-Medium-Type = IEEE-802,  
    Tunnel-Private-Group-Id = "1005",  
    Filter-Id = "filter1"
```



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

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

- Related Documentation**
- [Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch on page 56](#)
 - [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches](#)
 - [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)
 - [Understanding Dynamic Filters Based on RADIUS Attributes on page 49](#)

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

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

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

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

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

- [Requirements on page 56](#)
- [Overview and Topology on page 57](#)
- [Configuring the Port Firewall Filter and Counters on page 59](#)
- [Applying the Port Firewall Filter to the Supplicant User Profiles on the RADIUS Server on page 60](#)
- [Verification on page 61](#)

Requirements

This example uses the following software and hardware components:

- Junos OS Release 9.3 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.

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

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

- Set up a connection between the switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch”](#) on page 35.
- Configured 802.1X authentication on the switch, with the supplicant mode for interface ge-0/0/2 set to **multiple**. See [“Configuring 802.1X Interface Settings \(CLI Procedure\)”](#) on page 32 and [“Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch”](#) on page 44.
- Configured users on the RADIUS authentication server (in this example, the user profiles for Supplicant 1 and Supplicant 2 in the topology are modified on the RADIUS server).

Overview and Topology

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

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

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



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

[Figure 5 on page 58](#) 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.

Figure 5: Topology for Firewall Filter and RADIUS Server Attributes Configuration

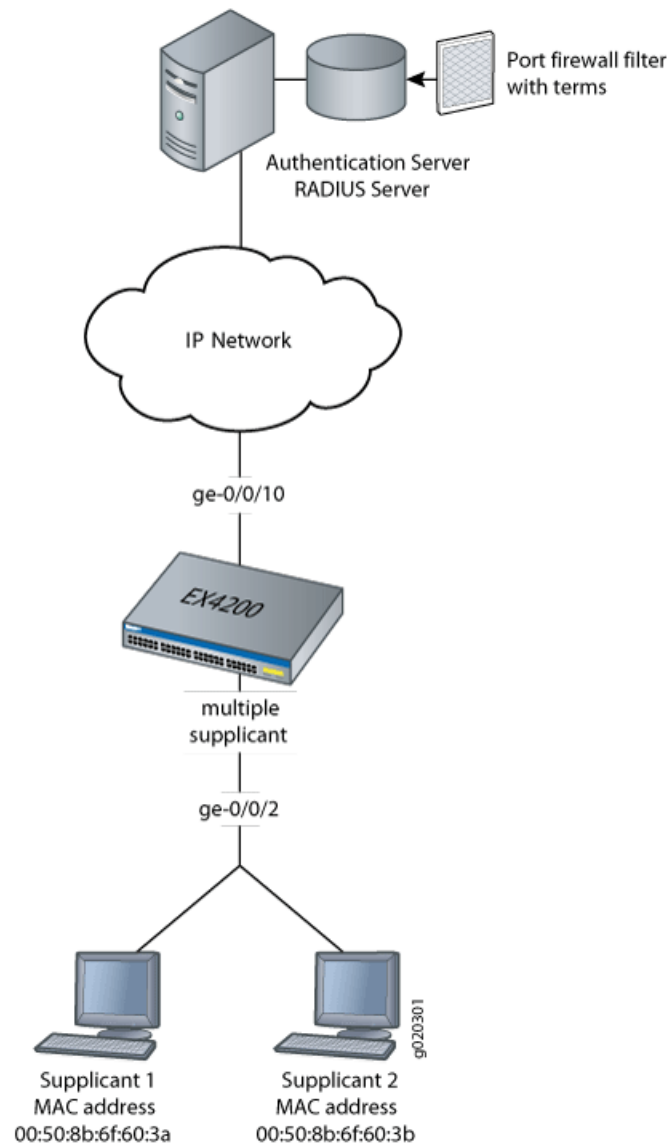


Table 7 on page 58 describes the components in this topology.

Table 7: Components of the Firewall Filter and RADIUS Server Attributes Topology

Property	Settings
Switch hardware	EX4200 access switch, 24 Gigabit Ethernet ports: 16 non-PoE ports and 8 PoE ports.
One RADIUS server	Backend database with the address 10.0.0.100 connected to the switch at port ge-0/0/10 .
802.1X supplicants connected to the switch on interface ge-0/0/2	<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 7: 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 **p1** limits the traffic rate based on the values for **exceeding** and **discard** parameters. Then, you check to see that the RADIUS server attribute is available on the RADIUS server and apply the filter to the user profiles of each end device on the RADIUS server. Finally, you verify the configuration by displaying output for the two counters.

Configuring the Port Firewall Filter and Counters

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

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

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

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


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


```
[edit]
user@switch# set firewall policer p1 if-exceeding bandwidth-limit 1m
user@switch# set firewall policer p1 if-exceeding burst-size-limit 1k
user@switch# set firewall policer p1 then discard
```

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

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

Results Display the results of the configuration:

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

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

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

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

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

2. Close the dictionary file.

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

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

The output shows:

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

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

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

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

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

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

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

Verification

Verifying That the Filter Has Been Applied to the Supplicants

Purpose After the end devices are authenticated, 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 **show firewall filter filter1** command 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-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 44](#)
 - [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches](#)
 - [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 83](#)
 - [Understanding Authentication on EX Series Switches on page 19](#)
 - [Understanding Dynamic Filters Based on RADIUS Attributes on page 49](#)

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 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*.

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

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

- [Requirements on page 62](#)
- [Overview and Topology on page 63](#)
- [Configuration on page 65](#)
- [Verification on page 67](#)

Requirements

This example uses the following software and hardware components:

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

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

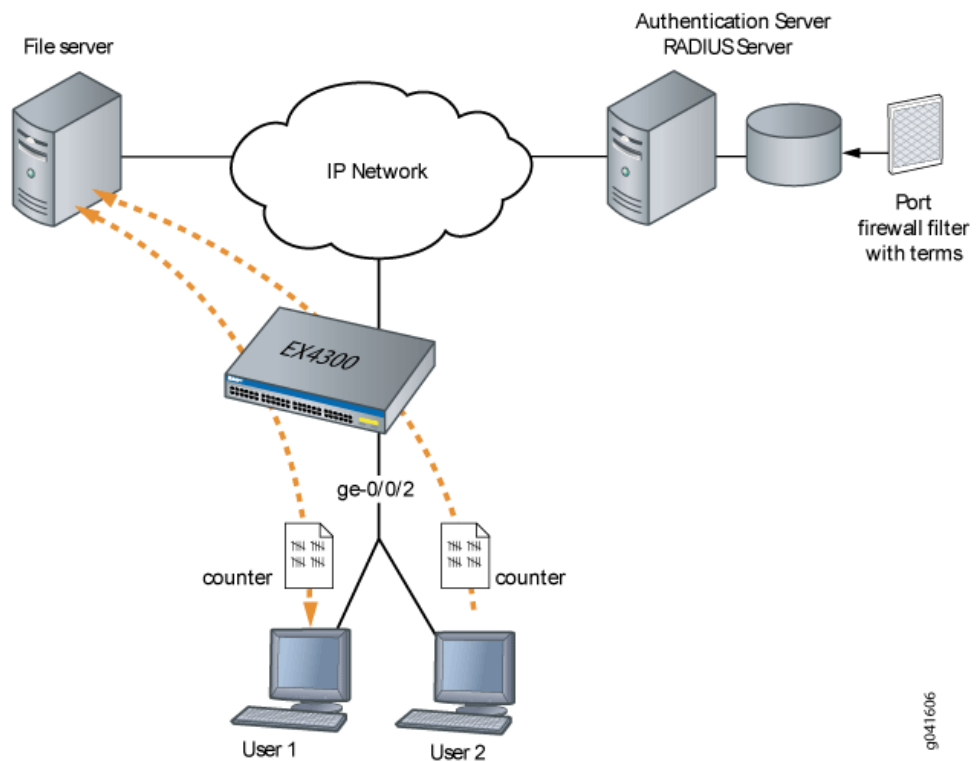
- Set up a connection between the switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 35](#).
- Configured 802.1X authentication on the switch, with the authentication mode for the interface ge-0/0/2 set to **multiple**. See [“Configuring 802.1X Interface Settings \(CLI Procedure\)” on page 32](#) and [“Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch” on page 44](#).
- 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 6 on page 64](#), 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.

Figure 6: Conceptual Model: Dynamic Filter Updated for Each New User



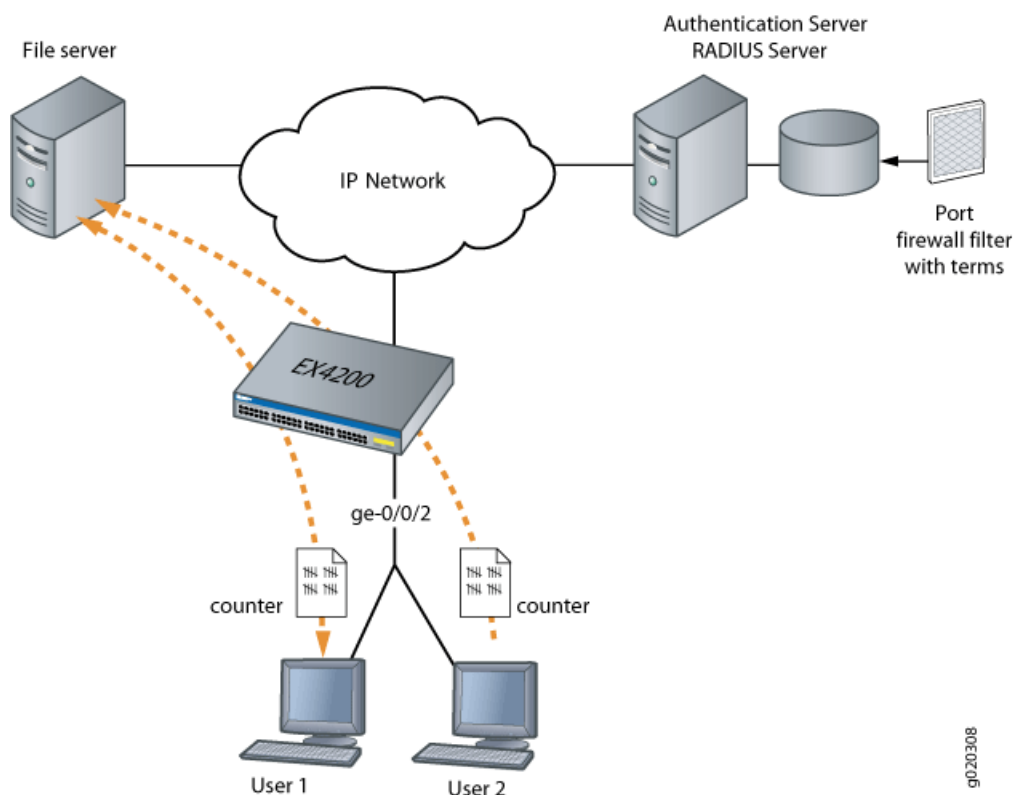
This is a conceptual model of the internal process—you cannot access or view the dynamic filter.



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 7 on page 65](#) shows the network topology for this example.

Figure 7: 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 by Using RADIUS Server Attributes on an EX Series Switch on page 56 • 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 52

Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch

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

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

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

- [Requirements on page 68](#)
- [Overview and Topology on page 68](#)
- [Configuration on page 70](#)
- [Verification on page 70](#)

Requirements

This example uses the following software and hardware components:

- 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*. 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 an EX Series Switch” on page 35](#).
- Configured users on the authentication server.

Overview and Topology

A RADIUS server timeout occurs if no authentication RADIUS servers are reachable when a supplicant logs in and attempts to access the LAN. Using server fail fallback, you configure alternative options for supplicants attempting LAN access. You can configure the switch to accept or deny access to supplicants or to maintain the access already granted to supplicants before the RADIUS server timeout. Additionally, you can configure the switch to move supplicants to a specific VLAN if a RADIUS timeout occurs or if the RADIUS server sends an EAP Access-Reject message.

[Figure 8 on page 69](#) 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`.

Figure 8: Topology for Configuring 802.1X Options

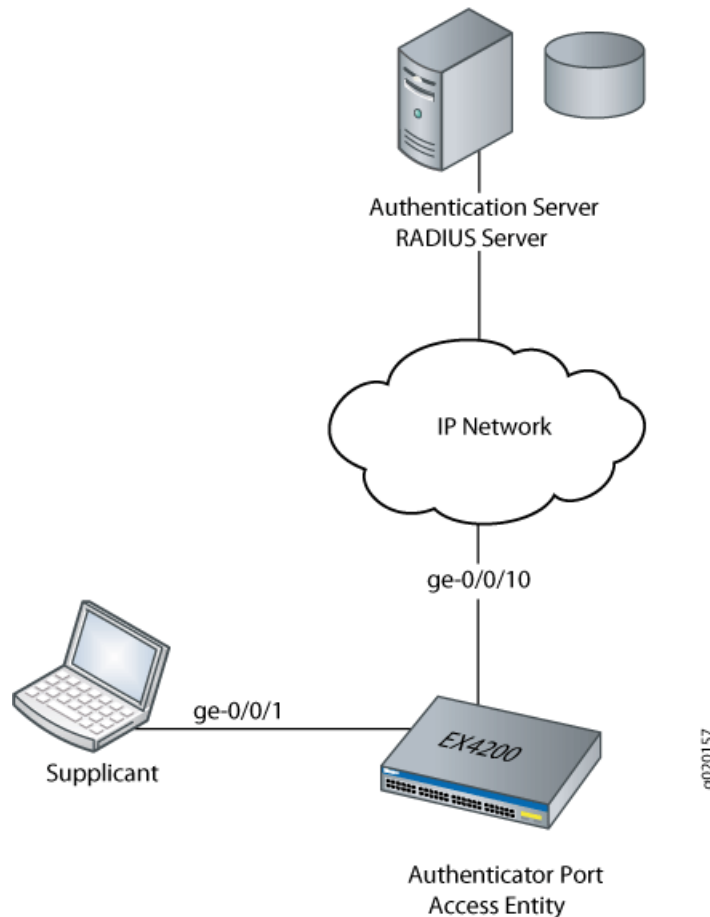


Table 8 on page 69 describes the components in this topology.

Table 8: Components of the Topology

Property	Settings
Switch hardware	EX4200 access switch, 24 Gigabit Ethernet ports: 16 non-PoE ports and 8 PoE ports.
VLAN names	default VLAN vlan-sf VLAN
Supplicant	Supplicant attempting access on interface <code>ge-0/0/1</code>
One RADIUS server	Backend database with an address of <code>10.0.0.100</code> connected to the switch at port <code>ge-0/0/10</code>

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

Configuration

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

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

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

1. Define the VLAN to which supplicants are diverted:

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

Results Display the results of the configuration:

```
user@switch> show configuration
interfaces {
  ge-0/0/1 {
    unit 0 {
      family ethernet-switching {
        vlan {
          members default;
        }
      }
    }
  }
}
protocols {
  dot1x {
    authenticator {
      interface {
        ge-0/0/1.0 {
          server-fail vlan-name vlan-sf;
        }
      }
    }
  }
}
```

Verification

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

- [Verifying That the Supplicants Are Moved to an Alternative VLAN During a RADIUS Timeout on page 71](#)

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

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

Related Documentation

- [Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 44](#)
- [Configuring RADIUS Server Fail Fallback \(CLI Procedure\) on page 42](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 83](#)
- [Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 52](#)
- [Understanding Server Fail Fallback and Authentication on EX Series Switches on page 28](#)

Understanding Guest VLANs for 802.1X on EX Series Switches

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

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

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

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

A guest VLAN is not used when MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected.

Related Documentation

- [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 73](#)
- [Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 84](#)
- [Understanding Authentication on EX Series Switches on page 19](#)

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

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

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

- [Requirements on page 74](#)
- [Overview and Topology on page 74](#)
- [Configuration of a Guest VLAN That Includes 802.1X Authentication on page 76](#)
- [Verification on page 76](#)

Requirements

This example uses the following software and hardware components:

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

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

- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*. 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 9 on page 75](#) shows the conference room connected to the switch at interface ge-0/0/1.

Figure 9: Topology for Guest VLAN Example

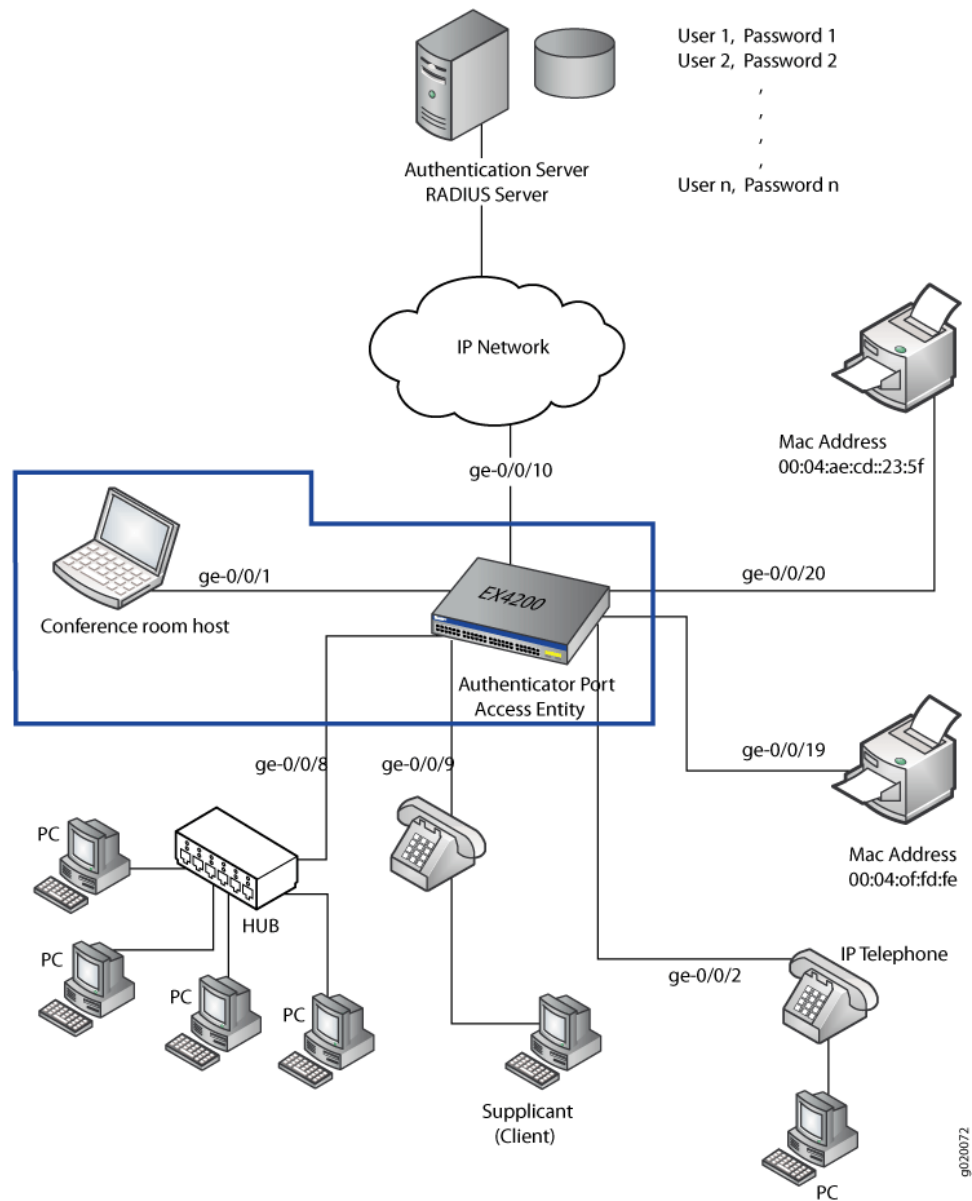


Table 9: Components of the Guest VLAN Topology

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

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

Configuration of a Guest VLAN That Includes 802.1X Authentication

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

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

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

1. Configure the VLAN ID for the guest VLAN:

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

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

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

Results Check the results of the configuration:

```
user@switch> show configuration
protocols {
  dot1x {
    authenticator {
      interface {
        all {
          guest-vlan {
            guest-vlan;
          }
        }
      }
    }
  }
}
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 76](#)

Verifying That the Guest VLAN Is Configured

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



NOTE: On switches running Junos OS for EX Series with support for ELS, the output for the `show vlans` command will contain additional information. If your switch runs software that supports ELS, see `show vlans`. For ELS details, see *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 an EX Series Switch on page 35](#)
 - [Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 44](#)
 - [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
 - [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)

Understanding 802.1X and RADIUS Accounting on EX Series Switches

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

- [RADIUS Accounting Process on page 78](#)
- [Supported RADIUS Attributes on page 79](#)

RADIUS Accounting Process

RADIUS accounting is based on a client/server model in which the switch, operating as the network access server (NAS), is the client. The client forwards user accounting statistics to a designated RADIUS accounting server. The RADIUS accounting server must send a response to the client when it has successfully received and recorded the accounting statistics.

The RADIUS accounting process between a switch and a RADIUS server is based on the exchange of two types of RADIUS packets—Accounting-Request and Accounting-Response. Accounting-Request packets are sent from the switch to the server and convey information used to account for a service provided to a user. Accounting-Response packets are sent from the server to acknowledge receipt of the Accounting-Request packets. The exchange of packets between the switch and the server proceeds as follows:

1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. For example, on FreeRADIUS, the default port is 1813.
2. When a supplicant is authenticated through 802.1X authentication and then connected to the LAN, the switch forwards an Accounting-Request packet with a record of the event to the accounting server. The Accounting-Request packet sent by the switch includes the RADIUS attribute Acct-Status-Type with a value of Start, which indicates the beginning of user service for this supplicant. The accounting server records this event in the accounting log file as a start record.
3. The accounting server sends an Accounting-Response packet back to the switch confirming that it received the accounting request. If the switch does not receive a response from the server, it continues to send accounting requests until an accounting response is returned from the accounting server.

4. The switch might send an interim message to the accounting server to periodically update the server with information pertaining to a specific session. Interim messages are sent as Accounting-Request messages with the Acct-Status-Type attribute value of Interim-Update. The accounting server sends an Accounting-Response packet back to the switch to confirm receipt of an interim update.
5. When the supplicant's session ends, the switch forwards an Accounting-Request packet with the Acct-Status-Type attribute value set to Stop, indicating the end of user service. The accounting server records this event in the accounting log file as a stop record that contains session information and the length of the session.

The statistics collected through this process can be displayed from the RADIUS server. To view those statistics, the user needs to access the accounting log file configured to receive them. On FreeRADIUS, the filename is the server's address—for example, 122.69.1.250.

Supported RADIUS Attributes

RADIUS accounting statistics are conveyed through the attributes included in each Accounting-Request packet sent from the NAS to the server. [Table 10 on page 79](#) list the RADIUS attributes supported for Accounting-Request packets.

Table 10: RADIUS Accounting Request Attributes

Type	Attribute	Description
1	User-Name	The name of the authenticated user.
5	NAS-Port	The physical port number of the NAS that authenticates the user. Either NAS-Port or NAS-Port-ID must be contained in the packet.
8	Framed-IP-Address	The IP address of the authenticated user. NOTE: The Framed-IP-Address attribute is sent only if a valid DHCP binding exists for the host in the DHCP snooping table.
30	Called-Station-ID	Enables the NAS to identify the phone number that the user called, using Dialed Number Identification (DNIS) or a similar technology.
31	Calling-Station-ID	Enables the NAS to identify the phone number that the call came from, using Automatic Number Identification (ANI) or a similar technology.
32	NAS-Identifier	Contains a string identifying the NAS originating the Accounting-Request message.
40	Acct-Status-Type	Indicates whether this Accounting-Request message marks the beginning (Start) or the end (Stop) of the user session. Can also be used for an interim update (Interim-Update).
44	Acct-Session-ID	A unique ID for a specific accounting session that can be used to match start and stop records for a session in the log file.

Table 10: RADIUS Accounting Request Attributes (*continued*)

Type	Attribute	Description
55	Event-Timestamp	Records the time an event occurred.

**Related
Documentation**

- [802.1X for EX Series Switches Overview on page 30](#)
- [Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 35](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 83](#)

Understanding RADIUS-Initiated Changes to an Authorized User Session

When using an authentication service that is based on a client/server RADIUS model, requests are typically initiated by the client and sent to the RADIUS server. There are instances in which a request might be initiated by the server and sent to the client in order to dynamically modify an authenticated user session already in progress. The client that receives and processes the messages is the switch, which acts as the network access server, or NAS. The server can send the switch a Disconnect message requesting to terminate a session, or a Change of Authorization (CoA) message requesting to modify the session authorization attributes.

The switch listens for unsolicited RADIUS requests on UDP port 3799, and accepts requests only from a trusted source. Authorization to send a Disconnect or CoA request is determined based on the source address and the corresponding shared secret, which must be configured on the switch as well as on the RADIUS server. For more information about configuring the source address and shared secret on the switch, see [“Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 35](#).

- [Disconnect Messages on page 80](#)
- [Change of Authorization Messages on page 81](#)
- [Error-Cause Codes on page 81](#)

Disconnect Messages

The RADIUS server sends a Disconnect-Request message to the switch in order to terminate a user session and discard all associated session context. The switch responds to a Disconnect-Request packet with a Disconnect-ACK message if the request is successful, that is, all associated session context is discarded and the user session is no longer connected, or with a Disconnect-NAK packet if the request fails, that is, the authenticator is unable to disconnect the session and discard all associated session context.

In Disconnect-Request messages, RADIUS attributes are used to uniquely identify the switch (NAS) and the user session. The combination of NAS identification attributes and session identification attributes included in the message must match at least one session for the request to be successful; otherwise, the switch responds with a Disconnect-NAK message. A Disconnect-Request message can contain only NAS and session identification

attributes; if any other attributes are included, the switch responds with a Disconnect-NAK message.

Change of Authorization Messages

Change of Authorization (CoA) messages contain information for dynamically modifying the authorization attributes for a user session to change the authorization level. CoA messages are typically used to change data filters or VLANs for an authenticated host. The switch responds to a CoA message with a CoA-ACK message if the authorization change is successful, or a with CoA-NAK message if the change is unsuccessful. If one or more authorization changes specified in a CoA-Request message cannot be carried out, the switch responds with a CoA-NAK message.

In CoA-Request messages, RADIUS attributes are used to uniquely identify the switch (acting as the NAS) and the user session. The combination of NAS identification attributes and session identification attributes included in the message must match the identification attributes of at least one session for the request to be successful; otherwise, the switch responds with a CoA-NAK message.

CoA-Request packets also include the session authorization attributes that will be modified if the request is accepted. The supported session authorization attributes are listed below. The CoA message can contain any or all of these attributes. If any attribute is not included as part of the CoA-Request message, the NAS assumes that the value for that attribute is to remain unchanged.

- Filter-ID
- Tunnel-Private-Group-ID
- Juniper-Switching-Filter
- Juniper-VoIP-VLAN
- Session-Timeout

Error-Cause Codes

When a disconnect or CoA operation is unsuccessful, an Error-Cause attribute (RADIUS attribute 101) can be included in the response message sent by the NAS to the server to provide detail about the cause of the problem. If the detected error does not map to one of the supported Error-Cause attribute values, the router sends the message without an error-cause attribute. See [Table 11 on page 81](#) for descriptions of error-cause codes that can be included in response messages sent from the NAS.

Table 11: Error-Cause Codes (RADIUS Attribute 101)

Code	Value	Description
201	Residual session context removed	Sent in response to a Disconnect-Request message if one or more user sessions are no longer active, but residual session context was found and successfully removed. This code is sent only within a Disconnect-ACK message.

Table 11: Error-Cause Codes (RADIUS Attribute 101) (*continued*)

Code	Value	Description
401	Unsupported attribute	The request contains an attribute that is not supported (for example, a third-party attribute).
402	Missing attribute	A critical attribute (for example, the session identification attribute) is missing from a request.
403	NAS identification mismatch	Request contains one or more NAS identification attributes that do not match the identity of the NAS receiving the request.
404	Invalid request	Some other aspect of the request is invalid—for example, if one or more attributes are not formatted properly.
405	Unsupported service	The Service-Type attribute included with the request contains an invalid or unsupported value.
406	Unsupported extension	The entity receiving the request (either an NAS or a RADIUS proxy) does not support RADIUS-initiated requests.
407	Invalid attribute value	The request contains an attribute with an unsupported value.
501	Administratively prohibited	The NAS is configured to prohibit honoring of Disconnect-Request or CoA-Request messages for the specified session.
503	Session context not found	The session context identified in the request does not exist on the NAS.
504	Session context not removable	The subscriber identified by attributes in the request is owned by a component that is not supported. This code is sent only within a Disconnect-NAK message.
506	Resources unavailable	A request could not be honored because of lack of available NAS resources (such as memory).
507	Request initiated	The CoA-Request message includes a Service-Type attribute with a value of Authorize Only.
508	Multiple session selection unsupported	The session identification attributes included in the request match multiple sessions, but the NAS does not support requests that apply to multiple sessions.

Related Documentation

- [Understanding Dynamic Filters Based on RADIUS Attributes on page 49](#)
- [Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 84](#)

Configuring 802.1X RADIUS Accounting (CLI Procedure)

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

RADIUS accounting is based on a client/server model in which the switch, operating as the network access server (NAS), is the client. The client is responsible for forwarding user accounting statistics to a designated RADIUS accounting server. To configure RADIUS accounting, specify one or more RADIUS accounting servers to receive the statistical data from the switch, and select the type of accounting data to be collected.

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

To configure RADIUS accounting by using the CLI:

1. Configure an access profile and specify the accounting servers to which the switch forwards accounting statistics:

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

2. Define the address of RADIUS accounting servers and configure the secret password (the secret password on the switch must match the secret password on the server):

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

3. Enable accounting for the access profile:

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

4. Configure the accounting order, making RADIUS the first method for sending accounting messages and updates:

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

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

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

6. (Optional) Configure the switch to send periodic updates for a user session at a specified interval to the accounting server:

```
[edit access]
user@switch# set profile profile-name accounting update-interval minutes
```

7. Display accounting statistics collected on the switch using the **show network-access aaa statistics accounting** command, for example:

```
user@switch> show network-access aaa statistics accounting
```

```
Accounting module statistics
Requests received: 1
Accounting Response failures: 0
Accounting Response Success: 1
Requests timedout: 0
```

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

```
[root@freeradius]# cd /usr/local/var/log/radius/radacct/192.168.0.1
[root@freeradius 192.168.0.1]# ls
```

```
detail-20071214
```

```
[root@freeradius 192.168.0.1]# vi details-20071214
```

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

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

- Related Documentation**
- [Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 35](#)
 - [Understanding 802.1X and RADIUS Accounting on EX Series Switches on page 78](#)

Understanding Dynamic VLAN Assignment Using RADIUS Attributes

VLANs can be dynamically assigned by a RADIUS server to supplicants requesting 802.1X authentication through that server. You configure the VLAN on the RADIUS server using RADIUS server attributes, which are clear-text fields encapsulated in messages sent from the authentication server to the switch when a supplicant connected to the switch requests authentication. The switch, acting as the authenticator, uses the information in the RADIUS attributes to assign the VLAN to the supplicant. Based on the results of

the authentication, a supplicant that began authentication in one VLAN might be assigned to another VLAN.

Successful authentication requires that the VLAN ID or VLAN name is configured on the switch acting as 802.1X authenticator, and that it matches the VLAN ID or VLAN name sent by the RADIUS server during authentication. If neither exists, the end device is not authenticated. If a guest VLAN is established, the unauthenticated end device is automatically moved to the guest VLAN.

The RADIUS server attributes used for dynamic VLAN assignment described in RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*.

- Tunnel-Type—Defined as RADIUS attribute type 64. The value should be set to **VLAN**.
- Tunnel-Medium-Type—Defined as RADIUS attribute type 65. The value should be set to **802**.
- Tunnel-Private-Group-ID—Defined as RADIUS attribute type 81. The value should be set to the VLAN ID or the VLAN name.

For more information about configuring dynamic VLANs on your RADIUS server, see the documentation for your RADIUS server.

**Related
Documentation**

- [Understanding Guest VLANs for 802.1X on EX Series Switches on page 73](#)
- [Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 100](#)
- [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 73](#)

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

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

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

- [Requirements on page 86](#)
- [Overview and Topology on page 86](#)
- [Configuration on page 88](#)
- [Verification on page 89](#)

Requirements

This example uses the following software and hardware components:

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

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

- Set up a connection between the switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch”](#) on page 35.
- Configured EAP-TTLS on the server. See your RADIUS server documentation.
- Configured users on the RADIUS server. See your RADIUS server documentation.

Overview and Topology

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

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

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

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

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

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



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

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

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

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

Figure 10 on page 87 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.

Figure 10: EX Series Switch Connecting OAC to RADIUS Server Using EAP-TTLS Authentication

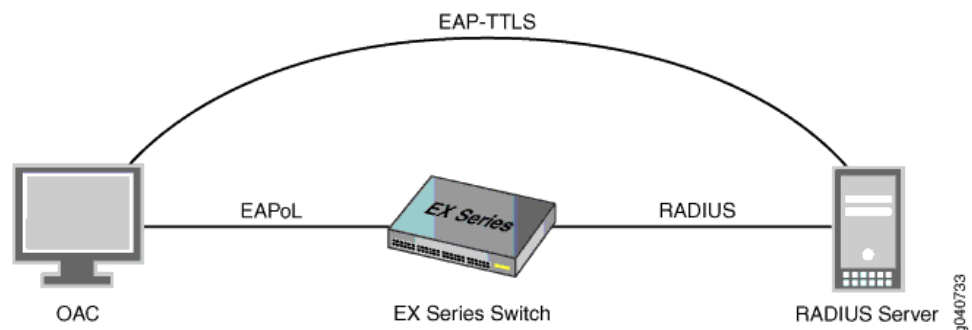


Table 12 on page 87 describes the components in this OAC deployment.

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

Table 12: Components of the OAC Deployment (*continued*)

Property	Settings
802.1X interface	ge-0/0/8
OAC supplicant	EAP-TTLS
One RADIUS authentication server	EAP-TTLS

Configuration

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

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

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



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

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


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


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


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


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


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


Results

Check the results of the configuration:

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

Verification

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

- [Verifying the Configuration of the 802.1X Interface on page 89](#)

Verifying the Configuration of the 802.1X Interface

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

Action user@switch> **show dot1x** interface ge-0/0/8.0 detail

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

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

- Related Documentation**
- [Understanding Authentication on EX Series Switches on page 19](#)

Controlling Authentication Session Timeouts (CLI Procedure)

For 802.1X and MAC RADIUS authentication sessions, you can specify authentication session timeout values by 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 by 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 an EX Series Switch \(CLI Procedure\)” on page 34](#).
- Configure 802.1X authentication on the switch. See [“Configuring 802.1X Interface Settings \(CLI Procedure\)” on page 32](#).

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-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 44](#)
 - [Understanding Authentication on EX Series Switches on page 19](#)
 - [Understanding Authentication Session Timeout on page 27](#)

Verifying 802.1X Authentication

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

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

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

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

Other 802.1X authentication methods supported on EX Series switches in addition to RADIUS authentication are:

- Guest VLAN—A nonresponsive host is granted Guest-VLAN access.
- MAC Radius—A nonresponsive host is authenticated based on its MAC address. The MAC address is configured as permitted on the RADIUS server, the RADIUS server notifies the switch that the MAC address is a permitted address, and the switch grants LAN access to the nonresponsive host on the interface to which it is connected.
- Server-fail deny—If the RADIUS servers time out, all supplicants are denied access to the LAN, preventing traffic from the supplicant from traversing through the interface. This is the default.

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

Related Documentation

- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 96](#)
- [Configuring RADIUS Server Fail Fallback \(CLI Procedure\) on page 42](#)

Monitoring 802.1X Authentication

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring feature to display details of authenticated users and users who have failed authentication.

Action

To display authentication details in the J-Web interface, select **Monitoring > Security > 802.1X**.

To display authentication details in the CLI, enter the following commands:

- `show dot1x interface detail | display xml`
- `show dot1x interface detail <interface> | display xml`
- `show dot1x auth-failed-users`

Meaning

The details displayed include:

- A list of authenticated users.
- The total number of users connected.
- A list of users who have failed authentication.

You can also specify an interface for which the details must be displayed.

Related Documentation

- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)

- [Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 44](#)

CHAPTER 3

Configuring MAC RADIUS Authentication to Control Network Access

- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 96](#)
- [Specifying RADIUS Server Connections on an EX Series Switch \(CLI Procedure\) on page 97](#)
- [Configuring RADIUS Server Fail Fallback \(CLI Procedure\) on page 98](#)
- [Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 100](#)
- [Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on page 106](#)
- [Controlling Authentication Session Timeouts \(CLI Procedure\) on page 112](#)

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 EX Series 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 EX Series switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 35.](#)

To configure MAC RADIUS authentication by using the CLI:

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

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

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

```
[root@freeradius]#
edit /etc/raddb
vi users
00040ffdacfe Auth-type:=Local, User-Password = "00040ffdacfe"
0004aecdc235f Auth-type:=Local, User-Password = "0004aecdc235f"
```


- Related Documentation**
- [Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 100](#)
 - [Verifying 802.1X Authentication on page 91](#)
 - [Understanding Authentication on EX Series Switches on page 19](#)

Specifying RADIUS Server Connections on an EX Series Switch (CLI Procedure)

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

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

To configure a RADIUS server on the switch:

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

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



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

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

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

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

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

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

```
[edit access profile profile-name]
user@switch# set radius authentication-server server-address server-address
```

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

[edit]

```
user@switch# set protocols dot1x authenticator authentication-profile-name  
access-profile-name
```

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

**Related
Documentation**

- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 96](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 83](#)

Configuring RADIUS Server Fail Fallback (CLI Procedure)

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

When you set up 802.1X or MAC RADIUS authentication on the switch, you specify a primary authentication server and one or more backup authentication servers. If the primary authentication server cannot be reached by the switch and the secondary authentication servers are also unreachable, a RADIUS server timeout occurs. If this happens, because it is the authentication server that grants or denies access to the end devices awaiting authentication, the switch does not receive access instructions for end devices attempting access to the LAN, and normal authentication cannot be completed.

You can configure the server fail fallback feature to specify an action that the switch applies to end devices when the authentication servers are unavailable. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN.

You can also configure the server reject fallback feature for end devices that receive a RADIUS access-reject message from the authentication server. The server reject fallback feature provides limited access to a LAN, typically only to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials.

Server fail fallback is supported for voice traffic starting in Release 14.1X53-D40 and Release 15.1R4. To configure server fail fallback actions for VoIP clients sending voice traffic, use the **server-fail-voip** statement. For all data traffic, use the **server-fail** statement. The switch determines the fallback method to use based on the type of traffic sent by the client. Untagged data frames are subject to the action configured with **server-fail**, even if they are sent by a VoIP client. Tagged VoIP VLAN frames are subject to the action configured with **server-fail-voip**. If **server-fail-voip** is not configured, the voice traffic is dropped.



NOTE: Server reject fallback is not supported for VoIP VLAN tagged traffic. If a VoIP client starts authentication by sending untagged data traffic to a VLAN while server reject fallback is in effect, the VoIP client is allowed to access the fallback VLAN. If the same client subsequently sends tagged voice traffic, the voice traffic is dropped.

If a VoIP client starts authentication by sending tagged voice traffic while server reject fallback is in effect, the VoIP client is denied access to the fallback VLAN.

You can use the following procedure to configure server fail actions for data clients. To configure server fail fallback for VoIP clients sending voice traffic, use the **server-fail-voip** statement in place of the **server-fail** statement.

To configure server fail fallback actions:

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

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

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

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

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

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

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

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

You can configure an interface that receives a RADIUS access-reject message from the authentication server to move end devices attempting LAN access on the interface to a server-reject VLAN, a specified VLAN already configured on the switch.

To configure a server reject fallback VLAN:

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

Release History Table

Release	Description
14.1X53-D40	Server fail fallback is supported for voice traffic starting in Release 14.1X53-D40 and Release 15.1R4.

Related Documentation

- [Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 67](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)
- [Monitoring 802.1X Authentication on page 92](#)
- [Understanding Server Fail Fallback and Authentication on EX Series Switches on page 28](#)

Example: Configuring MAC RADIUS Authentication on an EX Series Switch

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

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

- [Requirements on page 100](#)
- [Overview and Topology on page 101](#)
- [Configuration on page 103](#)
- [Verification on page 104](#)

Requirements

This example uses the following software and hardware components:

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

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

- Configured basic access between the EX Series switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 35](#).

- 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*. 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 32.

Overview and Topology

IEEE 802.1X port-based network access control (PNAC) authenticates and permits devices access to a LAN if the devices can communicate with the switch by using the 802.1X protocol (that is, the devices are 802.1X-enabled). To permit non-802.1X-enabled end devices to access the LAN, you can configure MAC RADIUS authentication on the interfaces to which the end devices are connected. When the MAC address of the end device appears on the interface, the switch consults the RADIUS server to check whether it is a permitted MAC address. If the MAC address of the end device is configured as permitted on the RADIUS server, the switch opens LAN access to the end device.

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

[Figure 11 on page 102](#) shows the two printers connected to the switch.

Figure 11: Topology for MAC RADIUS Authentication Configuration

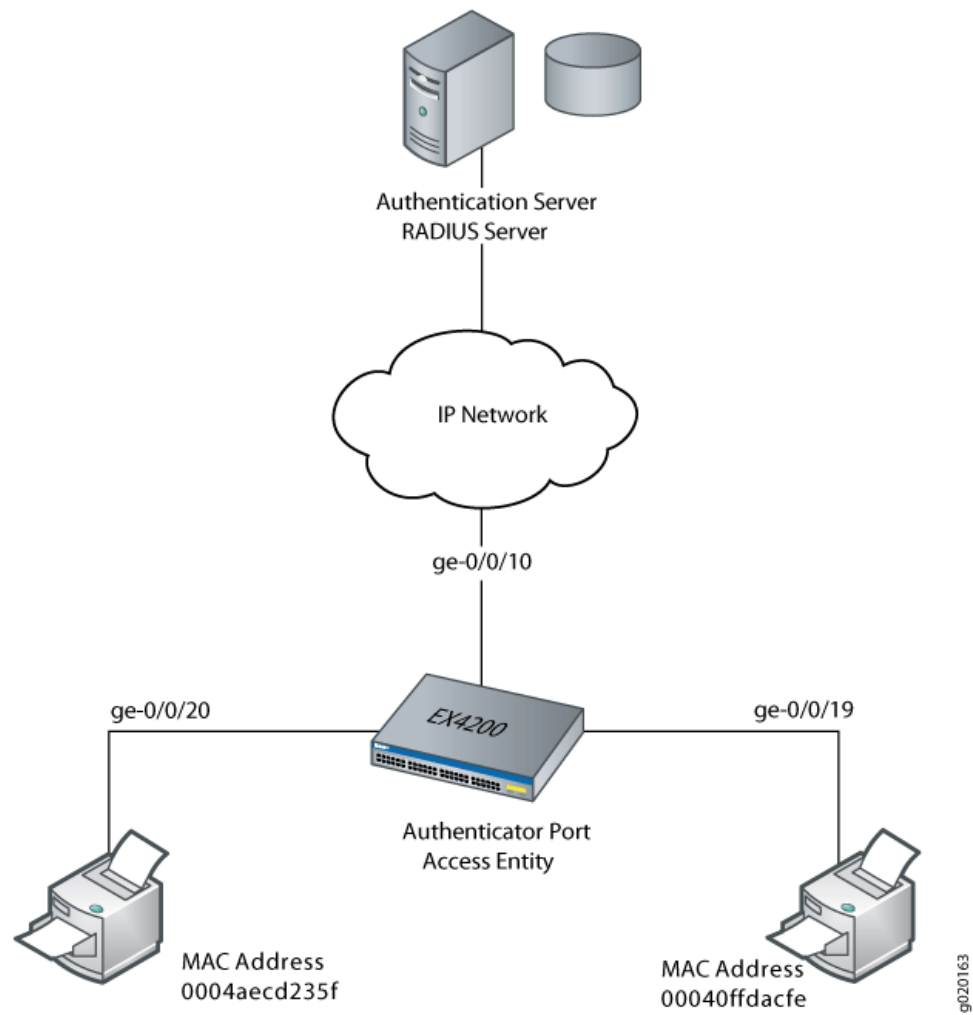


Table 13 on page 102 shows the components in the example for MAC RADIUS authentication.

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 0004aec235f
RADIUS server	Connected to the switch on interface ge-0/0/10

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

Configuration

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

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



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

Step-by-Step Procedure Configure MAC RADIUS authentication on the switch and on the RADIUS server:

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

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

2. On the RADIUS server, configure the MAC addresses 00040ffdacfe and 0004aecd235f as usernames and passwords:

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

Results Display the results of the configuration on the switch:

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

```
restrict;  
}  
}  
}  
}  
}
```

Verification

Verify that the supplicants are authenticated:

- [Verifying That the Supplicants Are Authenticated on page 104](#)

Verifying That the Supplicants Are Authenticated

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

Action Display information about the 802.1X-configured interfaces ge-0/0/19 and ge-0/0/20:

```

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

user@switch> show dot1x interface ge-0/0/20.0 detail
ge-0/0/20.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Enabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user102, 00:04:ae:cd:23:5f
      Operational state: Authenticated
      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 **Radius**. On interface ge-0/0/20, the MAC address is **00:04:ae:cd:23:5f**, which is the MAC address of the second printer configured for MAC

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

**Related
Documentation**

- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 96](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
- [Understanding Authentication on EX Series Switches on page 19](#)

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 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*.

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

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

- [Requirements on page 106](#)
- [Overview and Topology on page 107](#)
- [Configuration on page 109](#)
- [Verification on page 111](#)

Requirements

This example uses the following software and hardware components:

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

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

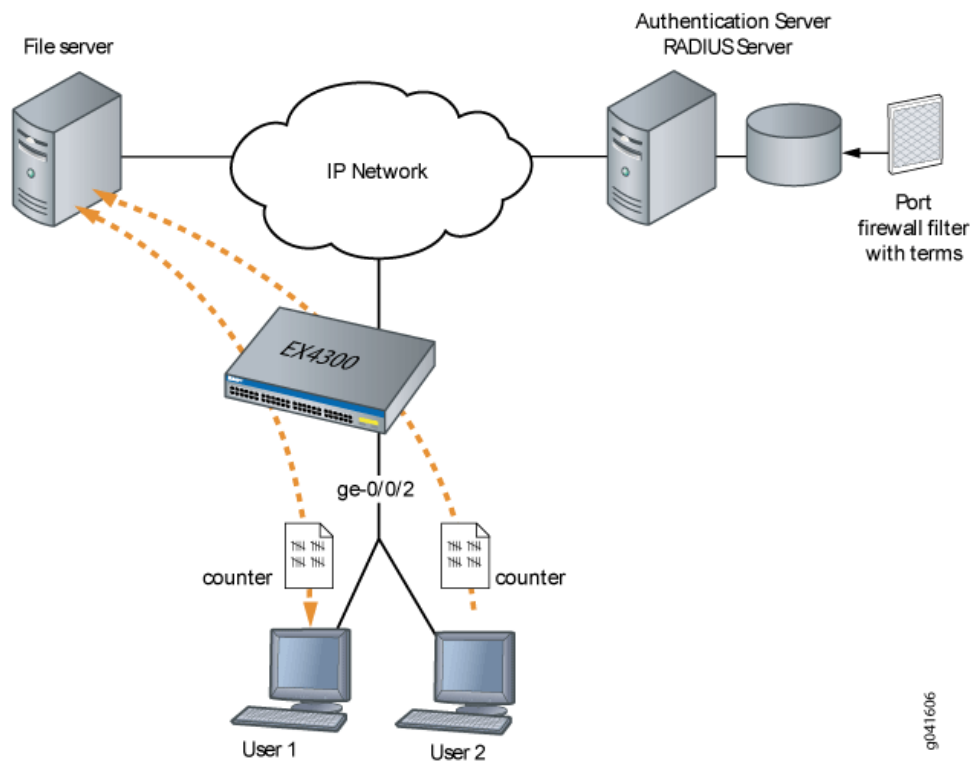
- Set up a connection between the switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch”](#) on page 35.
- Configured 802.1X authentication on the switch, with the authentication mode for the interface ge-0/0/2 set to **multiple**. See [“Configuring 802.1X Interface Settings \(CLI Procedure\)”](#) on page 32 and [“Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch”](#) on page 44.
- 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 6 on page 64](#), 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.

Figure 12: Conceptual Model: Dynamic Filter Updated for Each New User



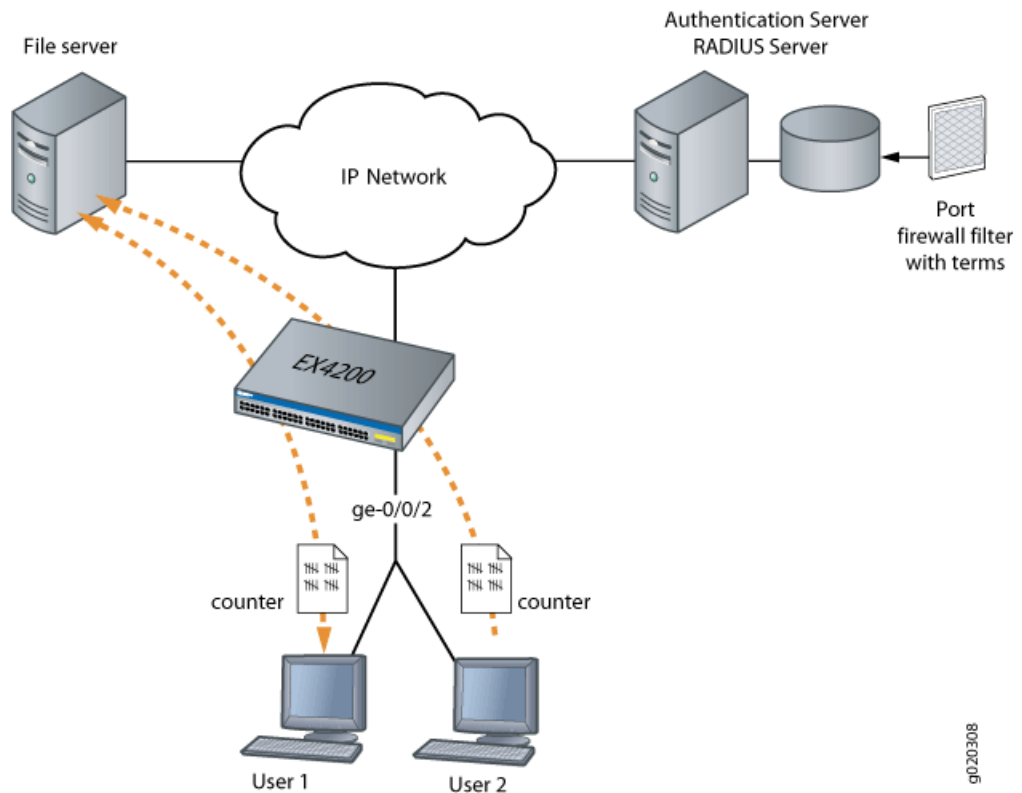
This is a conceptual model of the internal process—you cannot access or view the dynamic filter.



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 7 on page 65](#) shows the network topology for this example.

Figure 13: 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 by Using RADIUS Server Attributes on an EX Series Switch on page 56 • 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 52

Controlling Authentication Session Timeouts (CLI Procedure)

For 802.1X and MAC RADIUS authentication sessions, you can specify authentication session timeout values by 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 by 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 an EX Series Switch \(CLI Procedure\)”](#) on page 34.
- Configure 802.1X authentication on the switch. See [“Configuring 802.1X Interface Settings \(CLI Procedure\)”](#) on page 32.

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-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch](#) on page 44
- [Understanding Authentication on EX Series Switches](#) on page 19
- [Understanding Authentication Session Timeout](#) on page 27

Configuring Captive Portal Authentication to Control Network Access

- [Configuring Captive Portal Authentication \(CLI Procedure\) on page 113](#)
- [Designing a Captive Portal Authentication Login Page on an EX Series Switch on page 115](#)
- [Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 117](#)

Configuring Captive Portal Authentication (CLI Procedure)



NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Configuring Captive Portal Authentication (CLI Procedure)*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

Configure captive portal authentication (hereafter referred to as captive portal) on an EX Series switch so that users connected to the switch are authenticated before being allowed to access the network. When the user requests a webpage, a login page is displayed that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.
- Generated an SSL certificate and installed it on the switch. See *Generating SSL Certificates to Be Used for Secure Web Access*.

- Configured basic access between the EX Series switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 35.](#)
- Designed your captive portal login page. See [“Designing a Captive Portal Authentication Login Page on an EX Series Switch” on page 115.](#)

This topic includes the following tasks:

- [Configuring Secure Access for Captive Portal on page 114](#)
- [Enabling an Interface for Captive Portal on page 114](#)
- [Configuring Bypass of Captive Portal Authentication on page 114](#)

Configuring Secure Access for Captive Portal

To configure secure access for captive portal:

1. Associate the security certificate with the Web server and enable HTTPS on the switch:

```
[edit]
user@switch# set system services web-management https local-certificate certificate-name
```



NOTE: You can enable HTTP instead of HTTPS, but we recommend HTTPS for security purposes.

2. Configure captive portal to use HTTPS:

```
[edit]
user@switch# set services captive-portal secure-authentication https
```

Enabling an Interface for Captive Portal

To enable an interface for use with captive portal authentication:

```
[edit]
user@switch# set services captive-portal interface interface-name
```

Configuring Bypass of Captive Portal Authentication

You can allow specific clients to bypass captive portal authentication:

```
[edit]
user@switch# set switch-options authentication-whitelist mac-address
```



NOTE: Optionally, you can use `set switch-options authentication-whitelist mac-address interface interface-name` to limit the scope to the interface.



NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address session-mac-addr` command after adding its MAC address to the whitelist. Otherwise, the new entry for the MAC address is not added to the Ethernet switching table and the authentication bypass is not allowed.

- Related Documentation**
- [Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 117](#)
 - [Understanding Authentication on EX Series Switches on page 19](#)

Designing a Captive Portal Authentication Login Page on an EX Series Switch

You can set up captive portal authentication on your switch to redirect all Web browser requests to a login page that requires users to input a username and password before they are allowed access. Upon successful authentication, users are allowed access to the network and redirected to the original page requested.

Junos OS provides a customizable template for the captive portal window that allows you to easily design and modify the look of the captive portal login page. You can modify the design elements of the template to change the look of your captive portal login page and to add instructions or information to the page. You can also modify any of the design elements of a captive portal login page.

The first screen displayed before the captive login page requires the user to read the terms and conditions of use. By clicking the Agree button, the user can access the captive portal login page.

Figure 14 on page 115 shows an example of a captive portal login page:

Figure 14: Example of a Captive Portal Login Page

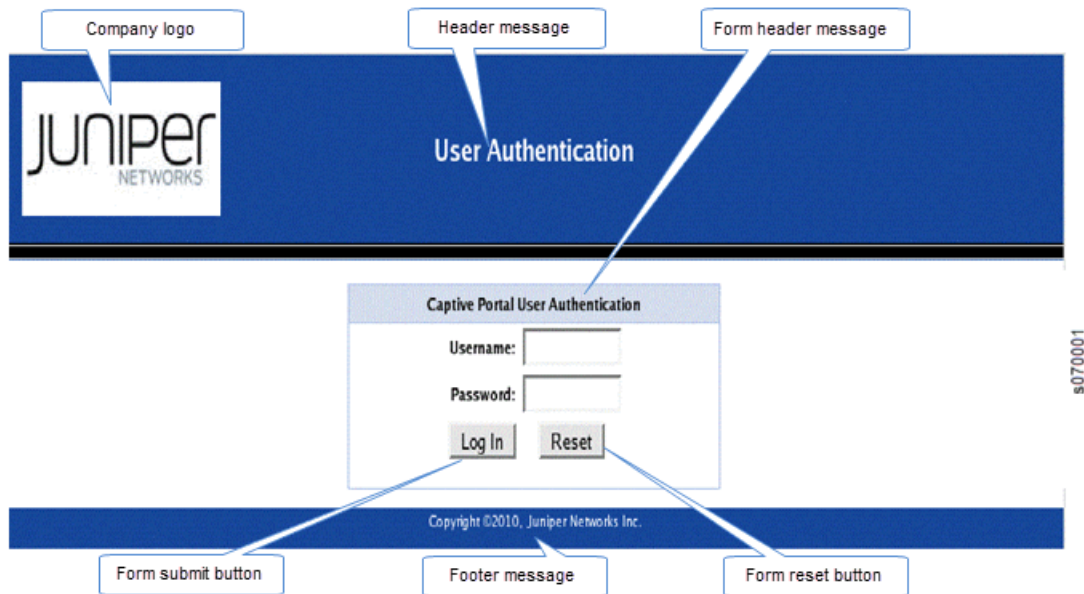


Table 14 on page 116 summarizes the configurable elements of a captive portal login page.

Table 14: Configurable Elements of a Captive Portal Login Page

Element	CLI Statement	Description
Footer background color	footer-bgcolor <i>hex-color</i>	The HTML hexadecimal code for the background color of the captive portal login page footer.
Footer message	footer-message <i>text-string</i>	Text displayed in the footer of the captive portal login page. You can include copyright information, links, and additional information such as help instructions, legal notices, or a privacy policy. The default text shown in the footer is Copyright ©2010, Juniper Networks Inc.
Footer text color	footer- text-color <i>color</i>	Color of the text in the footer. The default color is white.
Form header background color	form-header-bgcolor <i>hex-color</i>	The HTML hexadecimal code for the background color of the header bar across the top of the form area of the captive portal login page.
Form header message	form-header-message <i>text-string</i>	Text displayed in the header of the captive portal login page. The default text is Captive Portal User Authentication .
Form header text color	form-header- text- color <i>color</i>	Color of the text in the form header. The default color is black.
Form reset button label	form-reset-label <i>label-name</i>	Using the Reset button, the user can clear the username and password fields on the form.
Form submit button label	form-submit-label <i>label-name</i>	Using the Login button, the user can submit the login information.
Header background color	header-bgcolor <i>hex-color</i>	The HTML hexadecimal code for the background color of the captive portal login page header.
Header logo	header-logo <i>filename</i>	Filename of the file containing the image of the logo that you want to appear in the header of the captive portal login page. The image file can be in GIF, JPEG, or PNG format. You can upload a logo image file to the switch. Copy the logo to the /var/tmp directory on the switch (during commit, the files are saved to persistent locations). If you do not specify a logo image, the Juniper Networks logo is displayed.
Header message	header-message <i>text-string</i>	Text displayed in the page header. The default text is User Authentication .
Header text color	header-text- color <i>color</i>	Color of the text in the header. The default color is white.
Post-authentication URL	post-authentication-url <i>url</i>	URL to which the users are directed on successful authentication. By default, users are directed to the page they had originally requested.

To design the captive portal login page:

1. (Optional) Upload your logo image file to the switch:

- ```
user@switch> file copy ftp://username:prompt@ftp.hostname.net/var/tmp/my-logo.jpeg
```
2. Configure the custom options to specify the background colors and text displayed in the captive portal page:

```
[edit system services captive-portal]
user@switch# set custom-options header-bgcolor #006600
set custom-options header-message "Welcome to Our Network"
set custom-options banner-message "Please enter your username and password".The banner
displays the message "XXXXXXX" by default. The user can modify this message.
set custom-options footer-message "Copyright ©2010, Our Network"
```

Now you can commit the configuration.



**NOTE:** For the custom options that you do not specify, the default value is used.

#### Related Documentation

- [Example: Setting Up Captive Portal Authentication on an EX Series Switch](#)
- [Understanding Authentication on EX Series Switches on page 19](#)
- [captive-portal](#)

## Example: Setting Up Captive Portal Authentication on an EX Series Switch



**NOTE:** This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Example: Setting Up Captive Portal Authentication on an EX Series Switch*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

You can set up captive portal authentication (hereafter referred to as captive portal) on a switch to redirect Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

This example describes how to set up captive portal on an EX Series switch:

- [Requirements on page 117](#)
- [Overview and Topology on page 118](#)
- [Configuration on page 118](#)
- [Verification on page 120](#)
- [Troubleshooting on page 121](#)

## Requirements

This example uses the following software and hardware components:

- Junos OS Release 13.2X50 or later for EX Series switches

- An EX Series switch with support for ELS

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.
- Generated an SSL certificate and installed it on the switch. See *Generating SSL Certificates to Be Used for Secure Web Access*.
- Configured basic access between the EX Series switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 35](#).
- Designed your captive portal login page. See [“Designing a Captive Portal Authentication Login Page on an EX Series Switch” on page 115](#).

## Overview and Topology

This example shows the configuration required on the switch to enable captive portal on an interface. To permit a printer connected to the captive portal interface to access the LAN, add its MAC address to the authentication whitelist and assign it to a VLAN, vlan1. The MAC addresses on this list are permitted access on the interface without captive portal authentication.

The topology for this example consists of one EX Series switch connected to a RADIUS authentication server. One interface on the switch is configured for captive portal. In this example, the interface is configured in multiple supplicant mode.

## Configuration

To configure captive portal on your switch:

### CLI Quick Configuration

To quickly configure captive portal on the switch after completing the tasks in the Requirements section, copy the following commands and paste them into the switch terminal window:

```
[edit]
set system services web-management https local-certificate my-signed-cert
set services captive-portal secure-authentication https
set services captive-portal interface ge-0/0/10.0 supplicant multiple
set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment vlan1
set custom-options post-authentication-url http://www.my-home-page.com
```

### Step-by-Step Procedure

1. To create a secure channel for Web access to the switch, configure captive portal for HTTPS:
  - a. Associate the security certificate with the Web server and enable HTTPS on the switch:

```
[edit]
user@switch# set system services web-management https local-certificate
my-signed-cert
```



**NOTE:** You can enable HTTP instead of HTTPS, but we recommend that you enable HTTPS for security purposes.

- b. Configure captive portal to use HTTPS:

```
[edit]
user@switch# set services captive-portal secure-authentication https
```

2. Enable an interface for captive portal:

```
[edit]
user@switch# set services captive-portal interface ge-0/0/10 supplicant multiple
```

3. (Optional) Allow specific clients to bypass captive portal authentication:



**NOTE:** If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address mac-address` command after adding its MAC address to the whitelist. Otherwise, the new entry for the MAC address will not be added to the Ethernet switching table and the authentication bypass will not be allowed.

```
[edit]
user@switch# set switch-options authentication-whitelist 00:10:12:e0:28:22
vlan-assignment vlan1
```



**NOTE:** Optionally, you can use `set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment vlan1 interface ge-0/0/10.0` to limit the scope to the interface.

4. (Optional) To redirect clients to a specified page rather than the page they originally requested, configure the post-authentication URL:

```
[edit services captive-portal]
user@switch# set custom-options post-authentication-url http://www.my-home-page.com
```

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

```
[edit]
user@switch# show
system {
 services {
 web-management {
 https {
 local-certificate my-signed-cert;
 }
 }
 }
}
security {
 certificates {
 local {
 my-signed-cert {
 "-----BEGIN RSA PRIVATE KEY-----\ABC123
 ABC123ABC123ABC123 ... ABC123
 ----END CERTIFICATE-----\n"; ## SECRET-DATA
```

```
 }
 }
}
services {
 captive-portal {
 interface {
 ge-0/0/10.0 {
 supplicant multiple;
 }
 }
 secure-authentication https;
 custom-options {
 post-authentication-url http://www.my-home-page.com;
 }
 }
}
switch-options {
 authentication-whitelist {
 00:10:12:e0:28:22/48 {
 vlan-assignment vlan1;
 }
 }
}
```

## Verification

To confirm that captive portal authentication is configured and working properly, perform these tasks:

- [Verifying That Captive Portal Is Enabled on the Interface on page 120](#)
- [Verify That Captive Portal Is Working Correctly on page 121](#)

---

### Verifying That Captive Portal Is Enabled on the Interface

**Purpose** Verify that captive portal is configured on the interface `ge-0/0/10`.

**Action** Use the operational mode command `show captive-portal interface interface-name detail`:

```
user@switch> show captive-portal interface ge-0/0/10.0 detail
ge-0/0/10.0
 Supplicant mode: Multiple
 Number of retries: 3
 Quiet period: 60 seconds
 Configured CP session timeout: 3600 seconds
 Server timeout: 15 seconds
```

**Meaning** The output confirms that captive portal is configured on the interface `ge-0/0/10`, with the default settings for number of retries, quiet period, CP session timeout, and server timeout.



### Verify That Captive Portal Is Working Correctly

- Purpose** Verify that captive portal is working on the switch.
- Action** Connect a client to the interface ge-0/0/10. From the client, open a Web browser and request a webpage. The captive portal login page that you designed should be displayed. After you enter your login information and are authenticated against the RADIUS server, the Web browser should display either the page you requested or the post-authentication URL that you configured.

## Troubleshooting

To troubleshoot captive portal, perform this task:

- [Troubleshooting Captive Portal on page 121](#)

### Troubleshooting Captive Portal

- Problem** The switch does not return the captive portal login page when a user connected to a captive portal interface on the switch requests a webpage.
- Solution** You can examine the ARP, DHCP, HTTPS, and DNS counters—if one or more of these counters are not incrementing, this provides an indication of where the problem lies. For example, if the client cannot get an IP address, you might check the switch interface to determine whether the DHCP counter is incrementing—if the counter increments, the DHCP packet was received by the switch.

```
user@switch> show captive-portal firewall ge-0/0/10.0
ge-0/0/10.0
 Filter name: dot1x_ge-0/0/10
Counters:

Name	Bytes	Packets
dot1x_ge-0/0/10_CP_arp	7616	119
dot1x_ge-0/0/10_CP_dhcp	0	0
dot1x_ge-0/0/10_CP_http	0	0
dot1x_ge-0/0/10_CP_https	0	0
dot1x_ge-0/0/10_CP_t_dns	0	0
dot1x_ge-0/0/10_CP_u_dns	0	0


```

- Related Documentation**
- [Configuring Captive Portal Authentication \(CLI Procedure\) on page 113](#)
  - [Designing a Captive Portal Authentication Login Page on an EX Series Switch on page 115](#)



## CHAPTER 5

# Configuring Central Web Authentication to Control Network Access

- [Understanding Central Web Authentication on page 123](#)
- [Configuring Central Web Authentication on page 125](#)

## Understanding Central Web Authentication

---

Web authentication redirects Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed access to the network. Web authentication is useful for providing network access to temporary users, such as visitors to a corporate site, who try to access the network using devices that are not 802.1X-enabled. Web authentication can also be used as a fallback authentication method for regular network users who have 802.1X-enabled devices, but fail authentication because of other issues, such as expired network credentials.

Web authentication can be done locally on the switch using captive portal, but this requires that the Web portal pages be configured on each switch used as a network access device. Central Web authentication (CWA) provides efficiency and scaling benefits by redirecting the client's Web browser to a central Web authentication server (CWA server), which handles the complete login process.

- [Central Web Authentication Process on page 123](#)
- [Dynamic Firewall Filters for Central Web Authentication on page 125](#)
- [Redirect URL for Central Web Authentication on page 125](#)

## Central Web Authentication Process

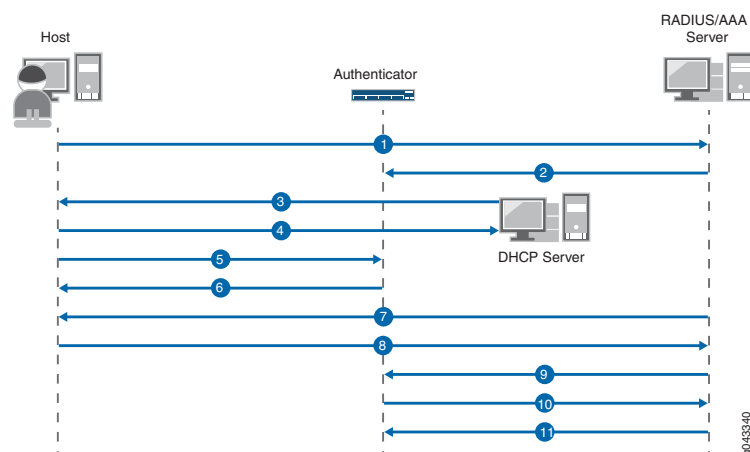
Central Web authentication is invoked after a host has failed MAC RADIUS authentication. The host can attempt authentication using 802.1X authentication first, but must then attempt MAC RADIUS authentication before attempting central Web authentication. The switch, operating as the authenticator, exchanges RADIUS messages with the authentication, authorization, and accounting (AAA) server. After MAC RADIUS authentication fails, the switch receives an Access-Accept message from the AAA server. This message includes a dynamic firewall filter and a redirect URL for central Web authentication. The switch applies the filter, which allows the host to receive an IP address, and uses the URL to redirect the host to the Web authentication page.

The host is prompted for login credentials and might also be asked to agree to an acceptable use policy. If Web authentication is successful, the AAA server sends a Change of Authorization (CoA) message, which updates the terms of the authorized session in progress. This enables the authenticator to update the filter or VLAN assignment applied to the controlled port, to allow the host to access the LAN.

The sequence of events in central Web authentication is as follows (see [Figure 15 on page 124](#)):

1. A host connected to the switch (authenticator) initiates MAC RADIUS authentication.
2. MAC RADIUS authentication fails. Instead of sending an Access-Reject message to the switch, the AAA server sends an Access-Accept message that includes a dynamic firewall filter and a CWA redirect URL.
3. The host is allowed by the terms of the filter to send DHCP requests.
4. The host receives an IP address and DNS information from the DHCP server. The AAA server initiates a new session that has a unique session ID.
5. The host opens a Web browser.
6. The authenticator sends the CWA redirect URL to the host.
7. The host is redirected to the CWA server and is prompted for login credentials.
8. The host provides the username and password.
9. After successful Web authentication, the AAA server sends a CoA message to update the filter or VLAN assignment applied on the controlled port, allowing the host to access the LAN.
10. The authenticator responds with a CoA-ACK message and sends a MAC RADIUS authentication request to the AAA server.
11. The AAA server matches the session ID to the appropriate access policy and sends an Access-Accept message to authenticate the host.

**Figure 15: Central Web Authentication Process**



## Dynamic Firewall Filters for Central Web Authentication

Central Web authentication uses dynamic firewall filters, which are centrally defined on the AAA server and dynamically applied to supplicants that request authentication through that server. The filter allows the host to get an IP address dynamically using DHCP. You define the filters by using RADIUS attributes, which are included in the Access-Accept messages sent from the server. Filters can be defined using either the Juniper-Switching-Filter attribute, which is a vendor-specific attribute (VSA), or the Filter-ID attribute, which is an IETF RADIUS attribute.

To use the Juniper-Switching-Filter VSA for central Web authentication, you must configure the filter with the correct terms that allow the destination IP address of the CWA server. This configuration is done directly on the AAA server. To use the Filter-ID attribute for central web authentication, enter the value as JNPR\_RSVD\_FILTER\_CWA on the AAA server. The filter terms for this attribute are internally defined for central Web authentication, because of which no additional configuration is required. For more information about configuring dynamic firewall filters for central web authentication, see [“Configuring Central Web Authentication” on page 125](#).

## Redirect URL for Central Web Authentication

In central Web authentication, the authenticator redirects the host's Web browser request to the CWA server by using a redirect URL. After redirection, the CWA server completes the login process. The redirect URL for central web authentication can be configured on the AAA server or on the authenticator. The redirect URL, along with the dynamic firewall filter, must be present to trigger the central web authentication process after the failure of MAC RADIUS authentication.

The redirect URL can be centrally defined on the AAA server by using the Juniper-CWA-Redirect VSA, which is attribute number 50 in the Juniper RADIUS dictionary. The URL is forwarded from the AAA server to the switch in the same RADIUS Access-Accept message that contains the dynamic firewall filter. You can also configure the redirect URL locally on the host interface by using the CLI statement **redirect-url** at the **[edit protocols dot1x authenticator interface *interface-name*]** hierarchy level. For more information about configuring the redirect URL, see [“Configuring Central Web Authentication” on page 125](#).

### Related Documentation

- [Understanding Dynamic Filters Based on RADIUS Attributes on page 49](#)
- [Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 84](#)
- [Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 52](#)
- [Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass](#)

---

## Configuring Central Web Authentication

Central Web authentication is a fallback method of authentication in which the host's Web browser is redirected to a central Web authentication (CWA) server. The CWA server provides a web portal where the user can enter a username and password. If these

credentials are validated by the CWA server, the user is authenticated and is allowed access to the network.

Central Web authentication is invoked after a host has failed MAC RADIUS authentication. The switch, operating as the authenticator, receives a RADIUS Access-Accept message from the AAA server that includes a dynamic firewall filter and a redirect URL for central Web authentication. The dynamic firewall filter and the redirect URL must both be present for the central Web authentication process to be triggered.

- [Configuring Dynamic Firewall Filters for Central Web Authentication on page 126](#)
- [Configuring the Redirect URL for Central Web Authentication on page 127](#)
- [Guidelines for Configuring Central Web Authentication on page 128](#)

## Configuring Dynamic Firewall Filters for Central Web Authentication

Dynamic firewall filters are used in central Web authentication to enable the host to get an IP address from a DHCP server, which allows the host to access the network. The filters are defined on the AAA server using RADIUS attributes, which are sent to the authenticator in an Access-Accept message. You can define the filter using either the Juniper-Switching-Filter attribute, which is a vendor-specific attribute (VSA), or the Filter-ID attribute, which is an IETF RADIUS attribute.

- To use the Juniper-Switching-Filter VSA for central Web authentication, you must configure the filter terms directly on the AAA server. The filter must include a term to match the destination IP address of the CWA server with the action **allow**.

For example:

```
001122334455 Auth-Type := EAP, Cleartext-Password := "001122334455"
 Session-Timeout = "300",
 Juniper-CWA-Redirect-URL = "https://10.10.10.10",
 Juniper-Switching-Filter = "Match Destination-ip 10.10.10.10 Action
allow, Match ip-protocol 17 Action allow, Match Destination-mac 00:01:02:33:44:55
Action deny"
```



**NOTE:** The switch does not resolve the DNS queries for the redirect URL. You must configure the Juniper-Switching-Filter attribute to allow the destination IP address of the CWA server.

- To use the Filter-ID attribute for central Web authentication, enter JNPR\_RSVD\_FILTER\_CWA as the value for the attribute on the AAA server. The filter terms for this attribute are internally defined for central Web authentication, because of which no additional configuration is required.

For example:

```
001122334455 Auth-Type := EAP, Cleartext-Password := "001122334455"
 Session-Timeout = "300",
 Juniper-CWA-Redirect-URL = "https://10.10.10.10",
 Filter-Id = "JNPR_RSVD_FILTER_CWA",
```

For more information about configuring dynamic firewall filters on the AAA server, see the documentation for your AAA server.

## Configuring the Redirect URL for Central Web Authentication

In central Web authentication, the authenticator redirects the host's Web browser request to the CWA server by using a redirect URL. The redirect URL for central Web authentication can be configured on the AAA server or locally on the host interface.

- To configure the redirect URL on the AAA server, use the Juniper-CWA-Redirect VSA, which is attribute number 50 in the Juniper RADIUS dictionary. The URL is forwarded from the AAA server to the switch in the same RADIUS Access-Accept message that contains the dynamic firewall filter.

For example:

```
001122334455 Auth-Type := EAP, Cleartext-Password := "001122334455"
 Session-Timeout = "300",
 Juniper-CWA-Redirect-URL = "https://10.10.10.10",
 Filter-Id = "JNPR_RSVD_FILTER_CWA",
```



**NOTE:** When the special Filter-ID attribute JNPR\_RSVD\_FILTER\_CWA is used for the dynamic firewall filter, the redirect URL must include the IP address of the AAA server, for example, <https://10.10.10.10>.

- To configure the redirect URL locally on the host interface, use the following CLI statement:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name redirect-url
```

For example:

```
user@switch# show protocols dot1x
authenticator {
 authentication-name-profile auth1;
 interface {
 ge-0/0/1.0 {
 supplicant single;
 mac-radius;
 redirect-url https://10.10.10.10;
 }
 }
}
```

## Guidelines for Configuring Central Web Authentication

Central Web authentication is triggered after the failure of MAC RADIUS authentication when the redirect URL and dynamic firewall filter are both present. The redirect URL and dynamic firewall filter can be configured in any of the following combinations:

1. The AAA server sends both the CWA redirect URL and dynamic firewall filter to the authenticator. The redirect URL is configured on the AAA server by using the Juniper-CWA-Redirect VSA and the dynamic firewall filter is configured on the AAA server by using the Juniper-Switching-Filter VSA. The filter must be configured to allow the destination IP address of the CWA server in this case.
2. The AAA server sends the dynamic firewall filter to the authenticator and the redirect URL is configured locally on the host port. The redirect URL is configured on the authenticator by using the **redirect-url** CLI statement and the dynamic firewall filter is configured on the AAA server by using the Juniper-Switching-Filter VSA. The filter must be configured to allow the destination IP address of the CWA server in this case.
3. The AAA server sends both the CWA redirect URL and dynamic firewall filter to the authenticator. The redirect URL is configured on the AAA server by using the Juniper-CWA-Redirect VSA and the dynamic firewall filter is configured on the AAA server by using the Filter-ID attribute with the value JNPR\_RSVD\_FILTER\_CWA. The redirect URL must contain the IP address of the CWA server in this case.
4. The AAA server sends the dynamic firewall filter to the authenticator and the redirect URL is configured locally on the host port. The redirect URL is configured on the authenticator by using the **redirect-url** CLI statement and the dynamic firewall filter is configured on the AAA server by using the Filter-ID attribute with the value JNPR\_RSVD\_FILTER\_CWA. The redirect URL must contain the IP address of the CWA server in this case.

### Related Documentation

- [Understanding Central Web Authentication on page 123](#)
- [Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass](#)



## CHAPTER 6

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

- [Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication \(CLI Procedure\) on page 129](#)
- [Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 130](#)

## Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication (CLI Procedure)

---

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

To configure the static MAC bypass list:

- Specify a MAC address to bypass authentication:  

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

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

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

### Related Documentation

- [Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 130](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)

## Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch

---

To allow devices to access your LAN through 802.1X-configured interfaces without authentication, you can configure a static MAC bypass list on the EX Series switch. The static MAC bypass list, also known as the *exclusion list*, specifies MAC addresses that are allowed on the switch without sending a request to an authentication server.

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

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

- [Requirements on page 130](#)
- [Overview and Topology on page 130](#)
- [Configuration on page 132](#)
- [Verification on page 133](#)

### Requirements

This example uses the following software and hardware components:

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

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

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

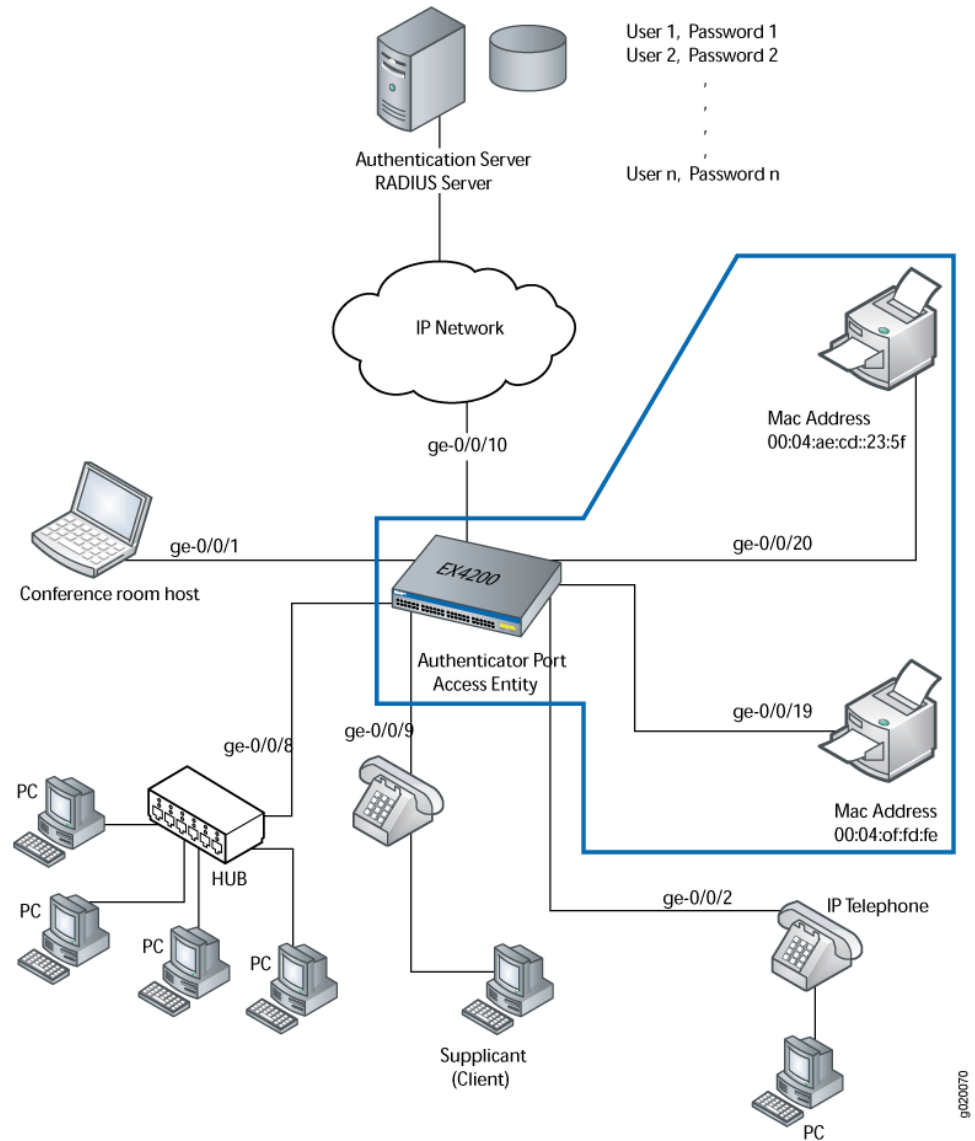
- Specified the RADIUS server connections and configured an access profile on the switch. See “[Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch](#)” on page 35.

### 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 16 on page 131 shows the two printers connected to the EX4200.

Figure 16: Topology for Static MAC Bypass of Authentication Configuration



The interfaces shown in Table 15 on page 131 will be configured for static MAC bypass of authentication.

Table 15: Components of the Static MAC Bypass of Authentication Configuration Topology

| Property        | Settings                                                                                         |
|-----------------|--------------------------------------------------------------------------------------------------|
| Switch hardware | EX4200, 24 Gigabit Ethernet ports: 16 non-PoE ports and 8 PoE ports (ge-0/0/0 through ge-0/0/23) |
| VLAN name       | default                                                                                          |

**Table 15: Components of the Static MAC Bypass of Authentication Configuration Topology** (*continued*)

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

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

## Configuration

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

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

**Step-by-Step Procedure** Configure the static MAC bypass list:

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

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

2. Configure the 802.1X authentication method:

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

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

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



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

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

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

```

ge-0/0/20 {
 unit 0 {
 family ethernet-switching {
 vlan members default;
 }
 }
}
protocols {
 dot1x {
 authenticator {
 authentication-profile-name profile1
 static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f];
 interface {
 all {
 supplicant multiple;
 }
 }
 }
 }
}
}

```

## Verification

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

- [Verifying Static MAC Bypass of Authentication on page 133](#)

### Verifying Static MAC Bypass of Authentication

**Purpose** Verify that the MAC addresses of both printers are configured and associated with the correct interfaces.

**Action** Issue the operational mode command:

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

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

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

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

- Related Documentation**
- [Configuring 802.1X Authentication \(J-Web Procedure\)](#)
  - [Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication \(CLI Procedure\) on page 129](#)
  - [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)

- [Understanding Authentication on EX Series Switches on page 19](#)

## CHAPTER 7

# Configuring Device Discovery Using LLDP and LLDP-MED

- [Understanding LLDP and LLDP-MED on EX Series Switches on page 135](#)
- [Configuring LLDP \(CLI Procedure\) on page 138](#)
- [Configuring LLDP-MED \(CLI Procedure\) on page 141](#)

### Understanding LLDP and LLDP-MED on EX Series Switches

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

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

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



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

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

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

TLVs fall into the following categories: basic management TLVs, organizationally defined TLVs, and LLDP-MED related TLVs.

EX Series switches support the following basic management TLVs:

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



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

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

EX Series switches support the following organizationally defined TLVs:

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





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

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

EX Series switches support the following LLDP-MED TLVs:

- LLDP MED Capabilities—A TLV that advertises the primary function of the port. The values of capabilities range from 0 through 15:
  - 0—Capabilities
  - 1—Network Policy
  - 2—Location Identification
  - 3—Extended Power via MDI-PSE
  - 4—Inventory
  - 5-15—Reserved
- LLDP-MED Device Class Values—Categorizes media endpoint devices into classes:
  - 0—Class not defined
  - 1—Class 1 (generic endpoints). This class definition is applicable to all endpoints that require the base LLDP discovery services.
  - 2—Class 2 (media endpoints). This class includes endpoints that have IP media capabilities.
  - 3—Class 3 (communication endpoints). Devices acting as end user communication appliances
  - 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 138](#)
  - [Configuring LLDP-MED \(CLI Procedure\) on page 141](#)
  - [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 138](#)
- [Adjusting LLDP Advertisement Settings on page 139](#)
- [Adjusting SNMP Notification Settings of LLDP Changes on page 139](#)
- [Specifying a Management Address for the LLDP Management TLV on page 140](#)
- [Configuring LLDP Power Negotiation on page 140](#)

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

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

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

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

For example:

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



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

## Adjusting SNMP Notification Settings of LLDP Changes

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

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

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

For example:

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

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

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

For example:

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

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

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

For example:

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

## Specifying a Management Address for the LLDP Management TLV

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

To configure the management address:

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



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

## Configuring LLDP Power Negotiation

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



**NOTE:** LLDP power negotiation is not supported on EX3200 or EX4200 switches (except for the EX4200-PX models).

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

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

- [edit poe]  
user@switch# **set management class**

To disable LLDP power negotiation:

- On switch interfaces:  
  
[edit protocols lldp interface all power-negotiation]  
user@switch# **disable**
- On a specific switch interface:  
  
[edit protocols lldp interface *interface-name* power-negotiation]  
user@switch# **disable**

#### Related Documentation

- [Configuring LLDP \(J-Web Procedure\)](#)
- [Configuring LLDP-MED \(CLI Procedure\) on page 141](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 135](#)

---

## Configuring LLDP-MED (CLI Procedure)

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

LLDP-MED is enabled by default on EX Series switches.

This topic describes:

- [Enabling LLDP-MED on Interfaces on page 141](#)
- [Configuring Location Information Advertised by the Switch on page 142](#)
- [Configuring a Fast Start for LLDP-MED on page 142](#)

### Enabling LLDP-MED on Interfaces

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



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

## Configuring Location Information Advertised by the Switch

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

- To specify a location by geography:

```
[edit protocols lldp-med]
user@switch# set interface ge-0/0/2.0 location civic-based country-code country-code
user@switch# set interface ge-0/0/2.0 location civic-based ca-type ca-type ca-value ca-value
```

- To specify a location by using an elin string:

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

## Configuring a Fast Start for LLDP-MED

When the switch detects an LLDP-MED capable device, it begins to send LLDP advertisements from the port connected to the device. The fast start count indicates how many advertisements will be sent in the first second after the switch detects the LLDP-MED device. The default is 3; to set it to another value:

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

For example:

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



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

### 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 an EX Series Switch on page 145](#)
- [Configuring LLDP \(CLI Procedure\) on page 138](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 135](#)

## CHAPTER 8

# Configuring VoIP

- [Understanding 802.1X and VoIP on EX Series Switches on page 143](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 145](#)
- [Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication on page 154](#)

### Understanding 802.1X and VoIP on EX Series Switches

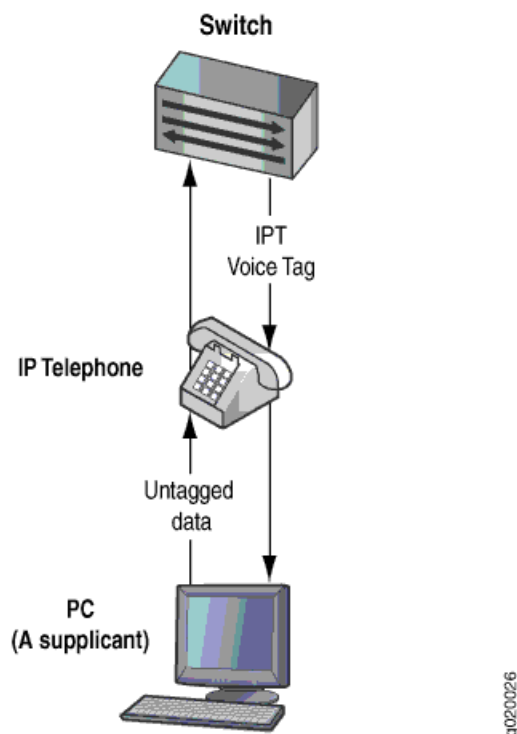
When you use VoIP, you can connect IP telephones to the switch and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. The 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.

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

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

You can configure 802.1X authentication to work with VoIP in multiple supplicant or single supplicant mode. In *multiple supplicant* mode, the 802.1X process allows multiple supplicants to connect to the interface. Each supplicant is authenticated individually. For an example of a VoIP multiple supplicant topology, see [Figure 17 on page 144](#).

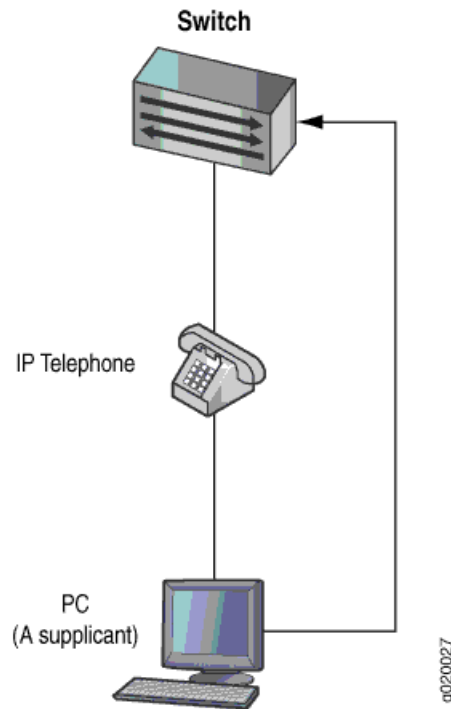
Figure 17: VoIP Multiple Supplicant Topology



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 18 on page 145](#).



Figure 18: 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 LLDP and LLDP-MED on EX Series Switches on page 135](#)
- [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 an EX Series Switch



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

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

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

- [Requirements on page 146](#)
- [Overview and Topology on page 147](#)
- [Configuration on page 149](#)
- [Verification on page 151](#)

## Requirements

This example uses the following software and hardware components:

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

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See the installation information for your switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.
- Configured the RADIUS server for 802.1X authentication and set up the access profile. See [“Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 35](#).
- (Optional) Configured the interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant uses a power adapter. For information about configuring PoE, see *Configuring PoE on EX Series Switches (CLI Procedure)*.



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

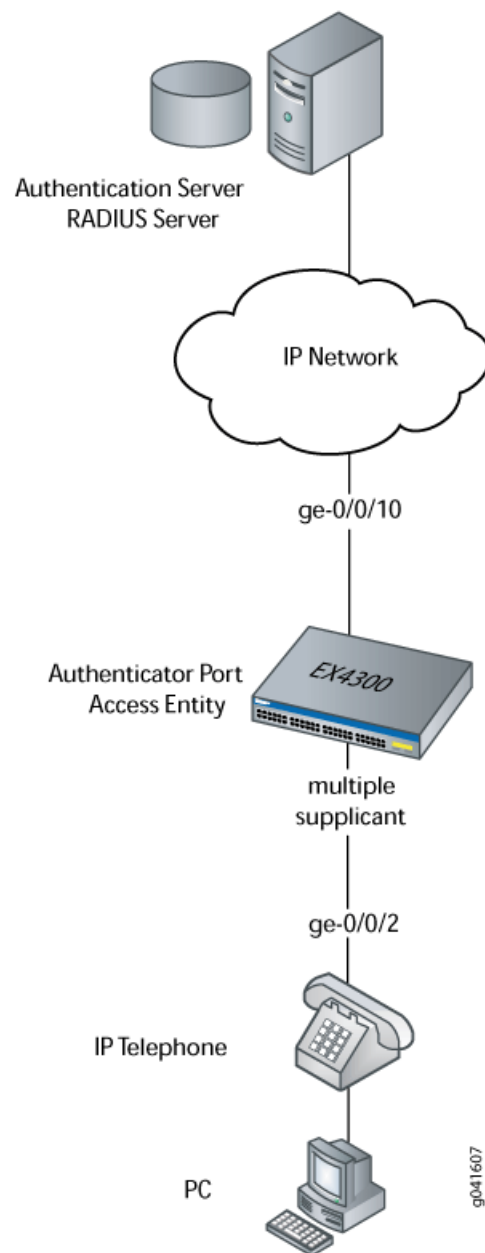
---

## Overview and Topology

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

In this example, the access interface ge-0/0/2 on the EX Series switch is connected to an Avaya IP telephone. Avaya phones have a built-in bridge that enables you to connect a desktop PC to the phone, so the desktop and phone in a single office require only one interface on the switch. The EX Series switch is connected to a RADIUS server on the ge-0/0/10 interface (see [Figure 19 on page 148](#)).

Figure 19: 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 16 on page 148](#) describes the components used in this VoIP configuration example.

Table 16: Components of the VoIP Configuration Topology

| Property        | Settings                               |
|-----------------|----------------------------------------|
| Switch hardware | EX Series switch with support for ELS. |

Table 16: Components of the VoIP Configuration Topology (*continued*)

| Property                                                                                                            | Settings                                                                       |
|---------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| VLAN names and IDs                                                                                                  | data-vlan, 77<br>voice-vlan, 99                                                |
| Connection to Avaya phone—with integrated hub, to connect phone and desktop PC to a single interface (requires PoE) | ge-0/0/2                                                                       |
| One RADIUS server                                                                                                   | Provides backend database connected to the switch through interface ge-0/0/10. |

Besides configuring a VoIP for interface ge-0/0/2, you configure:

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



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

## Configuration

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

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

**Step-by-Step Procedure** To configure VoIP with LLDP-MED and 802.1X:

1. Configure the VLANs for voice and data:
 

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

```
[edit vlans]
user@switch# set data-vlan switch-options interface ge-0/0/2.0
```

3. Configure the interface as an access interface, configure support for Ethernet switching, and add the interface as a member of the **data-vlan** VLAN:
 

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

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

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



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

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

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

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

```
}
vpls {
 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 151](#)
- [Verifying 802.1X Authentication for IP Phone and Desktop PC on page 152](#)
- [Verifying the VLAN Association with the Interface on page 153](#)

### Verifying LLDP-MED Configuration

---

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

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

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

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

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

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

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

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

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

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

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

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



**Action** user@switch> `show dot1x interface ge-0/0/2.0 detail`

```

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

```

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

### Verifying the VLAN Association with the Interface

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

**Action** user@switch> `show ethernet-switching interface ge-0/0/2.0`

```

Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
 LH - MAC limit hit, DN - interface down)

```

| Logical 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 an EX Series Switch on page 35](#)
- [Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 44](#)
- *Defining CoS Forwarding Classes (CLI Procedure)*

- [Defining CoS Forwarding Classes \(J-Web Procedure\)](#)
- [Configuring LLDP-MED \(CLI Procedure\) on page 141](#)

## Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication

---



**NOTE:** This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Example: 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 an EX Series switch to support IP telephones.

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

This example describes how to configure VoIP on an EX Series switch without 802.1X authentication by using static MAC bypass of authentication:

- [Requirements on page 154](#)
- [Overview on page 155](#)
- [Configuration on page 155](#)
- [Verification on page 157](#)

## Requirements

This example uses the following hardware and software components:

- One EX Series switch with support for ELS
- 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 EX Series switch. See the installation information for your switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

- Configured the RADIUS server for 802.1X authentication and set up the access profile. See [“Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 35](#).
- (Optional) Configured the interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant uses a power adapter. For information about configuring PoE, see *Configuring PoE on EX Series Switches (CLI Procedure)*.



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

## Overview

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

In this example, the access interface ge-0/0/2 on the EX Series switch is connected to 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 interface as a member of the **data-vlan** VLAN:  

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

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

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/2
```
6. Set the authentication profile with the name **auth-profile** (see [“Configuring 802.1X Interface Settings \(CLI Procedure\)”](#) on page 32 and [“Configuring 802.1X RADIUS Accounting \(CLI Procedure\)”](#) on page 83):  

```
[edit protocols]
user@switch# set dot1x authenticator authentication-profile-name auth-profile
```
7. Add the MAC address of the phone to the static MAC bypass list:  

```
[edit protocols]
user@switch# set dot1x authenticator static 00:04:f2:11:aa:a7
```
8. Set the supplicant mode to multiple:  

```
[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 {
 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 157](#)
- [Verifying Authentication for the Desktop PC on page 158](#)
- [Verifying the VLAN Association with the Interface on page 159](#)

### 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` command 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 role. The **Supplicant Mode** field shows that the interface is configured in **multiple** supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

### Verifying the VLAN Association with the Interface

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

**Action** user@switch> `show ethernet-switching interface ge-0/0/2.0`

```

Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
 LH - MAC limit hit, DN - interface down)

```

| Logical 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 **Vlan members** field 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 an EX Series Switch on page 145](#)
- [Understanding 802.1X and VoIP on EX Series Switches on page 143](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 135](#)





## CHAPTER 9

# Configuration Statements

- [\[edit access\] Configuration Statement Hierarchy on EX Series Switches on page 163](#)
- [\[edit protocols dot1x\] Configuration Statement Hierarchy on EX Series Switches on page 169](#)
- [accounting on page 172](#)
- [accounting \(Access Profile\) on page 173](#)
- [accounting-order on page 174](#)
- [accounting-port on page 175](#)
- [address-assignment \(Address-Assignment Pools\) on page 176](#)
- [address-protection on page 178](#)
- [authorization-order on page 179](#)
- [authentication-order \(Access Profile\) on page 180](#)
- [authentication-order \(Authenticator\) on page 181](#)
- [authentication-protocol on page 183](#)
- [authentication-whitelist on page 184](#)
- [authenticator on page 185](#)
- [client-accounting-algorithm on page 186](#)
- [client-authentication-algorithm on page 187](#)
- [coa-dynamic-variable-validation on page 188](#)
- [destination \(Accounting\) on page 189](#)
- [destination-host \(Gx-Plus\) on page 190](#)
- [destination-realm \(Gx-Plus\) on page 190](#)
- [diameter-instance \(Gx-Plus\) on page 191](#)
- [domain \(Domain Map\) on page 192](#)
- [domain-name-server \(Routing Instances and Access Profiles\) on page 193](#)
- [domain-name-server-inet \(Routing Instances and Access Profiles\) on page 194](#)
- [domain-name-server-inet6 \(Routing Instances and Access Profiles\) on page 195](#)
- [ethernet-port-type-virtual on page 195](#)
- [global \(Gx-Plus\) on page 196](#)

- [gx-plus \(Gx-Plus\) on page 196](#)
- [ignore on page 197](#)
- [include-ipv6 \(Gx-Plus\) on page 198](#)
- [interface \(Static MAC Bypass\) on page 199](#)
- [interface \(VoIP\) on page 200](#)
- [interface-description-format on page 201](#)
- [juniper-dsl-attributes on page 202](#)
- [lldp on page 203](#)
- [lldp-med \(Ethernet Switching\) on page 205](#)
- [mau-type on page 206](#)
- [max-outstanding-requests \(Gx-Plus\) on page 207](#)
- [nas-identifier on page 207](#)
- [nas-port-extended-format on page 208](#)
- [nas-port-id-delimiter \(Subscriber Management\) on page 209](#)
- [nas-port-id-format \(Subscriber Management\) on page 210](#)
- [nas-port-type \(Subscriber Management\) on page 212](#)
- [options on page 214](#)
- [partition \(Gx-Plus\) on page 215](#)
- [port on page 216](#)
- [provisioning-order on page 217](#)
- [radius \(Access Profile\) on page 218](#)
- [radius \(System\) on page 220](#)
- [radius-options \(Protocols 802.1X\) on page 221](#)
- [radius-options \(Access\) on page 222](#)
- [radius-server \(System\) on page 223](#)
- [redirect-url on page 224](#)
- [retry on page 225](#)
- [revert-interval on page 226](#)
- [routing-instance on page 226](#)
- [secret on page 227](#)
- [send-acct-status-on-config-change \(Access Profile\) on page 227](#)
- [server \(RADIUS Accounting\) on page 228](#)
- [server-fail-voip on page 229](#)
- [service \(Service Accounting\) on page 230](#)
- [source-address on page 231](#)
- [timeout \(RADIUS\) on page 232](#)
- [vlan \(VoIP\) on page 233](#)

- [vlan-assignment on page 234](#)
- [vlan-nas-port-stacked-format on page 235](#)
- [voip on page 235](#)
- [wait-for-acct-on-ack \(Access Profile\) on page 236](#)

## [\[edit access\] Configuration Statement Hierarchy on EX Series Switches](#)

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

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

This topic lists:

- [Supported Statements in the \[edit access\] Hierarchy Level on page 163](#)
- [Unsupported Statements in the \[edit access\] Hierarchy Level on page 168](#)

## Supported Statements in the [edit access] Hierarchy Level

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

```
access {
 address-assignment {
 abated-utilization;
 abated-utilization-v6;
 high-utilization;
 high-utilization-v6;
 neighbor-discovery-router-advertisement;
 pool name {
 family {
 inet {
 dhcp-attributes {
 boot-file filename;
 boot-server server-address;
 domain-name domain-name;
 grace-period seconds;
 maximum-lease-time (length | infinite);
 name-server ip-address;
 netbios-node-type (b-node | h-node | m-node | p-node);
 option option-identifier-code;
 option-match {
 option-82 {
 circuit-id match-value;
 remote-id match-value;
 }
 }
 }
 }
 }
 }
 }
}
```

```

 }
 }
 router ip-address;
 server-identifier;
 tftp-server;
 wins-server ip-address;
}
host;
network;
range;
xauth-attributes;
}
inet6 {
 dhcp-attributes;
 prefix;
 range;
}
}
link name {
 family {
 inet;
 inet6;
 }
}
}
}
address-pool pool-name {
 address address-or-prefix;
 address-range <low lower-limit> <high upper-limit>;
}
address-protection;
domain {
 delimiter characters;
 map name {
 aaa-logical-system name {
 aaa-routing-instance;
 }
 aaa-routing-instance aaa-routing-instance;
 }
 access-profile;
 address-pool;
 dynamic-profile;
 padn destination-ip-address;
 strip-domain;
 target-logical-system;
 target-routing-instance;
}
parse-direction (left-to-right | right-to-left);
}
domain-name-server address;
domain-name-server-inet address;
domain-name-server-inet6 address;
group-profile;
gx-plus {
 global {
 include-ipv6;
 max-outstanding-requests;
 }
}

```

```

 }
 partition {
 destination-host;
 destination-realm;
 diameter-instance;
 }
}
ldap-options {
 assemble {
 common-name name;
 }
 base-distinguished-name name;
 revert-interval seconds;
 search {
 admin-search {
 distinguished-name name;
 password password;
 }
 search-filter filter;
 }
}
ldap-server address {
 port number;
 retry number;
 routing-instance routing-instance;
 source-address address;
 timeout seconds;
}
ppp-options;
profile profile-name {
 accounting (Access Profile) {
 accounting-stop-on-access-deny;
 accounting-stop-on-failure;
 coa-immediate-update;
 immediate-update;
 order (radius | none);
 statistics (time | volume-time);
 wait-for-acct-on-ack;
 }
 accounting-order (radius | [accounting-order-data-list]);
 address-assignment {
 pool;
 }
 authentication-order (Access Profile) [(ldap | none | password | radius | secureid)];
 authorization-order (src | [authorization-order-data-list]);
 client client-name {
 chap-secret chap-secret;
 firewall-user {
 password password;
 }
 ike;
 no-rfc2486;
 pap-password password;
 }
 client-name-filter {
 count number;
 }
}

```

```
 domain-name name;
 separator character;
}
domain-name-server;
domain-name-server-inet;
domain-name-server-inet6;
ldap-options {
 assemble {
 common-name name;
 }
 base-distinguished-name name;
 revert-interval seconds;
 search {
 admin-search {
 distinguished-name name;
 password password;
 }
 search-filter filter;
 }
}
ldap-server address {
 port number;
 retry number;
 routing-instance routing-instance;
 source-address address;
 timeout seconds;
}
provisioning-order {
 gx-plus;
 jsr;
}
radius {
 accounting-server [server-addresses];
 attributes {
 exclude [exclude-options];
 ignore [ignore-options];
 }
 authentication-server [server-addresses];
 options {
 accounting-session-id-format (decimal | description);
 client-accounting-algorithm (direct | round-robin);
 client-authentication-algorithm (direct | round-robin);
 coa-dynamic-variable-validation;
 ethernet-port-type-virtual;
 interface-description-format {
 exclude-adapter;
 exclude-sub-interface;
 }
 juniper-dsl-attributes;
 nas-identifier nas-identifier;
 nas-port-extended-format {
 adapter-width adapter-width;
 ae-width ae-width;
 port-width port-width;
 slot-width slot-width;
 stacked-vlan-width stacked-vlan-width;
```

```

 vlan-width vlan-width;
 }
 nas-port-id-delimiter nas-port-id-delimiter;
 nas-port-id-format {
 agent-circuit-id;
 agent-remote-id;
 interface-description;
 nas-identifier;
 }
 nas-port-type {
 ethernet;
 }
 revert-interval seconds;
 vlans-nas-port-stacked-format;
}
}
radius-server address {
 max-outstanding-requests max-outstanding-requests;
 port port-number;
 retry retry;
 routing-instance instance-name;
 secret secret;
 source-address address;
 timeout seconds;
}
service {
 accounting-order {
 activation-protocol;
 radius;
 }
}
session-options {
 client-idle-timeout minutes;
 client-session-timeout minutes;
}
}
radius-options {
 interim-rate number;
 interim-update-tolerance interim-update-tolerance;
 request-rate number;
 revert-interval interval;
}
radius-server server-address {
 accounting-port port-number;
 max-outstanding-requests number;
 port port-number;
 retry attempts;
 routing-instance instance-name;
 secret password;
 source-address address;
 timeout seconds;
}
securid-server server-name{
 configuration-file file-path;
}
terminate-code {

```

```

 }
}

```

## Unsupported Statements in the [edit access] Hierarchy Level

Statements in the **[edit access]** hierarchy level that are displayed in the switch CLI are supported on the switch and operate as documented with the exceptions listed in [Table 17 on page 168](#):

**Table 17: Unsupported [edit access] Configuration Statements on EX Series Switches**

| Statement                                                                                                      | Hierarchy Level                                |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| <b>NOTE:</b> Variables, such as <i>filename</i> , are not shown in the statements or hierarchies listed below. |                                                |
| aaa                                                                                                            | [edit access terminate-code]                   |
| administrative-reset                                                                                           | [edit access terminate-code aaa shutdown]      |
| authentication-denied                                                                                          | [edit access terminate-code aaa deny]          |
| client-request                                                                                                 | [edit access terminate-code aaa dhcp]          |
| compliance                                                                                                     | [edit access ppp-options]                      |
| deny                                                                                                           | [edit access terminate-code aaa]               |
| dhcp                                                                                                           | [edit access terminate-code]                   |
| group-profile                                                                                                  | [edit access]                                  |
| ike                                                                                                            | [edit access profile client]                   |
| initiate-dead-peer-detection                                                                                   | [edit access profile client ike]               |
| lost-carrier                                                                                                   | [edit access terminate-code dhcp]              |
| nak                                                                                                            | [edit access terminate-code dhcp]              |
| nas-logout                                                                                                     | [edit access terminate-code dhcp]              |
| no-offers                                                                                                      | [edit access terminate-code dhcp]              |
| no-resources                                                                                                   | [edit access terminate-code aaa deny]          |
| ppp-options                                                                                                    | [edit access]                                  |
| preference                                                                                                     | [edit access profile client ike reverse-route] |
| remote-reset                                                                                                   | [edit access terminate-code aaa shutdown]      |
| rfc                                                                                                            | [edit access ppp-options compliance]           |



Table 17: Unsupported [edit access] Configuration Statements on EX Series Switches (*continued*)

| Statement              | Hierarchy Level                       |
|------------------------|---------------------------------------|
| reverse-route          | [edit access profile client ike]      |
| server-request-timeout | [edit access terminate-code aaa deny] |
| shutdown               | [edit access terminate-code aaa]      |
| terminate-code         | [edit access]                         |

- Related Documentation**
- [Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 35](#)
  - [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 83](#)
  - [Security Features for EX Series Switches Overview](#)

## [edit protocols dot1x] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit protocols dot1x] hierarchy level on EX Series switches.

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

This topic lists:

- [Supported Statements in the \[edit protocols dot1x\] Hierarchy Level on page 169](#)
- [Unsupported Statements in the \[edit protocols dot1x\] Hierarchy Level on page 170](#)

## Supported Statements in the [edit protocols dot1x] Hierarchy Level

The following hierarchy shows the [edit protocols dot1x] configuration statements supported on EX Series switches:

```

protocols {
 dot1x {
 authenticator {
 authentication-profile-name access-profile-name;
 interface (all | [interface-names]) {
 disable;
 guest-vlan (vlan-id | vlan-name);
 mac-radius {
 flap-on-disconnect;
 }
 }
 }
 }
}

```

```

 restrict;
}
maximum-requests number;
no-reauthentication;
quiet-period seconds;
reauthentication {
 interval seconds;
}
retries number;
server-fail (deny | permit | use-cache | vlan-id | vlan-name);
server-reject-vlan (vlan-id | vlan-name) {
 eapol-block;
 block-interval block-interval;
}
server-timeout seconds;
supplicant (single | single-secure | multiple);
supplicant-timeout seconds;
transmit-period seconds;
}
no-mac-table-binding {
 interface interface-names
 static mac-address
}
static mac-address {
 interface interface-names;
 vlan-assignment (vlan-id | vlan-name);
}
}
}
}
traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable> <match
 regex>;
 flag flag;
}

```

## Unsupported Statements in the [edit protocols dot1x] Hierarchy Level

All statements in the **[edit protocols dot1x]** hierarchy level that are displayed in the switch CLI are supported on the switch and operate as documented.

## Related Documentation

- [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 73](#)
- [Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 44](#)
- [Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 67](#)
- [Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 85](#)
- [Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 130](#)

- [802.1X for EX Series Switches Overview on page 30](#)
- *[edit protocols] Configuration Statement Hierarchy on EX Series Switches*

## accounting

```
Syntax accounting {
 events [login change-log interactive-commands];
 destination {
 radius {
 server {
 server-address {
 accounting-port port-number;
 secret password;
 source-address address;
 retry number;
 timeout seconds;
 }
 }
 }
 tacplus {
 server {
 server-address {
 port port-number;
 secret password;
 single-connection;
 timeout seconds;
 }
 }
 }
 }
 enhanced-avs-max <number>;
 }
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
**enhanced-avs-max** statement introduced in Junos OS Release 14.1.  
Support for the **source-address-inet6** statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

**Description** Configure audit of TACACS+ or RADIUS authentication events, configuration changes, and interactive commands. Auditing these factors helps you track network usage for auditing and billing purposes.

The remaining statements are explained separately.

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

**Related Documentation**

- *Configuring RADIUS System Accounting*
- *Configuring TACACS+ System Accounting*
- *enhanced-avs-max*

## accounting (Access Profile)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> accounting {   accounting-stop-on-access-deny;   accounting-stop-on-failure;   address-change-immediate-update;   coa-immediate-update;   coa-no-override service-class-attribute;   duplication;   duplication-filter;   duplication-vrf {     access-profile-name <i>profile-name</i>;     vrf-name <i>vrf-name</i>;   }   immediate-update;   order [<i>accounting-method</i>];   send-acct-status-on-config-change   statistics (time   volume-time);   update-interval <i>minutes</i>;   wait-for-acct-on-ack; } </pre> |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | <p>Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile.</p> <p>The remaining statements are explained separately.</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 Authentication and Accounting Parameters for Subscriber Access</i></li> <li>• <i>Configuring Per-Subscriber Session Accounting</i></li> <li>• <i>Understanding RADIUS Accounting Duplicate Reporting</i></li> </ul>                                                                                                                                                                                                                                                        |

## accounting-order

---

|                                 |                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | accounting-order (radius   [ <i>accounting-order-data-list</i> ]);                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> ]                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.0.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                                                |
| <b>Description</b>              | Enable RADIUS accounting for an L2TP profile.                                                                                                                                                                                                                                                |
| <b>Options</b>                  | <b>radius</b> —Use the RADIUS accounting method.<br><br><b>[<i>accounting-order-data-list</i>]</b> —Set of data listing the accounting order to be used, enclosed in brackets. This can be any combination of accounting methods, up to and including a list of the entire accounting order. |
| <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 Access Profiles for L2TP or PPP Parameters</i></li></ul>                                                                                                                                                                              |

## accounting-port

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>accounting-port <i>port-number</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>     | [edit access radius-server <i>server-address</i> ],<br>[edit access profile <i>profile-name</i> radius-server <i>server-address</i> ]                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches with support for Enhanced Layer 2 software (ELS).<br>Statement introduced on Junos OS without ELS in the following releases: <ul style="list-style-type: none"> <li>Junos OS Release 12.3 for EX Series switches: Release 12.3R10.</li> <li>Junos OS Release 14.1X53 for EX Series switches: Release 14.1X53-D25.</li> <li>Junos OS Release 15.1 for EX Series switches: Release 15.1R4.</li> </ul> |

**Description** Configure the port number on which to contact the RADIUS accounting server.



**NOTE:** Specifying the accounting port is optional, and port 1813 is the default. However, we recommend that you configure it in order to avoid confusion, as some RADIUS servers might refer to an older default.

|                                 |                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Options</b>                  | <b><i>port-number</i></b> —Port number on which to contact the RADIUS accounting server. Most RADIUS servers use port 1813, as specified in RFC 2866.<br><b>Default:</b> 1813                                                                                                                                                    |
| <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 RADIUS System Accounting</i></li> <li><i>Configuring Router or Switch Interaction with RADIUS Servers</i></li> <li><i>Configuring Authentication and Accounting Parameters for Subscriber Access</i></li> <li><i>Configuring RADIUS Authentication for L2TP</i></li> </ul> |

## address-assignment (Address-Assignment Pools)

```
Syntax address-assignment {
 abated-utilization percentage;
 abated-utilization-v6 percentage;
 high-utilization percentage;
 high-utilization-v6 percentage;
 neighbor-discovery-router-advertisement ndra-pool-name;
 pool pool-name {
 family family {
 dhcp-attributes {
 protocol-specific attributes;
 }
 host hostname {
 hardware-address mac-address;
 ip-address ip-address;
 }
 network ip-prefix / <prefix-length>;
 prefix ipv6-prefix;
 range range-name {
 high upper-limit;
 low lower-limit;
 prefix-length prefix-length;
 }
 }
 link pool-name;
 }
 }
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced in Junos OS Release 9.0.  
Statement introduced in Junos OS Release 12.1 for EX Series switches.

**Description** Configure address-assignment pools that can be used by different client applications.



**NOTE:** Support for subordinate statements is platform-specific. See individual statement topics for support information.

**Options** *pool-name*—Name assigned to an address-assignment pool.

The remaining statements are explained separately.

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

**Related Documentation**

- *Address-Assignment Pools Overview*
- *Configuring Address-Assignment Pools*



- *Configuring an Address-Assignment Pool for L2TP LNS with Inline Services*

## address-protection

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | address-protection;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit access],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> access]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | <p>Prevent IPv4 addresses and IPv6 prefixes from being assigned to more than one subscriber session when you use AAA to supply IPv4 addresses.</p> <p>For IPv4:</p> <p>If enabled, the router checks the following attributes received from external servers:</p> <ul style="list-style-type: none"><li>• <i>Framed-IP-Address</i></li><li>• <i>Framed-Pool</i></li></ul> <p>The router then takes one of the following actions:</p> <ul style="list-style-type: none"><li>• If an address matches an address in an address pool, the address is taken from the pool, provided it is available.</li><li>• If the address is already in use, it is rejected as unavailable.</li></ul> <p>For IPv6:</p> <p>If enabled, the router checks the following attributes received from external servers:</p> <ul style="list-style-type: none"><li>• <i>Framed-IPv6-Prefix</i></li><li>• <i>Framed-IPv6-Pool</i></li></ul> <p>The router then takes one of the following actions:</p> <ul style="list-style-type: none"><li>• If a prefix matches a prefix in an address pool, the prefix is taken from the pool, provided it is available.</li><li>• If the prefix is already in use, it is rejected as unavailable.</li><li>• If the prefix length requested from the external server does not exactly match the pool's prefix length, the authentication request is denied. If configured, the Acct-Stop message includes the cause for termination.</li></ul> |
| <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>• <i>Configuring Duplicate IPv6 Prefix Protection for Router Advertisement</i></li><li>• <i>Configuring Duplicate IPv4 Address Protection for AAA</i></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## authorization-order

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | authorization-order (jsrc   [ <i>authorization-order-data-list</i> ]);                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> ]                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.6.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                                                                                                                                                               |
| <b>Description</b>              | Configure AAA to use JSRC in an SRC environment to request authorization from the SAE when verifying that a DHCP subscriber can access the router or switch. When you include this statement, AAA ignores any configured authentication order settings. This statement is ignored for non-DHCP subscribers.                                                                                                 |
| <b>Options</b>                  | <p>jsrc—Use JSRC application to communicate with the SAE for subscriber authorization. JSRC is the only application that is currently available.</p> <p>[<i>authorization-order-data-list</i>]<i>—Set of data listing the authorization order to be used, enclosed in brackets. This can be any combination of authorization methods, up to and including a list of the entire authorization order.</i></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 JSRC</i></li> <li>• <i>Authorizing Subscribers with JSRC</i></li> </ul>                                                                                                                                                                                                                                                                             |

## authentication-order (Access Profile)

---

|                                 |                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | authentication-order [(none   ldap   password   radius   secureid)];                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> ]                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                    |
| <b>Description</b>              | (EX and QFX Series only) Configure the order of authentication, authorization, and accounting (AAA) methods to use while sending authentication messages.                                                                                                                                    |
| <b>Default</b>                  | Not enabled                                                                                                                                                                                                                                                                                  |
| <b>Options</b>                  | <b>none</b> —No authentication for specified subscribers.<br><br><b>ldap</b> —Lightweight Directory Access Protocol.<br><br><b>password</b> —Locally configured password in access profile.<br><br><b>radius</b> —RADIUS authentication.<br><br><b>secureid</b> —RSA SecurID authentication. |
| <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>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 35</a></li><li>• <a href="#">Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 83</a></li></ul>                                                 |

## authentication-order (Authenticator)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>authentication-order [dot1x   mac-radius   captive-portal];</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>     | <code>[edit protocols dot1x <b>authenticator</b> interface <i>interface-name</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b> | Statement introduced in Junos OS Release 15.1R3 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>         | <p>Configure the preferred order of authentication methods that the switch will use when attempting to authenticate a client. If multiple authentication methods are configured on a single interface, when one authentication method fails, the switch falls back to another method. You can configure the <b>authentication-order</b> statement to specify whether 802.1X authentication or MAC RADIUS authentication must be the first authentication method tried.</p> <p>By default, the switch attempts to authenticate a client by using 802.1X authentication first. If 802.1X authentication fails because there is no response from the client, and MAC RADIUS authentication is configured on the interface, the switch falls back to MAC RADIUS authentication. If MAC RADIUS fails, and captive portal is configured on the switch, the switch falls back to captive portal.</p> <p>Configuring MAC RADIUS authentication as the first method can help prevent the fallback timeout period which occurs after an 802.1X authentication attempt is made for a host that does not support 802.1X authentication. If MAC RADIUS authentication is configured as the first authentication method on an interface, then on receiving data from any client on that interface, the switch attempts to authenticate the client by using MAC RADIUS authentication. If MAC RADIUS authentication fails, then the switch falls back to 802.1X authentication. If 802.1X authentication fails, and captive portal is configured on the interface, the switch falls back to captive portal.</p> <p>802.1X authentication always has the highest priority, even if a client has been authenticated using another method. If the switch receives an EAP packet from a client that has been authenticated using MAC RADIUS authentication, the switch acknowledges the EAP packet and upgrades the authentication using 802.1X authentication credentials. Similarly, if a client has been authenticated through fallback to captive portal, and the switch receives an EAP packet from that client, the switch attempts to authenticate the client by using 802.1X authentication.</p> <p>The switch attempts authentication using only methods that are configured on the interface. If an authentication method is included in the authentication order, but is not configured on the interface, the switch ignores that method and attempts authentication using the next method in the order that is enabled. However, if a method is enabled on the interface, but is not included in the authentication order, the switch does not attempt using that method. For example, if captive portal is enabled for an interface, but the authentication order is configured as <b>[mac-radius dot1x]</b>, the authentication method for that interface does not fall back to captive portal.</p> <p>The authentication order can be configured for all interfaces by using the <b>interface all</b> option. If the authentication order is configured for an individual interface, and there is also an authentication order configured for all interfaces, then the order for the individual</p> |

interface is followed. If there is no authentication order configured for an individual interface, and there is an authentication order configured for all interfaces, then the configuration for all interfaces is followed.

Use the following guidelines when configuring the **authentication-order** statement:

- The authentication order must include at least two methods of authentication.
- 802.1X authentication must be one of the methods included in the authentication order.
- If captive portal is included in the authentication order, it must be the last method in the order.
- If **mac-radius-restrict** is configured on an interface, then the authentication order cannot be configured.

The valid combinations for **authentication-order** are as follows:

- **[dot1x mac-radius captive-portal]**
- **[dot1x captive-portal]**
- **[dot1x mac-radius]**
- **[mac-radius dot1x captive-portal]**

**Default** If **authentication-order** is not configured, the switch attempts to authenticate the client by using 802.1X authentication first, followed by MAC RADIUS authentication, and then captive portal, as follows:

1. 802.1X authentication—If 802.1X is configured on the interface, the switch sends EAPoL requests to the end device and attempts to authenticate the end device through 802.1X authentication. If the end device does not respond to the EAP requests, the switch checks whether MAC RADIUS authentication is configured on the interface.
2. MAC RADIUS authentication—If MAC RADIUS authentication is configured on the interface, the switch sends the MAC RADIUS address of the end device to the authentication server. If MAC RADIUS authentication is not configured, the switch checks whether captive portal is configured on the interface.
3. Captive portal authentication—If captive portal is configured on the interface, the switch attempts to authenticate the end device by using this method after attempting any other configured authentication methods.

**Options** **captive-portal**—Configure captive portal authentication in the order of authentication methods on the interface.

**dot1x**—Configure 802.1X authentication in the order of authentication methods on the interface.

**mac-radius**—Configure MAC RADIUS authentication in the order of authentication methods on the interface.

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

**Related Documentation**

- [Understanding Authentication on EX Series Switches on page 19](#)
- [Configuring Flexible Authentication Order on page 39](#)

## authentication-protocol

**Syntax** authentication-protocol (eap-md5 | pap);

**Hierarchy Level** [edit protocols dot1x **authenticator** interface *interface-name* mac-radius]

**Release Information** Statement introduced in Junos OS Release 15.1R3 for EX Series switches.

**Description** Specify that either the EAP-MD5 or Password Authentication Protocol (PAP) be used for authenticating clients by using the MAC RADIUS authentication method.

**Default** If **authentication-protocol** is not configured, the EAP-MD5 authentication protocol is used for MAC RADIUS authentication.

**Options**

**eap-md5**—Use the EAP-MD5 protocol for MAC RADIUS authentication. EAP-MD5 is an authentication method belonging to the Extensible Authentication Protocol (EAP) authentication framework. EAP-MD5 uses MD5 to hash the username and password. EAP-MD5 provides for a one-way client authentication. The server sends the client a random request for which the client must provide a response containing an encryption of the request and its password for establishing its identity.

**pap**—Use the PAP authentication protocol for MAC RADIUS authentication. PAP provides a simple password-based authentication for users to establish their identity by using a two-way handshake. PAP transmits plaintext passwords over the network without encryption. PAP must be configured if the Lightweight Directory Access Protocol (LDAP), which supports only plaintext passwords for client authentication, is used for RADIUS authentication.

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

**Related Documentation**

- [Understanding Authentication on EX Series Switches on page 19](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 83](#)

## authentication-whitelist

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>authentication-whitelist {<br/>    mac-address {<br/>        interface <i>interface-name</i>;<br/>        vlan-assignment ( <i>vlan-id</i>   <i>vlan-name</i> );<br/>    }<br/>}</pre>                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | <pre>[edit ethernet-switching-options];<br/>[edit switch-options]</pre>                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 10.1 for EX Series switches.</p> <p>The <b>[edit switch-options]</b> hierarchy level was introduced in Junos OS Release 13.2X50-D10 for EX Series switches (ELS).</p>                                                                                                                                                                                                           |
| <b>Description</b>              | <p>Configure MAC addresses for which RADIUS authentication is to be bypassed.</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>Example: Setting Up Captive Portal Authentication on an EX Series Switch</i></li><li>• <a href="#">Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 117</a></li><li>• <i>Configuring Captive Portal Authentication (CLI Procedure)</i></li><li>• <a href="#">Configuring Captive Portal Authentication (CLI Procedure) on page 113</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.

**Description** Configure an authenticator for 802.1X authentication.

The remaining statements are explained separately.



**NOTE:** You cannot configure 802.1X user authentication on interfaces on which Q-in-Q tunneling is enabled.

**Default** 802.1X authentication is disabled.

**Required Privilege** routing—To view this statement in the configuration.

**Level** routing-control—To add this statement to the configuration.

- Related Documentation**
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 32](#)
  - [Specifying RADIUS Server Connections on an EX Series Switch \(CLI Procedure\) on page 34](#)
  - [Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 130](#)


---

## client-accounting-algorithm

---

|                                 |                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | client-accounting-algorithm (direct   round-robin);                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> radius <a href="#">options</a> ]                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.0.<br>Statement introduced in Junos OS for EX Series switches Release 13.2X50-D10.                                                                                 |
| <b>Description</b>              | Configure the access method the router uses to access RADIUS accounting servers.                                                                                                                               |
| <b>Default</b>                  | direct                                                                                                                                                                                                         |
| <b>Options</b>                  | <b>direct</b> —Use the direct method.<br><br><b>round-robin</b> —Use the round-robin method.                                                                                                                   |
| <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="#">Configuring RADIUS Server Parameters for Subscriber Access</a></li><li>• <a href="#">Configuring RADIUS Server Options for Subscriber Access</a></li></ul> |

## client-authentication-algorithm

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | client-authentication-algorithm (direct   round-robin);                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> radius <b>options</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.0.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | <p>Configure the method that the authenticator uses to access RADIUS authentication servers when there are multiple servers configured. Initially, a RADIUS client sends a request to a RADIUS authentication or accounting server. The router or switch, acting as the authenticator, waits for a response from the server before sending another request.</p> <p>When there are multiple RADIUS server connections configured for a client, the authenticator attempts to reach the different servers in the order that they are configured. If there is no response from the first RADIUS server, the authenticator attempts to reach the next RADIUS server. This process repeats until the client is either granted access or there are no more configured servers.</p> <p>If the <b>direct</b> method is configured, the authenticator always treats the first server in the list as the primary server. The authenticator moves on to the second server only if the attempt to reach the first server fails. If the <b>round-robin</b> method is configured, the server chosen first will be rotated based on which server was used last. The first server in the list is treated as a primary for the first authentication request, but for the second request, the second server configured is treated as primary, and so on. With this method, all of the configured servers receive roughly the same number of requests on average so that no single server has to handle all of the requests.</p> |
|                                 | <p> <b>NOTE:</b> The round-robin access method is not recommended for use with EX Series switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Default</b>                  | The <b>direct</b> option is the default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <p><b>direct</b>—Use the direct access method. The authenticator contacts the first RADIUS server on the list for each request, the second server if the first one fails, and so on.</p> <p><b>round-robin</b>—Use the round-robin method. The authenticator contacts the first RADIUS server for the first request, the second server for the second request, and so on.</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>Configuring RADIUS Server Parameters for Subscriber Access</li> <li>Configuring RADIUS Server Options for Subscriber Access</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## coa-dynamic-variable-validation

---

|                                 |                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | coa-dynamic-variable-validation;                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> radius <a href="#">options</a> ]                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                                            |
| <b>Description</b>              | Specify that when a CoA operation includes a change to a client profile dynamic variable that cannot be applied (such as an update to a non-existent filter), the router does not apply any changes to client profile dynamic variables in the request, and responds with a NACK message. |
| <b>Default</b>                  | If you do not configure this statement, the router does not apply any incorrect variable updates, but does make any other changes to the client profile dynamic variables, and responds with an ACK message.                                                                              |
| <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 RADIUS Server Options for Subscriber Access</i></li><li>• <i>RADIUS Server Options for Subscriber Access</i></li><li>• <i>Configuring RADIUS Server Parameters for Subscriber Access</i></li></ul>                                 |

## destination (Accounting)

```
Syntax destination {
 radius {
 server {
 server-address {
 accounting-port port-number;
 retry number;
 secret password;
 source-address address;
 source-address-inet6 IPv6-source-address;
 timeout seconds;
 }
 }
 }
 tacplus {
 server {
 server-address {
 port port-number;
 secret password;
 single-connection;
 timeout seconds;
 }
 }
 }
}
```

**Hierarchy Level** [edit system [accounting](#)]

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

**Description** Configure the authentication server.

**Options** **source-address-inet6 *IPv6-source-address***—A valid IPv6 address configured on one of the routers or switch interfaces.

The remaining statements are explained separately.

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

**Related Documentation**

- *Configuring RADIUS System Accounting*
- *Configuring TACACS+ System Accounting*

## destination-host (Gx-Plus)

---

|                                 |                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>destination-host <i>hostname</i>;</code>                                                                                  |
| <b>Hierarchy Level</b>          | [edit access gx-plus <a href="#">partition</a> <i>partition-name</i> ]                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.  |
| <b>Description</b>              | Configure the host on which the PCRF application resides.                                                                       |
| <b>Options</b>                  | <i>hostname</i> —Host on which the PCRF is installed.                                                                           |
| <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 Gx-Plus</i></li><li>• <i>Configuring the Gx-Plus Partition</i></li></ul> |

## destination-realm (Gx-Plus)

---

|                                 |                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>destination-realm <i>realm</i>;</code>                                                                                    |
| <b>Hierarchy Level</b>          | [edit access gx-plus <a href="#">partition</a> <i>partition-name</i> ]                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.  |
| <b>Description</b>              | Configure the realm in which the PCRF host resides.                                                                             |
| <b>Options</b>                  | <i>realm</i> —Realm in which the PCRF host resides.                                                                             |
| <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 Gx-Plus</i></li><li>• <i>Configuring the Gx-Plus Partition</i></li></ul> |

## diameter-instance (Gx-Plus)

---

|                                 |                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>diameter-instance <i>instance-name</i>;</code>                                                                            |
| <b>Hierarchy Level</b>          | [edit access gx-plus <a href="#">partition</a> <i>partition-name</i> ]                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.  |
| <b>Description</b>              | Specify the Diameter instance associated with the Gx-Plus partition.                                                            |
| <b>Options</b>                  | <i>instance-name</i> —Name of the Diameter instance. Currently, only <b>master</b> is supported.                                |
| <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 Gx-Plus</i></li><li>• <i>Configuring the Gx-Plus Partition</i></li></ul> |

## domain (Domain Map)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>domain {   delimiter [<i>delimiter-character</i>];   map <i>domain-map-name</i> {     aaa-logical-system <i>logical-system-name</i> {       aaa-routing-instance <i>routing-instance-name</i>;     }     aaa-routing-instance <i>routing-instance-name</i>;     access-profile <i>profile-name</i>;     address-pool <i>pool-name</i>;     dynamic-profile <i>profile-name</i>;     padn <i>destination-address</i> {       mask <i>destination-mask</i>;       metric <i>route-metric</i>;     }     strip-domain;     target-logical-system <i>logical-system-name</i> {       target-routing-instance <i>routing-instance-name</i>;     }     target-routing-instance <i>routing-instance-name</i>;     tunnel-profile <i>profile-name</i>;   }   parse-direction (left-to-right   right-to-left);   parse-order (domain-first   realm-first);   realm-delimiter [<i>delimiter-character</i>];   realm-parse-direction (left-to-right   right-to-left); }</pre> |
| <b>Hierarchy Level</b>          | [edit access]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | <p>Configure a domain map, which is used to map access options and session parameters for subscriber sessions.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <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>Configuring a Domain Map</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



## domain-name-server (Routing Instances and Access Profiles)

|                            |                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>domain-name-server <i>dns-address</i>;</code>                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>     | <code>[edit access];</code><br><code>[edit access profile]</code>                                                                                                                                                                                                                                                                              |
| <b>Release Information</b> | Statement introduced in Junos OS Release 12.3.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                                                                                                 |
| <b>Description</b>         | Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the <b>[edit access]</b> hierarchy level or for an access profile at the <b>[edit access profile <i>profile-name</i>]</b> hierarchy level. You can configure more than one address by including the statement multiple times. |




**NOTE:** A DNS name server address configured with this statement is lower in preference than one configured with the [domain-name-server-inet](#) statement.

|                                 |                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Options</b>                  | <i>dns-address</i> —IPv4 address of the DNS name server.                                                                                                                  |
| <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 DNS Name Server Addresses for Subscriber Management</i></li> <li><i>DNS Name Server Address Overview</i></li> </ul> |

## domain-name-server-inet (Routing Instances and Access Profiles)

---

|                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                | domain-name-server-inet <i>dns-address</i> ;                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                       | [edit access],<br>[edit access profile]                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>                                                                                                                                                                                                                                   | Statement introduced in Junos OS Release 12.3.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                                                                                                 |
| <b>Description</b>                                                                                                                                                                                                                                           | Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the <b>[edit access]</b> hierarchy level or for an access profile at the <b>[edit access profile <i>profile-name</i>]</b> hierarchy level. You can configure more than one address by including the statement multiple times. |
| <div> <b>NOTE:</b> A DNS name server address configured with this statement is higher in preference than one configured with the <b>domain-name-server</b> statement.</div> |                                                                                                                                                                                                                                                                                                                                                |
| <b>Options</b>                                                                                                                                                                                                                                               | <i>dns-address</i> —IPv4 address of the DNS name server.                                                                                                                                                                                                                                                                                       |
| <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 DNS Name Server Addresses for Subscriber Management</i></li><li>• <i>DNS Name Server Address Overview</i></li></ul>                                                                                                                                                                     |

## domain-name-server-inet6 (Routing Instances and Access Profiles)

|                                 |                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>domain-name-server-inet6 <i>dns-address</i>;</code>                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | <code>[edit access],</code><br><code>[edit access profile]</code>                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                                                                                                 |
| <b>Description</b>              | Configure an IPv6 address for a DNS name server. You can configure an address globally for a routing instance at the <b>[edit access]</b> hierarchy level or for an access profile at the <b>[edit access profile <i>profile-name</i>]</b> hierarchy level. You can configure more than one address by including the statement multiple times. |
| <b>Options</b>                  | <i>dns-address</i> —IPv6 address of the DNS name server.                                                                                                                                                                                                                                                                                       |
| <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 DNS Name Server Addresses for Subscriber Management</i></li> <li>• <i>DNS Name Server Address Overview</i></li> </ul>                                                                                                                                                                  |

## ethernet-port-type-virtual

|                            |                                                                                                                                                                                                                                                          |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>ethernet-port-type-virtual;</code>                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>     | <code>[edit access profile <i>profile-name</i> radius options]</code>                                                                                                                                                                                    |
| <b>Release Information</b> | Statement introduced in Junos OS Release 9.1.<br>Statement introduced in Junos OS Release 9.1 for EX Series switches.                                                                                                                                    |
| <b>Description</b>         | Specify the physical port type the router or switch uses to authenticate clients. The router or switch passes a port type of <b>ethernet</b> in RADIUS attribute 61 (NAS-Port-Type) by default. This statement specifies a port type of <b>virtual</b> . |



**NOTE:** This statement takes precedence over the **nas-port-type** statement if you include both statements in the same access profile.

|                                 |                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <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 RADIUS Server Options for Subscriber Access</i></li> <li>• <i>Configuring RADIUS Server Parameters for Subscriber Access</i></li> </ul> |

## global (Gx-Plus)

---

|                                 |                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>global {<br/>    include-ipv6;<br/>    max-outstanding-requests <i>number</i>;<br/>}</pre>                                |
| <b>Hierarchy Level</b>          | [edit access <a href="#">gx-plus</a> ]                                                                                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. |
| <b>Description</b>              | Configure global attributes for the Gx-Plus application.<br><br>The remaining statements are explained separately.             |
| <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 Gx-Plus</i></li></ul>                                                   |

## gx-plus (Gx-Plus)

---

|                                 |                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>gx-plus {<br/>    global {<br/>        include-ipv6;<br/>        max-outstanding-requests <i>number</i>;<br/>    }<br/>    partition <i>partition-name</i> {<br/>        diameter-instance <i>instance-name</i>;<br/>        destination-host <i>hostname</i>;<br/>        destination-realm <i>realm</i>;<br/>    }<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit access]                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                                                                                        |
| <b>Description</b>              | Configure the Gx-Plus application to interact with a PCRF to authorize and provision subscribers.<br><br>The remaining statements are explained separately.                                                                                                                                                                           |
| <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 Gx-Plus</i></li></ul>                                                                                                                                                                                                                                                          |

## ignore

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>ignore {     dynamic-iflset-name;     framed-ip-netmask;     input-filter;     logical-system-routing-instance;     output-filter; }</pre>                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> radius attributes]                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p>                                                                                                                                                                                                                                                             |
| <b>Description</b>              | Configure the router or switch to ignore the specified attributes in RADIUS Access-Accept messages. By default, the router or switch processes the attributes it receives from the external server.                                                                                                                                                                                          |
| <b>Options</b>                  | <p><b>dynamic-iflset-name</b>—Ignore Interface-Set/Dynamic-Ifset-Name (VSA 26-130).</p> <p><b>framed-ip-netmask</b>—Ignore Framed-IP-Netmask (RADIUS attribute 9).</p> <p><b>input-filter</b>—Ignore Ingress-Policy-Name (VSA 26-10).</p> <p><b>logical-system-routing-instance</b>—Ignore Virtual-Router (VSA 26-1).</p> <p><b>output-filter</b>—Ignore Egress-Policy-Name (VSA 26-11).</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 How RADIUS Attributes Are Used for Subscriber Access</i></li> <li>• <i>Configuring RADIUS Server Parameters for Subscriber Access</i></li> </ul>                                                                                                                                                                                     |

## include-ipv6 (Gx-Plus)

---

|                                 |                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | include-ipv6;                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit access gx-plus <a href="#">global</a> ]                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.      |
| <b>Description</b>              | Include IPv6 subscribers in Gx-Plus provisioning requests.                                                                          |
| <b>Default</b>                  | By default, IPv6 subscribers are not included.                                                                                      |
| <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 Gx-Plus Global Attributes</i></li><li>• <i>Configuring Gx-Plus</i></li></ul> |

## interface (Static MAC Bypass)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>interface [<i>interface-names</i>];</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit protocols dot1x <a href="#">authenticator</a> authentication-profile-name static <i>mac-address</i> ],<br>[edit ethernet-switching-options <a href="#">authentication-whitelist</a> <i>mac-address</i> ],<br>[edit switch-options <a href="#">authentication-whitelist</a> <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).                                                                                                                                                                     |
| <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 258</a></li> <li>• <a href="#">Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 130</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> |

## interface (VoIP)

---

|                                 |                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>interface (all   [<i>interface-name</i>]   access-ports) {<br/>    <b>vlan</b> <i>vlan-name</i> ;<br/>    forwarding-class &lt;assured-forwarding   best-effort   expedited-forwarding  <br/>        network-control&gt;;<br/>}</pre>                                                                                                 |
| <b>Hierarchy Level</b>          | <ul style="list-style-type: none"><li>For platforms with ELS:<br/>[edit switch-options <b>voip</b>]</li><li>For platforms without ELS:<br/>[edit ethernet-switching-options <b>voip</b>],</li></ul>                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Hierarchy level [edit switch-options] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)                                                                                           |
| <b>Description</b>              | Enable voice over IP (VoIP) on interfaces.                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>                  | <p><b>all</b>—Enable VoIP on all interfaces.</p> <p><b><i>interface-name</i></b>—Enable VoIP on a specific interface.</p> <p><b>all</b>—(Switches without ELS only) Enable VoIP on all access ports.</p> <p>The remaining statements are explained separately.</p>                                                                         |
| <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> |



## interface-description-format

---

|                                 |                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>interface-description-format {     exclude-adapter;     exclude-sub-interface; }</pre>                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> radius <a href="#">options</a> ]                                                                                                                                                                                            |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p> <p>Options <b>exclude-adapter</b> and <b>exclude-sub-interface</b> introduced in Junos OS Release 10.4.</p>                         |
| <b>Description</b>              | Specify the information that is excluded from the interface description that the device passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). By default, the device includes both the subinterface and the adapter in the interface description. |
| <b>Options</b>                  | <p><b>exclude-adapter</b>—Exclude the adapter from the interface description.</p> <p><b>exclude-sub-interface</b>—Exclude the subinterface from the interface description.</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 RADIUS Server Options for Subscriber Access</i></li> <li>• <i>RADIUS Server Options for Subscriber Access</i></li> </ul>                                                                                     |

## juniper-dsl-attributes

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | juniper-dsl-attributes;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> radius <a href="#">options</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | <p>Configure AAA to add Juniper Networks DSL VSAs to the RADIUS authentication and accounting request messages for subscribers. If the router has not received and processed the corresponding ANCP attributes from the access node, then AAA provides only the following in these RADIUS messages:</p> <ul style="list-style-type: none"><li>• Downstream-Calculated-QoS-Rate (IANA 4874, 26-141)—Default configured advisory transmit speed.</li><li>• Upstream-Calculated-QoS-Rate (IANA 4874, 26-142)—Default configured advisory receive speed.</li></ul> |
| <b>Default</b>                  | The Juniper Networks DSL VSAs are not added to the RADIUS authentication and accounting request messages. However, the DSL Forum VSA—if available—is added to RADIUS messages by default.                                                                                                                                                                                                                                                                                                                                                                      |
| <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 AAA to Include Juniper Networks DSL VSAs in RADIUS Messages</i></li><li>• <i>Configuring the ANCP Agent</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;
 mau-type
 netbios-snooping;
 no-tagging;
 ptopo-configuration-maximum-hold-time seconds;
 ptopo-configuration-trap-interval seconds;
 traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable>
 <no-stamp> <replace>;
 flag flag <disable>;
 }
 transmit-delay seconds;
}
```

**Hierarchy Level** [edit protocols]

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

**Description** Configure Link Layer Discovery Protocol (LLDP). The switch uses LLDP to advertise its identity and capabilities on a LAN, as well as to receive information about other network devices. LLDP is defined in the IEEE standard 802.1AB-2005.

The remaining statements are explained separately.



**NOTE:** The `transmit-delay` and `netbios-snooping` options are not available on QFabric systems.



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

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

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

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

---

**Default** LLDP is enabled.

The following statements have default values:

- **advertisement-interval**—The default value is 30 seconds. The allowable range is from 5 through 32768 seconds.
- **hold-multiplier**—The default values is 4. The allowable range is from 2 through 10.
- **ptopo-configuration-maximum-hold-time**—The default value is 300 seconds. The allowable range is from 1 through 2147483647 seconds.
- **transmit-delay**—The default values is 2 seconds. The allowable range is from 1 through 8192 seconds.

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

**Related Documentation**

- [show lldp on page 260](#)
- [Configuring LLDP \(CLI Procedure\) on page 138](#)
- [Configuring LLDP](#)
- [Understanding LLDP](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 135](#)

## 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>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                              |
| <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 260</a></li> <li>• <i>Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch</i></li> <li>• <a href="#">Configuring LLDP-MED (CLI Procedure) on page 141</a></li> </ul>                                                                                                                                                                  |

## mau-type

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>mau-type;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit protocols <a href="#">lldp</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | <p>Configure the switch to advertise information about the medium attachment unit (MAU) type. The MAU is a transceiver that interconnects the attachment unit interface (AUI) port on an attached host computer to an Ethernet cable. MAU types are defined in the IEEE 802.3 standard.</p> <p>The MAU type is included in the MAC/PHY Configuration Status type, length, and value (TLV) message. TLVs are used by LLDP-capable devices to transmit information to neighbor devices. The MAC/PHY Configuration Status TLV is an organizationally defined TLV that advertises information about the physical interface. In addition to the MAU type, the MAC/PHY Configuration Status TLV also includes information such as autonegotiation status, support and advertised capabilities.</p> <p>The MAU type cannot be changed by configuration; however, you must configure the <b>mau-type</b> statement to include the MAU type value in the MAC/PHY Configuration Status TLV.</p> |
| <b>Default</b>                  | If the <b>mau-type</b> statement is not configured, the MAU type field of the MAC/PHY Configuration Status TLV contains the value <b>Unknown</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <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="#">Understanding LLDP and LLDP-MED on EX Series Switches on page 135</a></li><li>• <a href="#">Configuring LLDP</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## max-outstanding-requests (Gx-Plus)

|                                 |                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | max-outstanding-requests <i>number</i> ;                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit access gx-plus <a href="#">global</a> ]                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                   |
| <b>Description</b>              | Limit the number of outstanding requests to the PCRF that Gx-Plus can retry when the requests are improperly answered. Too many requests risks overloading the PCRF and increases the chance of losing messages. |
| <b>Options</b>                  | <i>number</i> —Number of outstanding requests from Gx-Plus to the PCRF that can exist at any time.<br><b>Default:</b> 40<br><b>Range:</b> 2 through 40                                                           |
| <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 Gx-Plus Global Attributes</i></li> <li>• <i>Configuring Gx-Plus</i></li> </ul>                                                                           |

## nas-identifier

|                                 |                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | nas-identifier <i>identifier-value</i> ;                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> radius <a href="#">options</a> ]                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.1.<br>Statement introduced in Junos OS Release 9.1 for EX Series switches.                                                                           |
| <b>Description</b>              | Configure the value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests.                                                     |
| <b>Options</b>                  | <i>identifier-value</i> —String to use for authentication and accounting requests.<br><b>Range:</b> 1 through 64 characters                                                                     |
| <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 RADIUS Server Options for Subscriber Access</i></li> <li>• <i>Configuring RADIUS Server Parameters for Subscriber Access</i></li> </ul> |

## nas-port-extended-format

**Syntax**

```
nas-port-extended-format {
 adapter-width width;
 ae-width width;
 port-width width;
 pw-width width;
 slot-width width;
 stacked-vlan-width width;
 vlan-width width;
 atm {
 adapter-width width;
 port-width width;
 slot-width width;
 vci-width width;
 vpi-width width;
 }
}
```

**Hierarchy Level** [edit access profile *profile-name* radius [options](#)]

**Release Information** Statement introduced in Junos OS Release 9.1.  
Statement introduced in Junos OS Release 9.1 for EX Series switches.  
**ae-width** option added in Junos OS Release 12.1.  
**atm** option added in Junos OS Release 12.3R3 and supported in later 12.3Rx releases.  
**atm** option supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)  
**pw-width** option added in Junos OS Release 15.1.

**Description** Configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute.

**Options**

- adapter-width *width***—Number of bits in the adapter field.
- ae-width *width***—Number of bits in the aggregated Ethernet identifier field.
- port-width *width***—Number of bits in the port field.
- pw-width *width***—Number of bits in the pseudowire field. Appears in the Cisco NAS-Port-Info AVP (100).
- slot-width *width***—Number of bits in the slot field.
- stacked-vlan-width *width***—Number of bits in the SVLAN ID field.
- vlan-width *width***—Number of bits in the VLAN ID field.



**NOTE:** The total of the widths must not exceed 32 bits, or the configuration will fail.



|                                 |                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <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 RADIUS Server Options for Subscriber Access</i></li> <li>• <i>Configuring RADIUS Server Parameters for Subscriber Access</i></li> </ul> |

## nas-port-id-delimiter (Subscriber Management)

|                                 |                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | nas-port-id-delimiter <i>delimiter-character</i> ;                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> radius <a href="#">options</a> ]                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.4.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                      |
| <b>Description</b>              | Specify the character that the router uses as a separator between the concatenated values in the NAS-Port-ID string. The router uses the delimiter when you configure more than one value in the <b>nas-port-id-format</b> statement.                               |
| <b>Default</b>                  | The hash (#) character.                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <b><i>delimiter-character</i></b> —Character used for the delimiter.                                                                                                                                                                                                |
| <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 RADIUS Server Options for Subscriber Access</i></li> <li>• <i>Configuring RADIUS Server Parameters for Subscriber Access</i></li> <li>• <i>Configuring a NAS-Port-ID with Additional Options</i></li> </ul> |

## nas-port-id-format (Subscriber Management)

**Syntax**

```
nas-port-id-format {
 agent-circuit-id;
 agent-remote-id;
 interface-description;
 interface-text-description;
 nas-identifier;
 order {
 agent-circuit-id;
 agent-remote-id;
 interface-description;
 interface-text-description;
 nas-identifier;
 postpend-vlan-tags;
 }
 postpend-vlan-tags;
}
```

**Hierarchy Level** [edit access profile *profile-name* radius [options](#)]

**Release Information** Statement introduced in Junos OS Release 11.4.  
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.  
Options **interface-text-description**, **order**, and **postpend-vlan-tags** introduced in Junos OS Release 15.1.

**Description** Specify the optional information that the router includes in the NAS-Port-ID (RADIUS attribute 87) that is passed to the RADIUS server during authentication and accounting. You can include any combination of the optional values.

When you specify the values for the NAS-Port-ID, you can configure the values to appear in either the default order or a custom order of your choice.



**NOTE:** The default and custom order methods are mutually exclusive. The configuration fails if you attempt to configure a NAS-Port-ID that includes values in both types of orders.

To specify that the optional values appear in the default order in the NAS-Port-ID, configure the values directly under the **nas-port-id-format** statement. The default order is as follows, in which the **#** character is the delimiter:

**nas-identifier # interface-description # interface-text-description # agent-circuit-id # agent-remote-id # postpend-vlan-tags**

To specify a custom order for the NAS-Port-ID string, you use the **order** option. Include the **order** option before each optional value you want to include in the string, in the order in which you want the options to appear. For example, the configuration, **order interface-text-description order nas-identifier order agent-remote-id** produces the following NAS-Port-ID, in which the **#** character is the delimiter:

**interface-text-description # nas-identifier # agent-remote-id**

**Default** The router includes the interface description in the NAS-Port-ID when no optional values are specified.

**Options** **agent-circuit-id**—Include the agent circuit ID from either DHCP option 82 or the DSL forum VSAs.

**agent-remote-id**—Include the agent remote ID from either DHCP option 82 or the DSL forum VSAs.

**interface-description**—Include the interface description (interface identifier).

**interface-text-description**—Include the textual interface description (the text description that is statically configured in the CLI).

**nas-identifier**—Include the NAS identifier value (RADIUS attribute 32).

**order**—Specify the optional values you want to include in the NAS-Port-ID and the customized order in which you want the values to appear. You must include the **order** option before each optional value (for example, **order agent-circuit-id order interface-description**).

**postpend-vlan-tags**—Include the VLAN tags. The router includes the tags in the format **:<outer-tag>-<inner-tag>** for a double-tagged VLAN, or **:<outer-tag>** for a single-tagged VLAN.

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

**Related Documentation**

- *Configuring RADIUS Server Options for Subscriber Access*
- *Configuring RADIUS Server Parameters for Subscriber Access*
- *Configuring a NAS-Port-ID with Additional Options*

## nas-port-type (Subscriber Management)

---

**Syntax**    nas-port-type {  
              ethernet {  
                  port-type;  
              }  
          }

**Hierarchy Level**    [edit access profile *profile-name* radius [options](#)]

**Release Information**    Statement introduced in Junos OS Release 11.4.  
                              Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**    Specify the port type used to authenticate subscribers. The router includes the port type in RADIUS attribute 61 (NAS-Port-Type attribute).



**NOTE:** This statement is ignored if the [ethernet-port-type-virtual](#) statement is included in the same access profile.

---

**Default**    The router uses a port type of **ethernet**.

**Options**    *port-type*—One of the following port types:

- *value*—A value from 0-65535
- **adsl-cap**—Asymmetric DSL, carrierless amplitude phase (CAP) modulation
- **adsl-dmt**—Asymmetric DSL, discrete multitone (DMT)
- **async**—Asynchronous
- **cable**—Cable
- **ethernet**—Ethernet
- **fddi**—Fiber Distributed Data Interface
- **g3-fax**—G.3 Fax
- **hdlc-clear-channel**—HDLC Clear Channel
- **iapp**—Inter-Access Point Protocol (IAPP)
- **isdsl**—ISDN DSL
- **isdn-sync**—ISDN Synchronous
- **isdn-v110**—ISDN Async V.110
- **isdn-v120**—ISDN Async V.120
- **piafs**—Personal Handyphone System (PHS) Internet Access Forum Standard
- **sdsl**—Symmetric DSL

- **sync**—Synchronous
- **token-ring**—Token Ring
- **virtual**—Virtual
- **wireless**—Other wireless
- **wireless-1x-ev**—Wireless 1xEV
- **wireless-cdma2000**—Wireless code division multiple access (CDMA) 2000
- **wireless-ieee80211**—Wireless 802.11
- **wireless-umts**—Wireless universal mobile telecommunications system (UMTS)
- **x25**—X.25
- **x75**—X.75
- **xdsl**—DSL of unknown type

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

**Related Documentation**    • *Configuring RADIUS Server Options for Subscriber Access*  
                                     • *Configuring RADIUS Server Parameters for Subscriber Access*

## options

```
Syntax options {
 accounting-session-id-format (decimal | description);
 calling-station-id-delimiter delimiter-character;
 calling-station-id-format {
 agent-circuit-id;
 agent-remote-id;
 interface-description;
 nas-identifier;
 }
 chap-challenge-in-request-authenticator;
 client-accounting-algorithm (direct | round-robin);
 client-authentication-algorithm (direct | round-robin);
 coa-dynamic-variable-validation;
 ethernet-port-type-virtual;
 access-loop-id-local;
 interface-description-format {
 exclude-adapter;
 exclude-sub-interface;
 }
 ip-address-change-notify message;
 juniper-dsl-attributes;
 nas-identifier identifier-value;
 nas-port-extended-format {
 adapter-width width;
 ae-width width;
 port-width width;
 slot-width width;
 stacked-vlan-width width;
 vlan-width width;
 atm {
 adapter-width width;
 port-width width;
 pw-width width;
 slot-width width;
 vci-width width;
 vpi-width width;
 }
 }
 nas-port-id-delimiter delimiter-character;
 nas-port-id-format {
 agent-circuit-id;
 agent-remote-id;
 interface-description;
 interface-text-description;
 nas-identifier;
 order {
 agent-circuit-id;
 agent-remote-id;
 interface-description;
 interface-text-description;
 nas-identifier;
 postpend-vlan-tags;
 }
 }
}
```

```

 }
 postpend-vlan-tags;
 }
 nas-port-type {
 ethernet {
 port-type;
 }
 }
 revert-interval interval;
 vlan-nas-port-stacked-format;
}

```

|                          |                                                                                                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hierarchy Level          | [edit access profile <i>profile-name</i> <i>radius</i> ]                                                                                                                         |
| Release Information      | Statement introduced in Junos OS Release 9.1.<br>Statement introduced in Junos OS Release 9.1 for EX Series switches.                                                            |
| Description              | Configure the options used by RADIUS authentication and accounting servers.<br><br>The remaining statements are explained separately.                                            |
| Required Privilege Level | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                  |
| Related Documentation    | <ul style="list-style-type: none"> <li>• <i>Configuring RADIUS Server Options for Subscriber Access</i></li> <li>• <i>RADIUS Server Options for Subscriber Access</i></li> </ul> |

## partition (Gx-Plus)

```

Syntax partition partition-name {
 diameter-instance instance-name;
 destination-host hostname;
 destination-realm realm;
 }

```

|                          |                                                                                                                                    |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Hierarchy Level          | [edit access <i>gx-plus</i> ]                                                                                                      |
| Release Information      | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.     |
| Description              | Configure a Gx-Plus partition.                                                                                                     |
| Options                  | <p><b><i>partition-name</i></b>—Name of the Gx-Plus partition.</p> <p>The remaining statements are explained separately.</p>       |
| Required Privilege Level | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                    |
| Related Documentation    | <ul style="list-style-type: none"> <li>• <i>Configuring Gx-Plus</i></li> <li>• <i>Configuring the Gx-Plus Partition</i></li> </ul> |

## port

---

|                                 |                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>port <i>port-number</i>;</code>                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit access radius-server <i>server-address</i> ],<br>[edit access profile <i>profile-name</i> radius-server <i>server-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.                                                                                         |
| <b>Description</b>              | Configure the port number on which to contact the RADIUS server.                                                                                                                                                  |
| <b>Options</b>                  | <b><i>port-number</i></b> —Port number on which to contact the RADIUS server.<br><b>Default:</b> 1812 (as specified in RFC 2865)                                                                                  |
| <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>Configuring Router or Switch Interaction with RADIUS Servers</i></li><li>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i></li></ul> |



## provisioning-order

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>provisioning-order (gx-plus   jsrc);</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | <code>[edit access profile <i>profile-name</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.6.<br>Support for Gx-Plus introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Configure AAA to use the specified application for subscriber service provisioning.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <p><code>gx-plus</code>—Specify Gx-Plus as the application used to communicate with a PCRF for subscriber service provisioning.</p> <p><code>jsrc</code>—Specify JSRC as the application used to communicate with the SAE for subscriber service provisioning. JSRC is used in an SRC environment to request services from the SAE for an authenticated subscriber. JSRC attempts to activate these services. If successful, JSRC returns an ACK message. If unsuccessful, the subscriber is denied access.</p> |
| <b>Required Privilege Level</b> | <p><code>admin</code>—To view this statement in the configuration.</p> <p><code>admin-control</code>—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Configuring JSRC</i></li> <li>• <i>Provisioning Subscribers with JSRC</i></li> <li>• <i>Configuring Gx-Plus</i></li> <li>• <i>Provisioning Subscribers with Gx-Plus</i></li> </ul>                                                                                                                                                                                                                                                                                  |

## radius (Access Profile)

```
Syntax radius {
 accounting-server [ip-address];
 attributes {
 exclude
 ...
 }
 ignore {
 framed-ip-netmask;
 input-filter;
 logical-system-routing-instance;
 output-filter;
 }
 }
 authentication-server [ip-address];
 options {
 accounting-session-id-format (decimal | description);
 calling-station-id-delimiter delimiter-character;
 calling-station-id-format {
 agent-circuit-id;
 agent-remote-id;
 interface-description;
 nas-identifier;
 }
 chap-challenge-in-request-authenticator;
 client-accounting-algorithm (direct | round-robin);
 client-authentication-algorithm (direct | round-robin);
 coa-dynamic-variable-validation;
 ethernet-port-type-virtual;
 interface-description-format {
 exclude-adapter;
 exclude-sub-interface;
 }
 ip-address-change-notify message;
 juniper-dsl-attributes;
 nas-identifier identifier-value;
 nas-port-extended-format {
 adapter-width width;
 ae-width width;
 port-width width;
 slot-width width;
 stacked-vlan-width width;
 vlan-width width;
 atm {
 adapter-width width;
 port-width width;
 slot-width width;
 vci-width width;
 vpi-width width;
 }
 }
 nas-port-id-delimiter delimiter-character;
 nas-port-id-format {
```

```

agent-circuit-id;
agent-remote-id;
interface-description;
interface-text-description;
nas-identifier;
order {
 agent-circuit-id;
 agent-remote-id;
 interface-description;
 interface-text-description;
 nas-identifier;
 postpend-vlan-tags;
}
postpend-vlan-tags;
}
nas-port-type {
 ethernet {
 port-type;
 }
}
revert-interval interval;
vlan-nas-port-stacked-format;
}
preauthentication-server ip-address;
}

```

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

**Release Information** Statement introduced in Junos OS Release 9.1.  
Statement introduced in Junos OS Release 9.1 for EX Series switches.

**Description** Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.

The remaining statements are explained separately.

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

**Related Documentation**

- *Configuring RADIUS Server Parameters for Subscriber Access*
- *RADIUS Server Options for Subscriber Access*

## radius (System)

---

**Syntax**

```
radius {
 server {
 server-address {
 accounting-port port-number;
 secret password;
 source-address address;
 retry number;
 timeout seconds;
 }
 }
}
```

**Hierarchy Level** [edit system accounting destination]

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

**Description** Configure the RADIUS accounting server.

**Options** *server-address*—Address of the RADIUS accounting server.  
  
The remaining statements are explained separately.

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

**Related Documentation**

- *Configuring RADIUS System Accounting*

## 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 dot1x <a href="#">authenticator</a> ]                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1 for EX Series switches.                                                                                                                                                                                                                                                    |
| <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 32</a></li> <li>• <a href="#">Specifying RADIUS Server Connections on an EX Series Switch (CLI Procedure) on page 34</a></li> <li>• <a href="#">authenticator on page 185</a></li> </ul>              |

## radius-options (Access)

---

|                                 |                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>radius-options {<br/>    revert-interval <i>seconds</i>;<br/>}</pre>                                         |
| <b>Hierarchy Level</b>          | [edit access];<br>[edit access profile <i>profile-name</i> ]                                                      |
| <b>Release Information</b>      | Statement introduced in Release 8.5 of Junos OS.                                                                  |
| <b>Description</b>              | Configure RADIUS options.                                                                                         |
| <b>Options</b>                  | The remaining statement is explained separately.                                                                  |
| <b>Required Privilege Level</b> | access—To view this statement in the configuration.<br>access-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Junos OS Security Configuration Guide</i></li></ul>                    |

---

## radius-server (System)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>radius-server {<br/>  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/>  }<br/>}</pre>                                                              |
| <b>Hierarchy Level</b>          | [edit system]                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                               |
| <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>                                                                                                                                                                                                             |
| <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 RADIUS Server Authentication</i></li></ul>                                                                                                                                                                                                                                               |

## redirect-url

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>redirect-url url;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>     | [edit protocols dot1x <b>authenticator</b> interface <i>interface-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b> | Statement introduced in Junos OS Release 15.1R3 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>         | <p>Configure a URL that redirects unauthenticated hosts to a central Web authentication (CWA) server. The CWA server provides a web portal where the user can enter a username and password. If these credentials are validated by the CWA server, the user is authenticated and is allowed access to the network.</p> <p>The redirect URL for central Web authentication can be configured centrally on the AAA server or locally on the switch. Use the <b>redirect-url</b> statement to configure the redirect URL locally on the interface connecting the host to the switch.</p> <p>The redirect URL and a dynamic firewall filter must both be present for the central Web authentication process to be triggered. For more information about configuring the redirect URL and the dynamic firewall filter for central Web authentication, see <a href="#">“Configuring Central Web Authentication” on page 125</a>.</p> |
| <b>Default</b>             | Disabled. The redirect URL is not enabled for central Web authentication by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>             | <p><b>url</b>—The URL that redirects the host to the server that will handle central web authentication. The redirect URL must use the HTTP or HTTPS protocol and include an IP address or website name. The following are examples of valid redirect URL formats:</p> <ul style="list-style-type: none"><li>• <code>http://www.example.com</code></li><li>• <code>https://www.example.com</code></li><li>• <code>http://10.10.10.10</code></li><li>• <code>https://10.10.10.10</code></li><li>• <code>http://www.example.com/login.html</code></li><li>• <code>https://www.example.com/login.html</code></li><li>• <code>http://10.10.10.10/login.html</code></li><li>• <code>https://10.10.10.10/login.html</code></li></ul>                                                                                                                                                                                                 |



**NOTE:** When the dynamic firewall filter is configured using the special Filter-ID attribute `JNPR_RSVD_FILTER_CWA`, the CWA redirect URL must include the IP address of the AAA server, for example, `https://10.10.10.10`.

---



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

**Related Documentation** • [Configuring Central Web Authentication on page 125](#)

## retry

**Syntax** `retry attempts;`

**Hierarchy Level** [edit access radius-server *server-address*];  
[edit access profile *profile-name* radius-server *server-address*]

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

**Description** Specify the number of times that the router or switch is allowed to attempt to contact a RADIUS authentication or accounting server. You can configure separate values for the accounting server with the *accounting-retry* statement.



**BEST PRACTICE:** We recommend that you do not configure the maximum retry duration: 30 retries times 90 seconds for the timeout. Configure either fewer retries, a shorter timeout, or both.

**Options** *attempts*—Number of times that the router is allowed to attempt to contact a RADIUS server.

**Range:** 1 through 30

**Default:** 3

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

**Related Documentation** • [Configuring Authentication and Accounting Parameters for Subscriber Access](#)  
• [Configuring Router or Switch Interaction with RADIUS Servers](#)  
• [Example: Configuring CHAP Authentication with RADIUS](#)  
• [Configuring RADIUS Authentication for L2TP](#)  
• [timeout on page 232](#)

## revert-interval

---

|                                 |                                                                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>revert-interval <i>interval</i>;</code>                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> radius <b>options</b> ];<br>[edit access radius-options]                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.1.<br>Statement introduced in Junos OS Release 9.1 for EX Series switches.                                                                                                                                                                       |
| <b>Description</b>              | Configure the amount of time the router or switch waits after a server has become unreachable. The router or switch rechecks the connection to the server when the specified interval expires. If the server is then reachable, it is used in accordance with the order of the server list. |
| <b>Options</b>                  | <i>interval</i> —Amount of time to wait.<br><b>Range:</b> 0 through 604,800 seconds<br><b>Default:</b> 60 seconds                                                                                                                                                                           |
| <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 RADIUS Server Options for Subscriber Access</i></li><li>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i></li></ul>                                                                                |

## routing-instance

---

|                                 |                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>routing-instance <i>routing-instance-name</i>;</code>                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit access radius-server <i>server-address</i> ],<br>[edit access profile <i>profile-name</i> radius-server <i>server-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.                                                                        |
| <b>Description</b>              | Configure the routing instance used to send RADIUS packets to the RADIUS server.                                                                                                                 |
| <b>Options</b>                  | <i>routing-instance-name</i> —Routing instance name.                                                                                                                                             |
| <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>Configuring the PPP Authentication Protocol</i></li><li>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i></li></ul> |

## secret

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>secret <i>password</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> radius-server <i>server-address</i> ],<br>[edit access radius-disconnect <i>client-address</i> ],<br>[edit access radius-server <i>server-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.                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Configure the password to use with the RADIUS server. The secret password used by the local router or switch must match that used by the server.                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <i>password</i> —Password to use; it can include spaces if the character string is enclosed in quotation marks.                                                                                                                                                                                                                                                                                                              |
| <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>Configuring Authentication and Accounting Parameters for Subscriber Access</i></li> <li>• <i>Configuring Router or Switch Interaction with RADIUS Servers</i></li> <li>• <i>Example: Configuring CHAP Authentication with RADIUS</i></li> <li>• <i>Configuring RADIUS Authentication for L2TP</i></li> <li>• <i>Configuring the RADIUS Disconnect Server for L2TP</i></li> </ul> |

## send-acct-status-on-config-change (Access Profile)

---


|                                 |                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>send-acct-status-on-config-change;</code>                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> <b>accounting</b> ]                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.1.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                             |
| <b>Description</b>              | Configure the router's authd process to send an Acct-On message when the first RADIUS server is added to an access profile, and to send an Acct-Off message when the last RADIUS server is removed from an access profile. |
| <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 RADIUS Server Parameters for Subscriber Access</i></li> <li>• <i>Configuring Per-Subscriber Session Accounting</i></li> </ul>                                      |

## server (RADIUS Accounting)

---

|                                 |                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>server {<br/>  server-address {<br/>    accounting-port <i>port-number</i>;<br/>    retry <i>number</i><br/>    secret <i>password</i>;<br/>    source-address <i>address</i>;<br/>    timeout <i>seconds</i>;<br/>  }<br/>}</pre>           |
| <b>Hierarchy Level</b>          | [edit system accounting destination radius]                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Support for the <b>source-address-inet6</b> statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches. |
| <b>Description</b>              | Configure RADIUS logging.<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>Configuring RADIUS System Accounting</i></li></ul>                                                                                                                                                     |

## server-fail-voip

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>server-fail (deny   permit   use-cache   vlan-name);</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>     | [edit protocols dot1x <b>authenticator</b> interface (all   [ <i>interface-names</i> ])]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b> | Statement introduced in Junos OS Releases 14.1X53-D40 and 15.1R4 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>         | <p>Configure authentication fallback options to specify how VoIP clients sending voice traffic are supported if the RADIUS authentication server becomes unavailable. Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by a supplicant's initial attempt at authentication through the RADIUS server.</p> <p>When you configure the server fail fallback feature you must specify an action that the switch applies to end devices when the authentication servers are unavailable. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN. The VLAN must already be configured on the switch.</p> <p>The <b>server-fail-voip</b> statement is specific to the VoIP-tagged traffic sent by clients. VoIP clients still require that the <b>server-fail</b> statement be configured for the un-tagged traffic that they generate. Therefore, when you configure the <b>server-fail-voip</b> statement you must also configure the <b>server-fail</b> statement.</p> |
|                            | <p> <b>NOTE:</b> An option other than <b>server-fail deny</b> must be configured for <b>server-fail-voip</b> to successfully commit.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Default</b>             | If the <b>server-fail-voip</b> statement is not configured, in the event that the RADIUS authentication server becomes unavailable, a VoIP client that begins authentication by sending voice traffic is not authenticated, and the voice traffic is dropped.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <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. This option can be used only for reauthentication.</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</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

the VLAN and is not authenticated. The VLAN must already be configured on 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 dot1x on page 251</a></li><li>• <a href="#">Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 67</a></li><li>• <a href="#">Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 35</a></li><li>• <a href="#">Configuring RADIUS Server Fail Fallback (CLI Procedure) on page 42</a></li><li>• <a href="#">Understanding Server Fail Fallback and Authentication on EX Series Switches on page 28</a></li></ul> |

---

## service (Service Accounting)

---

|                                 |                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>service {<br/>  accounting-order (activation-protocol   radius);<br/>  accounting{<br/>    update-interval <i>minutes</i>;<br/>    statistics (time   volume-time);<br/>  }<br/>}</pre>                                                                         |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> ]                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.4.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.<br><b>accounting</b> , <b>update-interval</b> , and <b>statistics</b> options added in Junos OS Release 14.2R1 for MX Series routers. |
| <b>Description</b>              | Define the subscriber service accounting configuration.<br><br>The remaining statement is explained separately.                                                                                                                                                      |
| <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="#">Configuring Service Accounting with JSRC</a></li><li>• <a href="#">Service Accounting with JSRC</a></li></ul>                                                                                                    |

---


## source-address

---

|                                 |                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>source-address <i>source-address</i>;</code>                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | <code>[edit access radius-server <i>server-address</i>];</code><br><code>[edit access profile <i>profile-name</i> radius-server <i>server-address</i>]</code>                                                                                                                                                                                       |
| <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.                                                                                                                                                                                                                           |
| <b>Description</b>              | Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address.                                                                                                                                                                                                        |
| <b>Options</b>                  | <b><i>source-address</i></b> —Valid IPv4 address configured on one of the router or switch interfaces.<br>On M Series routers only, the source address can be an IPv6 address and the UDP source port is 514.                                                                                                                                       |
| <b>Required Privilege Level</b> | <code>admin</code> —To view this statement in the configuration.<br><code>admin-control</code> —To add this statement to the configuration.                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Configuring Router or Switch Interaction with RADIUS Servers</i></li><li>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i></li><li>• <i>Example: Configuring CHAP Authentication with RADIUS</i></li><li>• <i>Configuring RADIUS Authentication for L2TP</i></li></ul> |

## timeout (RADIUS)

---

|                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                  | timeout <i>seconds</i> ;                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                         | [edit access radius-server <i>server-address</i> ],<br>[edit access profile <i>profile-name</i> radius-server <i>server-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.                                                                                                                                                                                                                           |
| <b>Description</b>                                                                                                                                                                                                                                                                             | Configure the amount of time that the local router or switch waits to receive a response from a RADIUS server. You can configure separate values for the accounting server with the <i>accounting-timeout</i> statement.                                                                                                                            |
| <div> <b>BEST PRACTICE:</b> We recommend that you do not configure the maximum retry duration: 30 retries times 90 seconds for the timeout. Configure either fewer retries, a shorter timeout, or both.</div> |                                                                                                                                                                                                                                                                                                                                                     |
| <b>Options</b>                                                                                                                                                                                                                                                                                 | <b><i>seconds</i></b> —Amount of time to wait.<br><b>Range:</b> 1 through 90 seconds<br><b>Default:</b> 3 seconds                                                                                                                                                                                                                                   |
| <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>Configuring Router or Switch Interaction with RADIUS Servers</i></li><li>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i></li><li>• <i>Example: Configuring CHAP Authentication with RADIUS</i></li><li>• <i>Configuring RADIUS Authentication for L2TP</i></li></ul> |



## vlan (VoIP)

|                                 |                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>vlan (vlan-id   vlan-name   untagged);</code>                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit ethernet-switching-options <b>voip interface (VoIP)</b> (all   [ <i>interface-name</i>   access-ports])                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | (EX Series switches only) Specify the VLAN name or VLAN tag identifier associated with the VLAN to be sent from the authenticating server to the IP phone.                                                                                                                                                                                           |
| <b>Options</b>                  | <p><i>vlan-name</i>—Name of a VLAN.</p> <p><i>vlan-id</i>—The VLAN tag identifier.</p> <p><b>Range:</b> 0 through 4095. Tags 0 and 4095 are reserved by Junos OS; do not configure them.</p> <p><i>untagged</i>—Allow untagged VLAN traffic.</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>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> |

## vlan-assignment

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>vlan-assignment (vlan-id   vlan-name);</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | <code>[edit protocols dot1x authenticator authentication-profile-name static (Protocols 802.1X) mac-address];</code><br><code>[edit ethernet-switching-options authentication-whitelist];</code><br><code>[edit switch-options authentication-whitelist]</code>                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement added to the <code>[edit ethernet-switching-options authentication-whitelist]</code> hierarchy in Junos OS Release 10.1 for EX Series switches.<br>Statement added to the <code>[edit switch-options authentication-whitelist]</code> hierarchy in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Configure the VLAN that is associated with the list of MAC addresses that are excluded from RADIUS authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <code>vlan-id   vlan-name</code> —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> | <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="#">show dot1x static-mac-address on page 258</a></li><li>• <a href="#">Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 130</a></li><li>• <a href="#">Example: Setting Up Captive Portal Authentication on an EX Series Switch</a></li><li>• <a href="#">Understanding Authentication on EX Series Switches on page 19</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> |

## vlan-nas-port-stacked-format

|                                 |                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>vlan-nas-port-stacked-format;</code>                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | <code>[edit access profile <i>profile-name</i> radius <a href="#">options</a>]</code>                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.1.<br>Statement introduced in Junos OS Release 9.1 for EX Series switches.                                                                                           |
| <b>Description</b>              | Configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.                                                                           |
| <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 RADIUS Server Options for Subscriber Access</i></li> <li>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i></li> </ul> |

## voip

|                                 |                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>voip {   <a href="#">interface</a> (all   [<i>interface-name</i>   access-ports]) {     <a href="#">vlan</a> <i>vlan-name</i> ;     forwarding-class &lt;assured-forwarding   best-effort   expedited-forwarding         network-control&gt;;   } }</pre>                                                                                       |
| <b>Hierarchy Level</b>          | <code>[edit ethernet-switching-options];</code><br><code>[edit switch-options]</code>                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Configure 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> |

## wait-for-acct-on-ack (Access Profile)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | wait-for-acct-on-ack;                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit access profile <i>profile-name</i> <b>accounting</b> ]                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | Configure the router's authd process to wait for an Acct-On-Ack response message from RADIUS before sending new authentication and accounting updates to the RADIUS server. This configuration ensures that when a new subscriber session starts, the authentication and accounting information for the new session does not get deleted when RADIUS clears previously existing session state information. |
| <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 RADIUS Server Parameters for Subscriber Access</i></li><li>• <i>Configuring Per-Subscriber Session Accounting</i></li></ul>                                                                                                                                                                                                                         |

## CHAPTER 10

# Command Summaries

- clear captive-portal
- clear dot1x
- clear lldp neighbors
- clear lldp statistics
- show captive-portal authentication-failed-users
- show captive-portal firewall
- show captive-portal interface
- show dot1x
- show dot1x authentication-failed-users
- show dot1x firewall
- show dot1x static-mac-address
- show lldp
- show lldp local-information
- show lldp neighbors
- show lldp remote-global-statistics
- show lldp statistics
- show network-access aaa statistics accounting
- show network-access aaa statistics authentication
- show network-access aaa statistics dynamic-requests

## clear captive-portal

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>clear captive-portal</b> ( <b>firewall</b> [ <i>interface-names</i> ]   <b>interface</b> (802.1X) (all   [ <i>interface-names</i> ])   <b>mac-address</b> [ <i>mac-addresses</i> ])                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.1 for EX Series switches.<br>Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Reset the authentication state of a captive portal interface or captive portal firewall statistics on one or more interfaces.                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <p><b>firewall</b> [<i>interface-names</i>]<i>—</i>Resets captive portal statistics on all interfaces or on the specified interface.</p> <p><b>interface</b> (all   <i>interface-names</i>)<i>—</i>Resets the authentication state of users connected to all interfaces or the specified interfaces.</p> <p><b>mac-address</b> <i>mac-addresses</i><i>—</i>Resets the authentication state for the specified MAC addresses.</p>                 |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show captive-portal authentication-failed-users on page 244</a></li> <li>• <a href="#">show captive-portal interface on page 248</a></li> <li>• <a href="#">show captive-portal firewall on page 246</a></li> <li>• <i>Example: Setting Up Captive Portal Authentication on an EX Series Switch</i></li> <li>• <i>Configuring Captive Portal Authentication (CLI Procedure)</i></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">clear captive-portal interface on page 239</a><br><a href="#">clear captive-portal interface on page 239</a><br><a href="#">clear captive-portal mac-address on page 239</a><br><a href="#">clear captive-portal firewall on page 239</a>                                                                                                                                                                                           |
| <b>Output Fields</b>            | <a href="#">Table 18 on page 238</a> lists the output fields for the <b>clear captive-portal interface</b> command. (The <b>clear captive-portal firewall</b> and <b>clear captive-portal mac-address</b> commands have no output). Output fields are listed in the approximate order in which they appear.                                                                                                                                     |

**Table 18: clear captive-portal interface Output Fields**

| Field Name       | Field Description                                      |
|------------------|--------------------------------------------------------|
| <b>Interface</b> | Interface on which captive portal has been configured. |

Table 18: clear captive-portal interface Output Fields (*continued*)

| Field Name         | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>State</b>       | <p>The state of the port:</p> <ul style="list-style-type: none"> <li>• <b>Authenticated</b>—The client has been authenticated through the RADIUS server or has been permitted access through server fail fallback.</li> <li>• <b>Authenticating</b>—The client is authenticating through the RADIUS server.</li> <li>• <b>Connecting</b>—Switch is attempting to contact the RADIUS server.</li> <li>• <b>Initialize</b>—The interface link is down.</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>MAC address</b> | The MAC address of the connected client on the interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>User</b>        | Users connected to the captive portal interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Sample Output

### clear captive-portal interface

```
user@switch> clear captive-portal interface
ge-0/0/3.0
```

### clear captive-portal interface

```
user@switch> clear captive-portal interface
Captive Portal Information:
Interface State MAC address User
ge-0/0/3.0 Authenticated 00:03:47:e1:ba:b9 ac1allow
ge-0/0/5.0 Connecting
ge-0/0/7.0 Connecting
ge-0/0/9.0 Connecting
```

### clear captive-portal mac-address

```
user@switch> clear captive-portal mac-address 00:03:47:e1:ba:b9
This command has no output.
```

### clear captive-portal firewall

```
user@switch> clear captive-portal firewall
This command has no output.
```

## clear dot1x

---

**Syntax** `clear dot1x (firewall <counter-name> | interface <[interface-name]> | mac-address [mac-addresses] | statistics <interface interface-name>)`

**Release Information** Command introduced in Junos OS Release 9.0 for EX Series switches.  
**firewall** option added in Junos OS Release 9.5 for EX Series switches.  
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

**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 251](#)
- [Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 44](#)
- [Filtering 802.1X Suplicants by Using RADIUS Server Attributes on page 52](#)

**List of Sample Output**

- [clear dot1x firewall on page 241](#)
- [clear dot1x interface \(Specific Interfaces\) on page 241](#)
- [clear dot1x mac-address \(Specific MAC Address\) on page 241](#)
- [clear dot1x statistics interface \(Specific Interface\) on page 241](#)

## 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>                   | <code>clear lldp neighbors</code><br><code>&lt;interface <i>interface</i>&gt;</code>                                                                                                                                                                       |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX 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 one or more selected interfaces.                                                     |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show lldp on page 260</a></li><li>• <a href="#">Configuring LLDP (CLI Procedure) on page 138</a></li><li>• <a href="#">Understanding LLDP and LLDP-MED on EX Series Switches on page 135</a></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">clear lldp neighbors on page 242</a><br><a href="#">clear lldp neighbors interface ge-0/1/1.0 on page 242</a>                                                                                                                                  |

### Sample Output

#### clear lldp neighbors

```
user@switch> clear lldp neighbors
```

#### clear lldp neighbors interface ge-0/1/1.0

```
user@switch> clear lldp neighbors interface ge-0/1/1.0
```

## clear lldp statistics

---

|                                 |                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear lldp statistics<br><interface <i>interface</i> >                                                                                                                                                        |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                            |
| <b>Description</b>              | Clear LLDP statistics on one or more interfaces.                                                                                                                                                              |
| <b>Options</b>                  | <p><b>none</b>—Clears LLDP statistics on all interfaces.</p> <p><b>interface <i>interface-names</i></b>—(Optional) Clear LLDP statistics on one or more interfaces.</p>                                       |
| <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 138</a></li> <li>• <a href="#">Understanding LLDP and LLDP-MED on EX Series Switches on page 135</a></li> </ul> |
| <b>List of Sample Output</b>    | <p><a href="#">clear lldp statistics on page 243</a></p> <p><a href="#">clear lldp statistics interface ge-0/1/1.0 on page 243</a></p>                                                                        |

### Sample Output

#### clear lldp statistics

```
user@switch> clear lldp statistics
```

#### clear lldp statistics interface ge-0/1/1.0

```
user@switch> clear lldp statistics interface ge-0/1/1.0
```

## show captive-portal authentication-failed-users

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show captive-portal authentication-failed-users</b>                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.1 for EX Series switches.<br>Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.                                                                                                                                                                                                                                         |
| <b>Description</b>              | Display the users that have failed captive portal authentication.                                                                                                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show captive-portal interface on page 248</a></li> <li>• <a href="#">show captive-portal firewall on page 246</a></li> <li>• <a href="#">clear captive-portal on page 238</a></li> <li>• <i>Example: Setting Up Captive Portal Authentication on an EX Series Switch</i></li> <li>• <i>Configuring Captive Portal Authentication (CLI Procedure)</i></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show captive-portal authentication-failed-users on page 244</a>                                                                                                                                                                                                                                                                                                                                          |
| <b>Output Fields</b>            | <a href="#">Table 19 on page 244</a> lists the output fields for the <b>show captive-portal authentication-failed-users</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                         |

**Table 19: show captive-portal authentication-failed-users Output Fields**

| Field Name           | Field Description                                                           | Level of Output |
|----------------------|-----------------------------------------------------------------------------|-----------------|
| <b>Interface</b>     | The MAC address configured to bypass captive portal authentication.         | all             |
| <b>MAC address</b>   | The MAC address configured statically on the interface.                     | all             |
| <b>User</b>          | Name of the user that has failed captive portal authentication.             | all             |
| <b>Failure Count</b> | The number of times that 802.1X authentication has failed on the interface. | all             |

### Sample Output

#### show captive-portal authentication-failed-users

```
user@host> show captive-portal authentication-failed-users
```

| Interface   | MAC address       | User         | Failure Count |
|-------------|-------------------|--------------|---------------|
| ge-0/0/17.0 | 00:37:00:00:00:00 | 003700000000 | 28            |
| ge-0/0/20.0 | 00:04:10:00:00:00 | 000410000000 | 32            |
| ge-0/0/18.0 | 00:00:03:00:0a:00 | 000003000a00 | 4             |
| ge-0/0/19.0 | 00:00:03:00:0b:00 | 000003000b00 | 18            |



## show captive-portal firewall

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show captive-portal firewall</code><br><code>&lt;brief   detail&gt;</code><br><code>&lt;interface-name&gt;</code><br><code>&lt;interface-name detail&gt;</code>                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.1 for EX Series switches.<br>Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.                                                                                                                                                                                                                                                      |
| <b>Description</b>              | Display information about the firewall filters for each user that is authenticated on each captive portal interface.                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <b>none</b> —Display all the firewall filters on all captive portal interfaces.<br><br><b>brief   detail</b> —(Optional) Display the specified level of output.<br><br><b>interface-name</b> —(Optional) Display all the terms of the firewall filters for the specified interface.<br><br><b>interface-name detail</b> —(Optional) Display all of the terms of the firewall filters for the specified interface.                 |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show captive-portal authentication-failed-users on page 244</a></li><li>• <a href="#">show captive-portal interface on page 248</a></li><li>• <a href="#">clear captive-portal on page 238</a></li><li>• <i>Example: Setting Up Captive Portal Authentication on an EX Series Switch</i></li><li>• <i>Configuring Captive Portal Authentication (CLI Procedure)</i></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">show captive-portal firewall brief on page 246</a><br><a href="#">show captive-portal firewall (Specific Interface) on page 247</a><br><a href="#">show captive-portal firewall on page 247</a>                                                                                                                                                                                                                       |
| <b>Output Fields</b>            | Output fields for the <b>show captive-portal firewall</b> command include any action modifier specified in firewall filters except policers. Policers are not supported in the terms of the internally generated dynamic firewall filters that are created when multiple supplicants authenticate on 802.1X-enabled interfaces.                                                                                                   |

## Sample Output

### show captive-portal firewall brief

```
user@switch> show captive-portal firewall brief
Captive Portal Information:
Interface State MAC address User
```

```

ge-0/0/1.0 Connecting
ge-0/0/10.0 Connecting 00:30:48:8c:66:bd No User

```

### show captive-portal firewall (Specific Interface)

```

user@switch> show captive-portal firewall ge-0/0/10.0
Filter name: dot1x_ge-0/0/10
Counters:
Name Bytes Packets
dot1x_ge-0/0/10_CP_arp 7616 119
dot1x_ge-0/0/10_CP_dhcp 0 0
dot1x_ge-0/0/10_CP_http 0 0
dot1x_ge-0/0/10_CP_https 0 0
dot1x_ge-0/0/10_CP_t_dns 0 0
dot1x_ge-0/0/10_CP_u_dns 0 0

```

### show captive-portal firewall

```

user@switch> show captive-portal firewall
Filter name: dot1x_ge-0/0/0
Counters:
Name Bytes Packets
dot1x_ge-0/0/0_CP_arp 0 0
dot1x_ge-0/0/0_CP_dhcp 0 0
dot1x_ge-0/0/0_CP_http 0 0
dot1x_ge-0/0/0_CP_https 0 0
dot1x_ge-0/0/0_CP_t_dns 0 0
dot1x_ge-0/0/0_CP_u_dns 0 0
Filter name: dot1x_ge-0/0/1
Counters:
Name Bytes Packets
dot1x_ge-0/0/1_CP_arp 0 0
dot1x_ge-0/0/1_CP_dhcp 0 0
dot1x_ge-0/0/1_CP_http 0 0
dot1x_ge-0/0/1_CP_https 0 0
dot1x_ge-0/0/1_CP_t_dns 0 0
dot1x_ge-0/0/1_CP_u_dns 0 0
Filter name: dot1x_ge-0/0/10
Counters:
Name Bytes Packets
dot1x_ge-0/0/10_CP_arp 7616 119
dot1x_ge-0/0/10_CP_dhcp 0 0
dot1x_ge-0/0/10_CP_http 0 0
dot1x_ge-0/0/10_CP_https 0 0
dot1x_ge-0/0/10_CP_t_dns 0 0
dot1x_ge-0/0/10_CP_u_dns 0 0
Filter name: dot1x_ge-0/0/11

```

## show captive-portal interface

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show captive-portal interface</b><br><b>&lt;interface-name&gt;</b><br><b>detail</b>                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.1 for EX Series switches.<br>Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Display the current operational state of all captive portal interfaces with the list of connected users and the configured values of captive portal attributes on the interfaces.                                                                                                                                                                                                                                                                                                                  |
| <b>Options</b>                  | <p><b>none</b>—Display all captive portal interfaces.</p> <p><b>interface-name</b>—(Optional) Display the state for the specified captive portal interface and lists the MAC address and user names of any clients authenticated on the interface.</p> <p><b>interface-name detail</b>—(Optional) Display the configured values of captive portal attributes on the specified captive portal interface.</p>                                                                                        |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show captive-portal authentication-failed-users on page 244</a></li> <li>• <a href="#">show captive-portal firewall on page 246</a></li> <li>• <a href="#">captive-portal</a></li> <li>• <a href="#">clear captive-portal on page 238</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> |
| <b>List of Sample Output</b>    | <p><a href="#">show captive-portal interface (Only Captive Portal Enabled) on page 250</a></p> <p><a href="#">show captive-portal interface (802.1X Authentication and Captive Portal Enabled) on page 250</a></p> <p><a href="#">show captive-portal interface detail (Only Captive Portal Enabled) on page 250</a></p> <p><a href="#">show captive-portal interface detail (802.1X Authentication and Captive Portal Enabled) on page 250</a></p>                                                |
| <b>Output Fields</b>            | <a href="#">Table 20 on page 248</a> lists the output fields for the <b>show captive-portal interface</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                         |

Table 20: show captive-portal interface Output Fields

| Field Name       | Field Description                                      | Level of Output |
|------------------|--------------------------------------------------------|-----------------|
| <b>Interface</b> | Interface on which captive portal has been configured. | All levels      |



Table 20: show captive-portal interface Output Fields (*continued*)

| Field Name                             | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Level of Output |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>State</b>                           | <p>The state of the interface:</p> <ul style="list-style-type: none"> <li>• <b>Authenticated</b>—The client has been authenticated through the RADIUS server or has been permitted access through server fail fallback.</li> <li>• <b>Authenticating</b>—The client is authenticating through the RADIUS server.</li> <li>• <b>Connecting</b>—Switch is attempting to contact the RADIUS server.</li> <li>• <b>Initialize</b>—The interface link is down.</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> | All levels      |
| <b>MAC address</b>                     | The MAC address of the connected client on the interface..                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | brief           |
| <b>User</b>                            | Users connected to the captive portal interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | brief           |
| <b>Fallen back</b>                     | <p>Indicates when 802.1X authentication and captive portal are both enabled on an interface:</p> <ul style="list-style-type: none"> <li>• If 802.1X authentication and captive portal are both enabled, <b>CP fallen back</b> status is <b>Yes</b>.</li> <li>• If 802.1X authentication and captive portal are not both enabled, <b>CP fallen back</b> status is <b>No</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                        |                 |
| <b>Supplicant mode</b>                 | Mode used to authenticate clients—multiple, single, or single-supplicant.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | detail          |
| <b>Number of retries</b>               | Number of times the user can attempt to submit authentication information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | detail          |
| <b>Quiet period</b>                    | Time, in seconds, after a user exceeds the maximum number of retries before they can attempt to authenticate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | detail          |
| <b>Configured CP session timeout</b>   | Time, in seconds, that a client can be idle before the session expires.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | detail          |
| <b>Server timeout</b>                  | Time, in seconds, that an interface will wait for a reply when relaying a response from the client to the authentication server before timing out and invoking the server-fail action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | detail          |
| <b>Number of connected supplicants</b> | <p>Number of users connecting through the captive portal interface. Information for each user includes:</p> <ul style="list-style-type: none"> <li>• <b>Supplicant</b>—User name and MAC address.</li> <li>• <b>Operational state</b>—See State (above).</li> <li>• <b>Dynamic CP session timeout</b>—Timeout value dynamically downloaded from the RADIUS server for this user, if any.</li> <li>• <b>CP Session expiration due in</b>—Time remaining in session.</li> </ul>                                                                                                                                                                                                                                                                                 | detail          |

## Sample Output

### show captive-portal interface (Only Captive Portal Enabled)

```
user@switch> show captive-portal interface
Captive Portal Information:
Interface State MAC address User Fallen back
ge-0/0/1.0 Connecting
ge-0/0/10.0 Connecting 00:30:48:8c:66:bd No User
ge-6/0/5.0 Authenticated 00:30:48:8d:7a:9b abcdeX No
```

### show captive-portal interface (802.1X Authentication and Captive Portal Enabled)

```
user@switch> show captive-portal interface
Captive Portal Information:
Interface State MAC address User Fallen back
ge-0/0/1.0 Connecting
ge-0/0/10.0 Connecting 00:30:48:8c:66:bd No User
ge-6/0/5.0 Authenticated 00:30:48:8d:7a:9b abcdeX Yes
```

### show captive-portal interface detail (Only Captive Portal Enabled)

```
user@switch> show captive-portal interface detail ge-6/0/5.0
Supplicant mode: Multiple
Number of retries: 3
Quiet period: 60 seconds
Configured CP session timeout: 3600 seconds
Server timeout: 15 seconds
CP fallen back: No
Number of connected supplicants: 1
 Supplicant: abcdeX, 00:30:48:8d:7a:9b
 Operational state: Authenticated
 Dynamic CP Session Timeout: 3600 seconds
 CP Session Expiration due in: 3583 seconds
```

### show captive-portal interface detail (802.1X Authentication and Captive Portal Enabled)

```
user@switch> show captive-portal interface detail ge-6/0/5.0
Supplicant mode: Multiple
Number of retries: 3
Quiet period: 60 seconds
Configured CP session timeout: 3600 seconds
Server timeout: 15 seconds
CP fallen back: Yes
Number of connected supplicants: 1
 Supplicant: abcdeX, 00:30:48:8d:7a:9b
 Operational state: Authenticated
 Dynamic CP Session Timeout: 3600 seconds
 CP Session Expiration due in: 3583 seconds
```

## 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 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <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> —(Optional) 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 240</a></li> <li>• <a href="#">Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 44</a></li> <li>• <a href="#">Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 67</a></li> <li>• <a href="#">Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 85</a></li> <li>• <a href="#">Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 52</a></li> <li>• <a href="#">Verifying 802.1X Authentication on page 91</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show dot1x interface brief on page 255</a><br><a href="#">show dot1x interface detail on page 255</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Output Fields</b>            | <a href="#">Table 21 on page 251</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 21: show dot1x Output Fields**

| Field Name       | Field Description | Level of Output |
|------------------|-------------------|-----------------|
| <b>Interface</b> | Name of a port.   | All levels      |

Table 21: show dot1x Output Fields (*continued*)

| Field Name                  | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Level of Output      |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <b>MAC address</b>          | The MAC address of the connected supplicant on the port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | All levels           |
| <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 username 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 (by 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>—Only the first supplicant is authenticated. All other supplicants who connect later to the port are allowed full access without any further authentication. They effectively “piggyback” on the first supplicant’s authentication.</li> <li>• <b>single-secure</b>—Only one supplicant is allowed to connect to the port. No other supplicant is allowed to connect until the first supplicant logs out.</li> <li>• <b>multiple</b>—Multiple supplicants are allowed 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 waits following a failed authentication exchange with the supplicant before reattempting the authentication. The default value is 60 seconds. The range is 0 through 65,535 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                               | <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 21: 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 the host by using the MAC address.</li> <li>• <b>disabled</b>—The default. The switch does not attempt to authenticate the MAC address of the connecting host.</li> </ul>                                        | <b>detail</b>   |
| <b>MAC radius authentication protocol</b>                   | MAC RADIUS authentication protocol: <ul style="list-style-type: none"> <li>• <b>EAP-MD5</b>—The EAP-MD5 protocol is used for MAC RADIUS authentication. EAP-MD5 is an authentication method belonging to the Extensible Authentication Protocol (EAP) authentication framework. EAP-MD5 is the default authentication protocol.</li> <li>• <b>PAP</b>—The Password Authentication Protocol (PAP) authentication protocol is used for MAC RADIUS authentication.</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 times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out. The default value is 2. The range is 1 through 10.                                                                                                                                                                                                                                                                                     | <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 username and MAC address of the connected supplicant.                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>detail</b>   |

Table 21: show dot1x Output Fields (*continued*)

| Field Name                          | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Level of Output |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Authentication method               | <p>The authentication method used for a supplicant:</p> <ul style="list-style-type: none"> <li>• <b>CWA Authentication</b>—A supplicant is authenticated by the central Web authentication (CWA) server.</li> <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</b>—One of the following fallback actions is in effect because the RADIUS server is unreachable. Indicates whether EAPOL block is in effect, and the amount of time remaining for EAPOL block (in seconds). <ul style="list-style-type: none"> <li>• <b>deny</b>—The supplicant is denied access to the LAN, preventing traffic from flowing from the supplicant through the interface. This is the default server fail fallback action.</li> <li>• <b>permit</b>—The supplicant is permitted access to the LAN as if the supplicant had been successfully authenticated by the RADIUS server.</li> <li>• <b>use-cache</b>—In the event that the RADIUS server times out when the supplicant is attempting reauthentication, the supplicant is reauthenticated only if it was previously authenticated; otherwise, the supplicant is denied LAN access.</li> <li>• <b>VLAN</b>—The supplicant is configured to be moved to a specified VLAN if the RADIUS server is unavailable to reauthenticate the supplicant. (The VLAN must already exist on the switch.)</li> </ul> </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          |
| Session Accounting Interim Interval | The number of seconds between interim RADIUS accounting messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | detail          |
| Accounting Update due in            | The number of seconds until the next interim RADIUS accounting update is due.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | detail          |
| CWA Redirect URL                    | The URL used to redirect the supplicant to a central Web server for authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | detail          |

## 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 00:a6:55:f2:94:ae user3
```

### show dot1x interface detail

```
user@switch> show dot1x interface ge-0/0/16.0 detail

ge-0/0/16.0
Role: Authenticator
Administrative state: Auto
Supplicant mode: Single
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Enabled
Mac Radius Restrict: Disabled
Mac Radius Authentication Protocol: PAP
Reauthentication: Enabled
Configured Reauthentication interval: 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.                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | Display the 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 240</a></li> <li>• <a href="#">Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 130</a></li> <li>• <a href="#">Configuring 802.1X Interface Settings (CLI Procedure) on page 32</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show dot1x authentication-failed-users on page 256</a>                                                                                                                                                                                                                                                                   |
| <b>Output Fields</b>            | <a href="#">Table 22 on page 256</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 22: 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 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.                                                                                                                                   |
| <b>Description</b>              | Display information about the firewall filters for each user or nonresponsive host that is authenticated on each 802.1X-enabled interface that is configured for multiple supplicants. For example, if the firewall filter is configured with a term for counters, the command shows the count for each user. |
| <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 240</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 257</a><br><a href="#">show dot1x firewall on page 257</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 <i>[interface-name]</i>)&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 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Display 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 <i>interface-name</i></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 240</a></li> <li>• <a href="#">Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 130</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 32</a></li> <li>• <a href="#">Understanding Authentication on EX Series Switches on page 19</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show dot1x static-mac-address on page 258</a><br><a href="#">show dot1x static-mac-address interface (Specific Interface) on page 259</a>                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Output Fields</b>            | Table 23 on page 258 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 23: 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 lldp

|                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                            | <code>show lldp</code><br><code>&lt;detail&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-D20 for OCX Series switches.<br>Command introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                |
| <b>Description</b>                                                                                                                                       | 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.                                                                                                 |
| <div>  <b>NOTE:</b> LLDP-MED is not available on the QFX Series. </div> |                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Options</b>                                                                                                                                           | <b>none</b> —Display LLDP information for all interfaces.<br><br><b>detail</b> —(Optional) Display detailed LLDP information for all interfaces.                                                                                                                                                                                                                                    |
| <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 138</a></li> <li>• <a href="#">Configuring LLDP-MED (CLI Procedure) on page 141</a></li> <li>• <a href="#">Understanding LLDP and LLDP-MED on EX Series Switches on page 135</a></li> <li>• <a href="#">Configuring LLDP</a></li> <li>• <a href="#">Understanding LLDP</a></li> </ul> |
| <b>List of Sample Output</b>                                                                                                                             | <a href="#">show lldp (EX3200 switches) on page 263</a><br><a href="#">show lldp (EX4300 switches) on page 263</a><br><a href="#">show lldp detail (EX4300 switches) on page 264</a>                                                                                                                                                                                                |
| <b>Output Fields</b>                                                                                                                                     | <a href="#">Table 24 on page 260</a> lists the output fields for the <b>show lldp</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                              |

**Table 24: 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 24: 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 <i>advertisement-interval</i> 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 <i>hold-multiplier</i> 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 <i>ptopo-configuration-trap-interval</i> 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 <i>ptopo-configuration-maximum-hold-time</i> 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 24: show lldp Output Fields (*continued*)

| Field Name                | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Level of Output |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| LLDP                      | LLDP operating state. The state can be <b>Enabled</b> or <b>Disabled</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | All levels      |
| Power Negotiation         | LLDP power negotiation operating state. The state can be <b>Enabled</b> or <b>Disabled</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | All levels      |
| Neighbor count            | Total number of new LLDP neighbors detected since the last switch reboot.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>detail</b>   |
| Interface                 | Name of the interface that is advertising VLAN information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | All levels      |
| Vlan-id                   | VLAN tag associated with the interface sending LLDP frames. If the interface is not a member of a VLAN, the VLAN ID is advertised as 0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>detail</b>   |
| Vlan-name                 | VLAN name associated with the VLAN ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>detail</b>   |
| LLDP basic TLVs supported | <p>Basic TLVs supported on the switch:</p> <ul style="list-style-type: none"> <li>• <b>Chassis identifier</b>—TLV that advertises the MAC address associated with the local system.</li> <li>• <b>Port identifier</b>—TLV that advertises the port identification for the specified port in the local system.</li> <li>• <b>Port description</b>—Interface name for the port.</li> <li>• <b>System name</b>—TLV that advertises the user-configured name of the local system.</li> <li>• <b>System description</b>—TLV that advertises the system description containing information about the software and current image running on the system. This information is taken from the software and is not configurable.</li> <li>• <b>System capabilities</b>—TLV that advertises the primary functions performed by the system—for example, bridge or router.</li> <li>• <b>Management address</b>—TLV that advertises the IP management address of the local system.</li> </ul> | <b>detail</b>   |
| Supported LLDP 802 TLVs   | <p>802.3 TLVs supported on the switch:</p> <ul style="list-style-type: none"> <li>• <b>MAC/PHY configuration status</b>—TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information is based on the physical interface structure and is not configurable.</li> <li>• <b>Power via MDI</b>—TLV that advertises MDI power support, PSE power pair, and power class information.</li> <li>• <b>Link aggregation</b>—TLV that advertises if the interface is aggregated and its aggregated interface ID.</li> <li>• <b>Maximum frame size</b>—TLV that advertises the maximum transmission unit (MTU) of the interface sending LLDP frames.</li> <li>• <b>Port VLAN tag</b>—TLV that advertises the VLAN tag configured on the interface.</li> <li>• <b>Port VLAN name</b>—TLV that advertises the VLAN name configured on the interface.</li> </ul>                                                     | <b>detail</b>   |

Table 24: show lldp Output Fields (*continued*)

| Field Name              | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Level of Output |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Supported LLDP MED TLVs | <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> | detail          |

## Sample Output

### show lldp (EX3200 switches)

```

user@switch> show lldp
LLDP : Enabled
Advertisement interval : 30 seconds
Transmit delay : 2 seconds
Hold timer : 4 seconds
Notification interval : 0 Second(s)
Config Trap Interval : 0 seconds
Connection Hold timer : 300 seconds

LLDP MED : Disabled
MED fast start count : 3 Packets

```

|           |                  |         |          |                   |
|-----------|------------------|---------|----------|-------------------|
| Interface | Parent Interface | LLDP    | LLDP-MED | Power Negotiation |
| all       | -                | Enabled | Enabled  | Enabled           |

### show lldp (EX4300 switches)

```

user@switch> show lldp
LLDP : Enabled
Advertisement interval : 30 seconds
Transmit delay : 2 seconds
Hold timer : 120 seconds
Notification interval : 0 Second(s)
Config Trap Interval : 0 seconds
Connection Hold timer : 300 seconds

LLDP MED : Disabled
MED fast start count : 3 Packets

```

| Interface | Parent Interface | LLDP    | LLDP-MED | Power Negotiation |
|-----------|------------------|---------|----------|-------------------|
| all       | -                | Enabled | Enabled  | Enabled           |

**show lldp detail (EX4300 switches)**

```

user@switch> show lldp detail
LLDP : Enabled
Advertisement interval : 30 seconds
Transmit delay : 2 seconds
Hold timer : 120 seconds
Notification interval : 0 Second(s)
Config Trap Interval : 0 seconds
Connection Hold timer : 300 seconds

LLDP MED : Disabled
MED fast start count : 3 Packets

```

| Interface      | Parent Interface | LLDP    | LLDP-MED | Power Negotiation |
|----------------|------------------|---------|----------|-------------------|
| Neighbor count |                  |         |          |                   |
| all            | -                | Enabled | Enabled  | Enabled           |
| 8              |                  |         |          |                   |

| Interface  | Parent Interface | Vlan-id | Vlan-name |
|------------|------------------|---------|-----------|
| xe-3/0/0.0 | ae31.0           | 100     | v100      |
| xe-3/0/0.0 | ae31.0           | 101     | v101      |
| xe-3/0/0.0 | ae31.0           | 4000    | v4000     |
| xe-3/0/1.0 | ae31.0           | 100     | v100      |
| xe-3/0/1.0 | ae31.0           | 101     | v101      |
| xe-3/0/1.0 | ae31.0           | 4000    | v4000     |
| xe-3/0/2.0 | ae31.0           | 100     | v100      |
| xe-3/0/2.0 | ae31.0           | 101     | v101      |
| xe-3/0/2.0 | ae31.0           | 4000    | v4000     |

**LLDP basic TLVs supported:**

Chassis identifier, Port identifier, Port description, System name, System description, System capabilities, Management address.

**Supported LLDP 802 TLVs:**

MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum frame size, Port VLAN tag, Port VLAN name.

**Supported LLDP MED TLVs:**

LLDP MED capabilities, Network policy, Endpoint location, Extended power Via MDI.



## show lldp local-information

|                                 |                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <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 14.1X53-D20 for OCX Series switches.<br>Command introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                       |
| <b>Description</b>              | Display the information that the switch provides in Link Layer Discovery Protocol (LLDP) advertisements to its neighbors.                                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring LLDP (CLI Procedure) on page 138</a></li> <li>• <a href="#">Understanding LLDP and LLDP-MED on EX Series Switches on page 135</a></li> <li>• <i>management-address</i></li> <li>• <i>Configuring LLDP</i></li> <li>• <i>Understanding LLDP</i></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show lldp local-information (EX Series Switch) on page 266</a>                                                                                                                                                                                                                                                 |
| <b>Output Fields</b>            | <a href="#">Table 25 on page 265</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 25: show lldp local-information Output Fields**

| Field Name                            | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>LLDP Local Information details</b> | <p>Information about the local system (the switch):</p> <ul style="list-style-type: none"> <li>• <b>Chassis ID</b>—MAC address associated with the switch.</li> <li>• <b>System name</b>—User-configured name of the switch.</li> <li>• <b>System descr</b>—System description containing information about the switch model and the current software image running on the switch. This information is taken from the software and is not configurable.</li> </ul>                                                                                                                                                                                                                               |
| <b>System Capabilities</b>            | Capabilities (such as <b>bridge</b> or <b>router</b> ) that are supported or enabled on the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Management Information</b>         | <p>Details of the management information: <b>Port Name</b>, <b>Port Address</b> (such as 10.204.34.35), <b>Address Type</b> (such as <b>ipv4</b> or <b>ipv6</b>), <b>Port ID</b> (SNMP interface index), <b>Port ID Subtype</b>, and <b>Port Subtype</b>.</p> <p>The <b>Port Subtype</b> displays:</p> <ul style="list-style-type: none"> <li>• <b>ifindex(2)</b>—IP address of the switch's management Ethernet interface (<b>me0</b>) or virtual management Ethernet (<b>VME</b>) interface address (for a virtual chassis) is used to manage the switch.</li> <li>• <b>unknown(1)</b>—IP management address has been configured with set <b>protocols lldp management-address</b>.</li> </ul> |

Table 25: 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>`

**Release Information** Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Display the information about neighboring devices learned by the switch by using the Link Layer Discovery Protocol (LLDP).



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

**Options** `interface interface`—(Optional) Display LLDP neighbor information for a selected interface.

**Required Privilege Level** view

**Related Documentation**

- [Configuring LLDP \(CLI Procedure\) on page 138](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 135](#)

**List of Sample Output**

[show lldp neighbors on page 269](#)  
[show lldp neighbors interface ge-0/0/2 on page 270](#)  
[show lldp neighbors interface ge-0/0/0.0 \(for a VoIP Avaya Telephone with LLDP-MED Support\) on page 271](#)  
[show lldp neighbors interface ge-0/0/5.0 \(with NetBIOS Snooping Enabled on the Switch\) on page 272](#)

**Output Fields** [Table 26 on page 267](#) lists the output fields for the `show lldp neighbors` command. Output fields are listed in the approximate order in which they appear.

**Table 26: 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        | This field displays the port information received from neighbors.                     |

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

| Field Name                | Field Description                                                                                                                                                                                                                                                 |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System name               | List of system names gathered from neighbors.                                                                                                                                                                                                                     |
| LLDP Neighbor Information | Information about both the local system (the switch) and a neighbor system on the interface (appears when the <b>interface</b> option is used).                                                                                                                   |
| Local Information         | Information about the local system (appears when the <b>interface</b> option is used).                                                                                                                                                                            |
| Index                     | Local interface index (appears when the <b>interface</b> option is used).                                                                                                                                                                                         |
| Time to live              | Number of seconds for which this information is valid (appears when the <b>interface</b> option is used).                                                                                                                                                         |
| Time mark                 | Date and timestamp of information (appears when the <b>interface</b> option is used).                                                                                                                                                                             |
| Local Interface           | Name of the local physical interface (appears when the <b>interface</b> option is used).                                                                                                                                                                          |
| Parent Interface          | Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the <b>interface</b> option is used).                                                                                                                             |
| Local Port ID             | Local interface SNMP index (appears when the <b>interface</b> option is used).                                                                                                                                                                                    |
| Ageout Count              | Number of times the complete set of information advertised by the neighbor has been deleted from LLDP neighbor information maintained by the local system because the information timeliness interval expired (appears when the <b>interface</b> option is used). |
| Neighbor Information      | Information about a neighbor system on the interface (appears when the <b>interface</b> option is used).                                                                                                                                                          |
| Chassis type              | Type of chassis identifier supplied, such as <b>Mac address</b> (appears when the <b>interface</b> option is used).                                                                                                                                               |
| Chassis ID                | Chassis identifier of the chassis type listed (appears when the <b>interface</b> option is used).                                                                                                                                                                 |
| Port type                 | Type of port identifier supplied, such as <b>Locally assigned</b> (appears when the <b>interface</b> option is used).                                                                                                                                             |
| Port ID                   | Port identifier of the port type listed (appears when the <b>interface</b> option is used).                                                                                                                                                                       |
| Port description          | The port description field uses the configured port description, the port name or the SNMP ifIndex (appears when the <b>interface</b> option is used).                                                                                                            |
| System name               | Name supplied by the system on the interface (appears when the <b>interface</b> option is used).                                                                                                                                                                  |

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

| Field Name                 | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System Description</b>  | Description supplied by the system on the interface (appears when the <b>interface</b> option is used).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>System capabilities</b> | Capabilities (such as <b>Bridge</b> , <b>Bridge Router</b> , and <b>Bridge Telephone</b> ) that are supported or enabled by the system on the interface (appears when the <b>interface</b> option is used).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Management Info</b>     | <p>Details of management information: <b>Type</b> (such as IPv4 or IPv6), <b>Address</b> (such as 10.204.34.35), <b>Port ID</b>, <b>Subtype</b>, <b>Interface Subtype</b>, and organization identifier (<b>OID</b>) (appears when the <b>interface</b> option is used).</p> <p>The <b>Interface Subtype</b> displays:</p> <ul style="list-style-type: none"> <li><b>ifIndex(2)</b>— IP address of the neighbor's management Ethernet interface (<b>me0</b>) or virtual management Ethernet (<b>VME</b>) interface address (for a Virtual Chassis) is used to manage the switch.</li> <li><b>unknown(1)</b>—Neighbor's IP management address has been configured with set <b>protocols lldp management-address</b>.</li> </ul> |
| <b>Media Info</b>          | Additional details about the endpoint device appear when a device that supports LLDP-MED is attached to the interface. The specific details depend upon the capabilities of the device. Details might include: <b>Media endpoint class</b> (such as Class 3 for communication devices such as IP phones), <b>MED Hardware revision</b> , <b>MED Firmware revision</b> , <b>MED Software revision</b> , <b>MED Serial number</b> , <b>MED Manufacturer name</b> , <b>MED Model name</b> .                                                                                                                                                                                                                                      |
| <b>Organization Info</b>   | One or more entries listing remote information by organizationally unique identifier ( <b>OUI</b> ), <b>Subtype</b> , <b>Index</b> , and <b>Info</b> (appears when the <b>interface</b> option is used).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Age</b>                 | How long the neighbor has been identified (appears when the <b>interface</b> option is used and NetBIOS snooping is enabled on the switch).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Local Interface</b>     | Name of the local physical interface (appears when the <b>interface</b> option is used and NetBIOS snooping is enabled on the switch).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Parent Interface</b>    | Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the <b>interface</b> option is used and NetBIOS snooping is enabled on the switch).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Chassis ID</b>          | Chassis identifier of the chassis type listed (appears when the <b>interface</b> option is used and NetBIOS snooping is enabled on the switch).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>System name</b>         | NetBIOS name of the host (appears when the <b>interface</b> option is used and NetBIOS snooping is enabled on the switch).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Sample Output

### show lldp neighbors

```
user@switch> show lldp neighbors
```

| Local Interface | Parent Interface | Chassis Id        | Port info  | System Name |
|-----------------|------------------|-------------------|------------|-------------|
| xe-3/0/4.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/0/0.0 | newyork31   |
| xe-3/0/5.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/0/1.0 | newyork31   |
| xe-3/0/6.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/0/2.0 | newyork31   |
| xe-3/0/7.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/0/3.0 | newyork31   |
| xe-3/0/0.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/1/0.0 | newyork31   |
| xe-3/0/1.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/1/1.0 | newyork31   |
| xe-3/0/2.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/1/2.0 | newyork31   |
| xe-3/0/3.0      | ae31.0           | b0:c6:9a:63:80:40 | xe-0/1/3.0 | newyork31   |

### show lldp neighbors interface ge-0/0/2

```
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 : IEEE 802.3 Private (0x00120f)
Subtype : MAC/PHY Configuration/Status (1)
Info : Autonegotiation [supported, enabled (0x3)], PMD Autonegotiation
Capability (0x1d00), MAU Type (0x0)
Index : 1
```

#### Organization Info

```
OUI : IEEE 802.3 Private (0x00120f)
Subtype : MDI Power (2)
Info : MDI Power Support [PSE supported], MDI Power Pair (signal),
MDI Power Class (class0)
Index : 2
```

**show lldp neighbors interface ge-0/0/0.0 (for a VoIP AvayaTelephone with LLDP-MED Support)**

```
user@switch>show lldp neighbors interface ge-0/0/0.0
```

**LLDP Neighbor Information:****Local Information:**

```
Index: 20 Time to live: 120 Time mark: Thu Apr 15 22:26:22 2010 Age: 16 secs
Local Interface : ge-0/0/0.0
Parent Interface : -
Local Port ID : 517
Ageout Count : 0
```

**Neighbour Information:**

```
Chassis type : Network address
Chassis ID : 0.0.0.0
Port type : Mac address
Port ID : 00:04:0d:fc:55:48
System name : AVAFC5548
```

**System capabilities**

```
Supported : Bridge Telephone
Enabled : Bridge
```

**Management Info**

```
Type : IPv4
Address : 0.0.0.0
Port ID : 1
Subtype : 1
Interface Subtype : ifIndex(2)
OID : 1.3.6.1.2.1.31.1.1.1.1.1
```

```
Media endpoint class: Class III Device
```

```
MED Hardware revision : 4610D01A
MED Firmware revision : b10d01b2_9.bin
MED Software revision : a10d01b2_9.bin
MED Serial number : 07N510103424
MED Manufacturer name : Avaya
MED Model name : 4610
```

**Organization Info**

```
OUI : IEEE 802.3 Private (0x00120f)
Subtype : MAC/PHY Configuration/Status (1)
Info : Autonegotiation [supported, enabled (0x3)], PMD Autonegotiation
Capability (0x1d00), MAU Type (0x0)
Index : 1
```

**Organization Info**

```
OUI : IEEE 802.3 Private (0x00120f)
Subtype : MDI Power (2)
Info : MDI Power Support [PSE supported], MDI Power Pair (signal),
MDI Power Class (class0)
Index : 2
```

**Organization Info**

```
OUI : IEEE 802.3 Private (0x00120f)
Subtype : Link Aggregation (3)
Info : Aggregation Status (supported), Aggregation Port ID (0)
Index : 3
```

**Organization Info**

```
OUI : IEEE 802.3 Private (0x00120f)
```

```
Subtype : Maximum Frame Size (4)
Info : MTU Size (1514)
Index : 4
```

Organization Info

```
OUI : Ethernet Bridged (0x0080c2)
Subtype : Port Vid (1)
Info : VLAN ID (10),
Index : 5
```

Organization Info

```
OUI : Juniper Specific (0x009069)
Subtype : Chassis Serial Type (1)
Info : Juniper Slot Serial [BQ0208211462]
Index : 6
```

Organization Info

```
OUI : Ethernet Bridged (0x0080c2)
Subtype : VLAN Name (3)
Info : VLAN ID (10), VLAN Name (vtest)
Index : 7
```

**show lldp neighbors interface ge-0/0/5.0 (with NetBIOS Snooping Enabled on the Switch)**

```
user@switch> show lldp neighbors interface ge-0/0/5
```

```
Age: 299999 secs
Local Interface : ge-0/0/5.0
Parent Interface : -
Chassis ID : 00:10:94:00:00:02
Port description : 192.0.2.1
System name : JNPRU\
```



## show lldp remote-global-statistics

|                                 |                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show lldp remote-global-statistics                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.0 for EX Series switches.                                                                                                                                           |
| <b>Description</b>              | Display remote Link Layer Discovery Protocol (LLDP) global statistics.                                                                                                                                        |
| <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>• <a href="#">Configuring LLDP (CLI Procedure) on page 138</a></li> <li>• <a href="#">Understanding LLDP and LLDP-MED on EX Series Switches on page 135</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show lldp remote-global-statistics on page 274</a>                                                                                                                                                |
| <b>Output Fields</b>            | <a href="#">Table 27 on page 273</a> describes the output fields for the <b>show lldp remote-global-statistics</b> command. Output fields are listed in the approximate order in which they appear.           |

**Table 27: show lldp remote-global-statistics Output Fields**

| Field Name                          | Field Description                                                                                     |
|-------------------------------------|-------------------------------------------------------------------------------------------------------|
| LLDP Remote Database Table Counters | Information about remote database table counters.                                                     |
| LastchangeTime                      | Time elapsed between LLDP agent startup and the last change to the remote database table information. |
| Inserts                             | Number of insertions made in the remote database table.                                               |
| Deletes                             | Number of deletions made in the remote database table.                                                |
| Drops                               | Number of LLDP frames dropped from the remote database table because of errors.                       |
| Ageouts                             | Number of remote database table entries that have aged out of the table.                              |

## Sample Output

### show lldp remote-global-statistics

```
user@host> show lldp remote-global-statistics
user@host> show lldp remote-global-statistics
LLDP Remote Database Table Counters
LastchangeTime Inserts Deletes Drops Ageouts
00:00:76 (76 sec) 192 0 0 0
```

## show lldp statistics

|                                 |                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show lldp statistics</b><br><b>&lt;interface <i>interface</i>&gt;</b>                                                                                                                                      |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                            |
| <b>Description</b>              | Display LLDP statistics for all interfaces or for the specified interface.                                                                                                                                    |
| <b>Options</b>                  | <b>none</b> —Display LLDP statistics for all interfaces.<br><br><b>interface <i>interface</i></b> —(Optional) Display LLDP statistics for the specified interface.                                            |
| <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 138</a></li> <li>• <a href="#">Understanding LLDP and LLDP-MED on EX Series Switches on page 135</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show lldp statistics on page 276</a><br><a href="#">show lldp statistics interface xe-3/0/0.0 on page 276</a>                                                                                     |
| <b>Output Fields</b>            | <a href="#">Table 28 on page 275</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 28: show lldp statistics Output Fields**

| Field Name              | Field Description                                                                                                                                                                                                                                                              |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Interface</b>        | Name of the interface.                                                                                                                                                                                                                                                         |
| <b>Parent Interface</b> | Name of the aggregated Ethernet interface, if any, to which the interface belongs.<br><br><b>NOTE:</b> Because LLDP packets are transmitted and received on member interfaces only, statistics are available only for the member interfaces, not for the aggregated interface. |
| <b>Received</b>         | Total number of LLDP frames received on an interface.                                                                                                                                                                                                                          |
| <b>Unknown TLVs</b>     | Number of unrecognized LLDP TLVs received on an interface.                                                                                                                                                                                                                     |
| <b>With Errors</b>      | Number of invalid LLDP TLVs received on an interface.                                                                                                                                                                                                                          |
| <b>Discarded</b>        | Number of LLDP TLVs received and then discarded on an interface.                                                                                                                                                                                                               |
| <b>Transmitted</b>      | Total number of LLDP frames that were transmitted on an interface.                                                                                                                                                                                                             |
| <b>Untransmitted</b>    | Total number of LLDP frames that were untransmitted on an interface.                                                                                                                                                                                                           |

## Sample Output

### show lldp statistics

```
user@switch> show lldp statistics
```

| Interface  | Parent Interface | Received | Unknown TLVs | With Errors |
|------------|------------------|----------|--------------|-------------|
| xe-3/0/0.0 | ae31.0           | 1564     | 0            | 0           |
| xe-3/0/1.0 | ae31.0           | 1564     | 0            | 0           |
| xe-3/0/2.0 | ae31.0           | 1565     | 0            | 0           |
| xe-3/0/3.0 | ae31.0           | 1566     | 0            | 0           |
| xe-3/0/4.0 | ae31.0           | 1598     | 0            | 0           |
| xe-3/0/5.0 | ae31.0           | 1598     | 0            | 0           |
| xe-3/0/6.0 | ae31.0           | 1596     | 0            | 0           |
| xe-3/0/7.0 | ae31.0           | 1597     | 0            | 0           |
| xe-5/0/6.0 | -                | 0        | 0            | 0           |
| xe-5/0/7.0 | -                | 0        | 0            | 0           |

| Discarded TLVs | Transmitted | Untransmitted |
|----------------|-------------|---------------|
| 0              | 3044        | 1             |
| 0              | 3044        | 1             |
| 0              | 3044        | 1             |
| 0              | 3044        | 1             |
| 0              | 3075        | 1             |
| 0              | 3075        | 1             |
| 0              | 3075        | 1             |
| 0              | 3075        | 1             |
| 0              | 17312       | 0             |
| 0              | 17312       | 0             |

### show lldp statistics interface xe-3/0/0.0

```
user@switch> show lldp statistics interface xe-3/0/0.0
```

| Interface  | Parent Interface | Received | Unknown TLVs | With Errors |
|------------|------------------|----------|--------------|-------------|
| xe-3/0/0.0 | ae31.0           | 1566     | 0            | 0           |

| Discarded TLVs | Transmitted | Untransmitted |
|----------------|-------------|---------------|
| 0              | 3046        | 1             |

## show 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>• <i>accounting-server</i></li> <li>• <i>accounting-stop-on-access-deny</i></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 277</a>                                                                                                                                  |
| <b>Output Fields</b>            | <a href="#">Table 29 on page 277</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 29: show network-access aaa statistics accounting Output Fields**

| Field Name                          | Field Description                                                                                       |
|-------------------------------------|---------------------------------------------------------------------------------------------------------|
| <b>Requests received</b>            | The number of accounting-request packets sent from a switch to a RADIUS accounting server.              |
| <b>Accounting Response failures</b> | The number of accounting-response failure packets sent from the RADIUS accounting server to the switch. |
| <b>Accounting Response Success</b>  | The number of accounting-response success packets sent from the RADIUS accounting server to the switch. |
| <b>Requests timedout</b>            | 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><i>authentication-server</i></li> <li><a href="#">Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 35</a></li> </ul>       |
| <b>List of Sample Output</b>    | <a href="#">show network-access aaa statistics authentication on page 278</a><br><a href="#">show network-access aaa statistics authentication (in QFX Series Switches) on page 278</a>        |
| <b>Output Fields</b>            | Table 30 on page 278 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 30: show network-access aaa statistics authentication Output Fields

| Field Name        | Field Description                                                   |
|-------------------|---------------------------------------------------------------------|
| Requests received | The number of authentication requests received by the switch.       |
| Accepts           | The number of authentication accepts received by the RADIUS server. |
| Rejects           | The number authentication rejects sent by the RADIUS server.        |
| Challenges        | The number of authentication challenges sent by the RADIUS server.  |

## Sample Output

### show network-access aaa statistics authentication

```

user@switch> show network-access aaa statistics authentication
Authentication module statistics
Requests received: 2
Accepts: 1
Rejects: 0
Challenges: 1

```

### show network-access aaa statistics authentication (in QFX Series Switches)

```

user@switch> show network-access aaa statistics authentication
Authentication module statistics
Requests received: 2
Accepts: 1

```

Rejects: 0  
Challenges: 1

## show network-access aaa statistics dynamic-requests

|                                 |                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <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><i>authentication-server</i></li> <li><a href="#">Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 35</a></li> </ul>                         |
| <b>List of Sample Output</b>    | <a href="#">show network-access aaa statistics authentication on page 280</a>                                                                                                                                    |
| <b>Output Fields</b>            | <a href="#">Table 31 on page 280</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 31: show network-access aaa statistics dynamic-requests Output Fields**

| Field Name               | Field Description                                                                              |
|--------------------------|------------------------------------------------------------------------------------------------|
| Requests received        | The number of dynamic requests received by the RADIUS server.                                  |
| Processed successfully   | The number of dynamic requests successfully processed by the RADIUS server.                    |
| Errors during processing | The number of errors that occurred while the RADIUS server was processing the dynamic request. |
| Silently dropped         | The number of silently dropped requests.                                                       |

## Sample Output

### show network-access aaa statistics authentication

```

user@switch> show network-access aaa statistics dynamic-requests
Dynamic-requests module statistics
 Requests received: 0
 Processed successfully: 0
 Errors during processing: 0
 Silently dropped: 0

```