



Junos[®] OS for EX Series Ethernet Switches

Access Control Feature Guide for EX Series Switches

Release
15.1



Modified: 2016-04-26

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.

Junos[®] OS for EX Series Ethernet Switches Access Control Feature Guide for EX Series Switches
Release 15.1
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	xv
	Documentation and Release Notes	xv
	Supported Platforms	xv
	Using the Examples in This Manual	xv
	Merging a Full Example	xvi
	Merging a Snippet	xvi
	Documentation Conventions	xvii
	Documentation Feedback	xix
	Requesting Technical Support	xix
	Self-Help Online Tools and Resources	xix
	Opening a Case with JTAC	xx
Part 1	Overview	
Chapter 1	Security Features Overview	3
	Security Features for EX Series Switches Overview	3
Chapter 2	Access Control Overview	7
	802.1X for EX Series Switches Overview	7
	How 802.1X Authentication Works	7
	802.1X Features Overview	8
	Understanding Authentication on EX Series Switches	10
	Sample Authentication Topology	10
	802.1X Authentication	11
	MAC RADIUS Authentication	13
	Captive Portal Authentication	13
	Static MAC Bypass of Authentication	14
	Fallback of Authentication Methods	15
	Understanding Guest VLANs for 802.1X on EX Series Switches	16
	Understanding 802.1X and RADIUS Accounting on EX Series Switches	16
	RADIUS Accounting Process	16
	Supported RADIUS Attributes	17
	Understanding LLDP and LLDP-MED on EX Series Switches	18
	Understanding 802.1X and VoIP on EX Series Switches	21
	Understanding Dynamic Filters Based on RADIUS Attributes	23
	Understanding Dynamic VLAN Assignment Using RADIUS Attributes	24
	Understanding RADIUS-Initiated Changes to an Authorized User Session	25
	Disconnect Messages	25
	Change of Authorization Messages	26
	Error-Cause Codes	26

	Understanding Server Fail Fallback and Authentication on EX Series Switches	28
	Authentication Process Flow for EX Series Switches	29
	Understanding Authentication Session Timeout	31
	Understanding NetBIOS Snooping	32
	What Is a NetBIOS Name?	32
	How NetBIOS Snooping Works	32
	Understanding Centralized Network Access Control and EX Series Switches	33
	NAC Using Any RADIUS Server and Access Policies Defined on the Local Switch	33
	Centralized NAC Using Junos Pulse Access Control Service	33
	Captive Portal Authentication	34
	Understanding Central Web Authentication	35
	Central Web Authentication Process	35
	Dynamic Firewall Filters for Central Web Authentication	37
	Redirect URL for Central Web Authentication	37
Part 2	Configuration	
Chapter 3	Configuration Examples	41
	Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch	41
	Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch	45
	Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch	50
	Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch	56
	Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support	64
	Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication	68
	Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch	75
	Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch	79
	Example: Configuring MAC RADIUS Authentication on an EX Series Switch	85
	Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch	91
	Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication	97
	Example: Setting Up Captive Portal Authentication on an EX Series Switch	102
	Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients	107
	Example: Configuring Centralized Access Control to Network Resources, with an EX Series Switch Connected to Junos Pulse Access Control Service	111
Chapter 4	Configuration Tasks	125
	Configuring 802.1X Interface Settings (CLI Procedure)	126
	Configuring 802.1X Authentication (J-Web Procedure)	127

Configuring 802.1X RADIUS Accounting (CLI Procedure)	130
Filtering 802.1X Supplicants by Using RADIUS Server Attributes	131
Configuring Firewall Filters on the RADIUS Server	132
Applying a Locally Configured Firewall Filter from the RADIUS Server	135
Configuring LLDP (CLI Procedure)	136
Enabling LLDP on Interfaces	136
Adjusting LLDP Advertisement Settings	137
Adjusting SNMP Notification Settings of LLDP Changes	137
Specifying a Management Address for the LLDP Management TLV	138
Configuring LLDP Power Negotiation	138
Configuring LLDP (J-Web Procedure)	139
Configuring LLDP-MED (CLI Procedure)	140
Enabling LLDP-MED on Interfaces	140
Configuring Location Information Advertised by the Switch	141
Configuring a Fast Start for LLDP-MED	141
Juniper-Switching-Filter VSA Match Conditions and Actions	142
Configuring RADIUS Server Fail Fallback (CLI Procedure)	144
Configuring MAC RADIUS Authentication (CLI Procedure)	146
Configuring Flexible Authentication Order	147
Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication (CLI Procedure)	149
Specifying RADIUS Server Connections on an EX Series Switch (CLI Procedure)	150
Configuring Captive Portal Authentication (CLI Procedure)	151
Configuring Secure Access for Captive Portal	151
Enabling an Interface for Captive Portal	152
Configuring Bypass of Captive Portal Authentication	152
Designing a Captive Portal Authentication Login Page on an EX Series Switch	153
Controlling Authentication Session Timeouts (CLI Procedure)	155
Configuring NetBIOS Snooping (CLI Procedure)	156
Enabling NetBIOS Snooping	156
Disabling NetBIOS Snooping	156
Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)	157
Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure)	159
Configuring Central Web Authentication	160
Configuring Dynamic Firewall Filters for Central Web Authentication	161
Configuring the Redirect URL for Central Web Authentication	161
Guidelines for Configuring Central Web Authentication	162

Chapter 5	Configuration Statements	165
	[edit access] Configuration Statement Hierarchy on EX Series Switches	169
	Supported Statements in the [edit access] Hierarchy Level	169
	Unsupported Statements in the [edit access] Hierarchy Level	171
	[edit ethernet-switching-options] Configuration Statement Hierarchy on EX Series Switches	172
	Supported Statements in the [edit ethernet-switching-options] Hierarchy Level	173
	Unsupported Statements in the [edit ethernet-switching-options] Hierarchy Level	175
	[edit protocols] Configuration Statement Hierarchy on EX Series Switches	176
	[edit protocols dot1x] Configuration Statement Hierarchy on EX Series Switches	177
	Supported Statements in the [edit protocols dot1x] Hierarchy Level	177
	Unsupported Statements in the [edit protocols dot1x] Hierarchy Level	178
	[edit protocols lldp] Configuration Statement Hierarchy on EX Series Switches	179
	Supported Statements in the [edit protocols lldp] Hierarchy Level	179
	Unsupported Statements in the [edit protocols lldp] Hierarchy Level	180
	[edit protocols lldp-med] Configuration Statement Hierarchy on EX Series Switches	180
	Supported Statements in the [edit protocols lldp-med] Hierarchy Level	180
	Unsupported Statements in the [edit protocols lldp-med] Hierarchy Level	181
	access	182
	accounting (Access Profile)	183
	accounting	184
	accounting-port (RADIUS Server)	185
	accounting-port	186
	accounting-server	187
	accounting-session-id-format	188
	accounting-stop-on-access-deny	189
	accounting-stop-on-failure	190
	address (Access Address Pool)	191
	address (Access Control Service)	191
	address-pool	192
	address-range	192
	advertisement-interval	193
	attributes	194
	authentication-order (Access Profile)	195
	authentication-order (Authenticator)	196
	authentication-profile-name	198
	authentication-protocol	199
	authentication-server	200
	authentication-whitelist	201
	authenticator	202
	block-interval	203
	ca-type	204
	ca-value	205

captive-portal	206
certificate-verification	207
civic-based	208
country-code	209
custom-options	210
destination (Accounting)	212
disable (802.1X)	213
disable (LLDP)	214
disable (LLDP-MED)	214
disable (LLDP Power Negotiation)	215
dot1x	216
elin	217
eapol-block	218
ethernet-port-type-virtual	218
ethernet-switching-options	219
events	222
exclude (RADIUS)	223
fast-start (LLDP-MED)	227
forwarding-class (VoIP)	228
guest-vlan	229
hold-multiplier	230
ignore	231
immediate-update	232
infranet-controller	232
interface (802.1X)	233
interface (Access Control Service)	234
interface (Captive Portal)	235
interface (LLDP)	236
interface (LLDP-MED)	237
interface (Static MAC Bypass)	238
interface (VoIP)	239
interface-description-format	240
interval (Access Control Service)	241
lldp	242
lldp-configuration-notification-interval	244
lldp-med (Ethernet Switching)	245
lldp-med-bypass	246
lldp-priority	246
location (LLDP-MED)	247
mac-radius	248
management-address	249
maximum-requests	250
nas-identifier	250
nas-port-extended-format	251
netbios-snooping	252
no-mac-table-binding (802.1X)	252
no-reauthentication	253
no-tagging	253
options	254

order	256
password (Access Control Service)	257
port	257
port (Access Control Service)	258
port (RADIUS Server)	259
port (TACACS+ Server)	259
power-negotiation	260
profile	261
ptopo-configuration-maximum-hold-time	262
ptopo-configuration-trap-interval	262
quiet-period	263
quiet-period (Captive Portal)	263
radius (Access Profile)	264
radius (System)	266
radius	267
radius-options (Protocols 802.1X)	268
radius-server	269
radius-server (System)	270
reauthentication	271
redirect-url	272
retries	273
retries (Captive Portal)	274
retry	275
retry (RADIUS)	276
revert-interval	277
routing-instance	277
secret	278
secret	279
secure-authentication	279
server (RADIUS Accounting)	280
server (TACACS+ Accounting)	281
server-fail	282
server-reject-vlan	283
server-timeout	284
server-timeout (Captive Portal)	285
session-expiry	286
single-connection	287
source-address	287
source-address (NTP, RADIUS, System Logging, or TACACS+)	288
static (Protocols 802.1X)	289
statistics (Access Profile)	290
supplicant	291
supplicant-timeout	292
tacplus	293
timeout (System)	294
timeout (Access Control Service)	295
timeout (RADIUS)	296
timeout-action (Access Control Service)	297
traceoptions (802.1X)	298

	traceoptions (LLDP)	300
	transmit-delay	302
	transmit-period	303
	uac-policy	303
	uac-service	304
	unified-access-control	305
	update-interval	306
	vlan-assignment	307
	vlan-nas-port-stacked-format	308
	voip	308
	what	309
Part 3	Administration	
Chapter 6	Routine Monitoring	313
	Monitoring 802.1X Authentication	313
	Verifying 802.1X Authentication	314
Chapter 7	Operational Commands	317
	clear captive-portal	318
	clear dot1x	320
	clear lldp neighbors	322
	clear lldp statistics	323
	show captive-portal authentication-failed-users	324
	show captive-portal firewall	326
	show captive-portal interface	328
	show dot1x	331
	show dot1x authentication-failed-users	336
	show dot1x firewall	337
	show dot1x static-mac-address	338
	show ethernet-switching interfaces	340
	show lldp	344
	show lldp local-information	349
	show lldp neighbors	351
	show lldp remote-global-statistics	357
	show lldp statistics	359
	show network-access aaa statistics accounting	361
	show network-access aaa statistics authentication	362
	show network-access aaa statistics dynamic-requests	364
	show services unified-access-control authentication-table	365
	show services unified-access-control policies	367
	show services unified-access-control status	369
Part 4	Troubleshooting	
Chapter 8	Troubleshooting	373
	Troubleshooting Authentication of End Devices on EX Series Switches	373

List of Figures

Part 1	Overview	
Chapter 2	Access Control Overview	7
	Figure 1: Example Authentication Topology	11
	Figure 2: VoIP Multiple Supplicant Topology	22
	Figure 3: VoIP Single Supplicant Topology	23
	Figure 4: Authentication Process Flow for an EX Series Switch	30
	Figure 5: Central Web Authentication Process	37
Part 2	Configuration	
Chapter 3	Configuration Examples	41
	Figure 6: Topology for Configuration	43
	Figure 7: Topology for Guest VLAN Example	47
	Figure 8: Topology for Configuring Supplicant Modes	52
	Figure 9: VoIP Topology	58
	Figure 10: Topology for Static MAC Bypass of Authentication Configuration	76
	Figure 11: Topology for Configuring 802.1X Options	81
	Figure 12: Topology for MAC RADIUS Authentication Configuration	87
	Figure 13: Topology for Firewall Filter and RADIUS Server Attributes Configuration	93
	Figure 14: Conceptual Model: Dynamic Filter Updated for Each New User	99
	Figure 15: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server	100
	Figure 16: EX Series Switch Connecting OAC to RADIUS Server Using EAP-TTLS Authentication	109
	Figure 17: Centralized Access Control to Network Resources with an EX Series Switch Connected to Junos Pulse Access Control Service	114
Chapter 4	Configuration Tasks	125
	Figure 18: Example of a Captive Portal Login Page	153

List of Tables

	About the Documentation	xv
	Table 1: Notice Icons	xvii
	Table 2: Text and Syntax Conventions	xvii
Part 1	Overview	
Chapter 2	Access Control Overview	7
	Table 3: RADIUS Accounting Request Attributes	18
	Table 4: Error-Cause Codes (RADIUS Attribute 101)	27
Part 2	Configuration	
Chapter 3	Configuration Examples	41
	Table 5: Components of the Topology	43
	Table 6: Components of the Guest VLAN Topology	47
	Table 7: Components of the Supplicant Mode Configuration Topology	52
	Table 8: Components of the VoIP Configuration Topology	58
	Table 9: Components of the Static MAC Bypass of Authentication Configuration Topology	77
	Table 10: Components of the Topology	81
	Table 11: Components of the MAC RADIUS Authentication Configuration Topology	87
	Table 12: Components of the Firewall Filter and RADIUS Server Attributes Topology	93
	Table 13: Components of the OAC Deployment	109
	Table 14: Components of the Topology for Access Control Service and the EX Series Switch	114
Chapter 4	Configuration Tasks	125
	Table 15: RADIUS Server Settings	128
	Table 16: 802.1X Exclusion List	128
	Table 17: 802.1X Port Settings	129
	Table 18: Global Settings	140
	Table 19: Edit Port Settings	140
	Table 20: Match Conditions	142
	Table 21: Actions for VSAs	143
	Table 22: Configurable Elements of a Captive Portal Login Page	153
Chapter 5	Configuration Statements	165
	Table 23: Unsupported [edit access] Configuration Statements on EX Series Switches	171

Part 3

Chapter 7

Administration

Operational Commands	317
Table 24: clear captive-portal interface Output Fields	318
Table 25: show captive-portal authentication-failed-users Output Fields	324
Table 26: show captive-portal interface Output Fields	328
Table 27: show dot1x Output Fields	331
Table 28: show dot1x authentication-failed-users Output Fields	336
Table 29: show dot1x static-mac-address Output Fields	338
Table 30: show ethernet-switching interfaces Output Fields	341
Table 31: show lldp Output Fields	344
Table 32: show lldp local-information Output Fields	349
Table 33: show lldp neighbors Output Fields	351
Table 34: show lldp remote-global-statistics Output Fields	357
Table 35: show lldp statistics Output Fields	359
Table 36: show network-access aaa statistics accounting Output Fields	361
Table 37: show network-access aaa statistics authentication Output Fields	362
Table 38: show network-access aaa statistics dynamic-requests Output Fields	364

About the Documentation

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

Documentation and Release Notes

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

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

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

Supported Platforms

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

- 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 the *CLI User Guide*.

Documentation Conventions

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

Table 1: Notice Icons







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

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

Table 2: Text and Syntax Conventions

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

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

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	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>.

PART 1

Overview

- [Security Features Overview on page 3](#)
- [Access Control Overview on page 7](#)

CHAPTER 1

Security Features Overview

- [Security Features for EX Series Switches Overview on page 3](#)

Security Features for EX Series Switches Overview

Juniper Networks Junos operating system (Junos OS) is a network operating system that has been hardened through the separation of control forwarding and services planes, with each function running in protected memory. The control-plane CPU is protected by rate limiting, routing policy, and firewall filters to ensure switch uptime even under severe attack. Access port security features such as dynamic Address Resolution Protocol (ARP) inspection, DHCP snooping, and MAC limiting are controlled through a single Junos OS CLI command.

Juniper Networks EX Series Ethernet Switches provide the following hardware and software security features:

Console Port—Allows use of the console port to connect to the Routing Engine through an RJ-45 cable. You then use the command-line interface (CLI) to configure the switch.

Out-of-Band Management—A dedicated management Ethernet port on the rear panel allows out-of-band management.

Software Images—All Junos OS images are signed by Juniper Networks certificate authority (CA) with public key infrastructure (PKI).

User Authentication, Authorization, and Accounting (AAA)—Features include:

- User and group accounts with password encryption and authentication.
- Access privilege levels configurable for login classes and user templates.
- RADIUS authentication, TACACS+ authentication, or both, for authenticating users who attempt to access the switch.
- Auditing of configuration changes through system logging or RADIUS/TACACS+.

802.1X Authentication—Provides network access control. Supplicants (hosts) are authenticated when they initially connect to a LAN. Authenticating supplicants before they receive an IP address from a DHCP server prevents unauthorized supplicants from gaining access to the LAN. EX Series switches support Extensible Authentication Protocol (EAP) methods, including EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP.

Port Security—Access port security features include:

- DHCP snooping—Filters and blocks ingress DHCP server messages on untrusted ports; builds and maintains an IP-address/MAC-address binding database (called the DHCP snooping database).
- Dynamic ARP inspection (DAI)—Prevents ARP spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons.
- MAC limiting—Protects against flooding of the Ethernet switching table.
- MAC move limiting—Detects MAC movement and MAC spoofing on access ports.
- Trusted DHCP server—With a DHCP server on a trusted port, protects against rogue DHCP servers sending leases.
- IP source guard—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. The source IP address in the packet sent from an untrusted access interface is validated against the source MAC address in the DHCP snooping database. The packet is allowed for further processing if the source IP address to source MAC address binding is valid; if the binding is not valid, the packet is discarded.
- DHCP option 82—Also known as the DHCP relay agent information option. Helps protect the EX Series switch against attacks such as spoofing (forging) of IP addresses and MAC addresses and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.
- Unrestricted proxy ARP—The switch responds to all ARP messages with its own MAC address. Hosts that are connected to the switch's interfaces cannot communicate directly with other hosts. Instead, all communications between hosts go through the switch.
- Restricted proxy ARP—The switch does not respond to an ARP request if the physical networks of the source and target of the ARP request are the same. It does not matter whether the destination host has the same IP address as the incoming interface or a different (remote) IP address. An ARP request for a broadcast address elicits no reply.

Device Security—Storm control permits the switch to monitor unknown unicast and broadcast traffic and drop packets, or shut down, or temporarily disable the interface when a specified traffic level is exceeded, thus preventing packets from proliferating and degrading the LAN. You can enable storm control on access interfaces or trunk interfaces.

Firewall Filters—Allow auditing of various types of security violations, including attempts to access the switch from unauthorized locations. Firewall filters can detect such attempts and create audit log entries when they occur. The filters can also restrict access by limiting traffic to source and destination MAC addresses, specific protocols, or, in combination with policers, to specified data rates to prevent denial of service (DoS) attacks.

Policers—Provide rate-limiting capability to control the amount of traffic that enters an interface, which acts to counter DoS attacks.

Encryption Standards—Supported standards include:

- 128-, 192-, and 256-bit Advanced Encryption Standard (AES)
- 56-bit Data Encryption Standard (DES) and 168-bit 3DES

**Related
Documentation**

- [802.1X for EX Series Switches Overview on page 7](#)
- *Firewall Filters for EX Series Switches Overview*
- *Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity*
- *Understanding Proxy ARP on EX Series Switches*
- *Understanding Storm Control on EX Series Switches*
- *Understanding the Use of Policers in Firewall Filters*
- [Understanding Centralized Network Access Control and EX Series Switches on page 33](#)

CHAPTER 2

Access Control Overview

- [802.1X for EX Series Switches Overview on page 7](#)
- [Understanding Authentication on EX Series Switches on page 10](#)
- [Understanding Guest VLANs for 802.1X on EX Series Switches on page 16](#)
- [Understanding 802.1X and RADIUS Accounting on EX Series Switches on page 16](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 18](#)
- [Understanding 802.1X and VoIP on EX Series Switches on page 21](#)
- [Understanding Dynamic Filters Based on RADIUS Attributes on page 23](#)
- [Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 24](#)
- [Understanding RADIUS-Initiated Changes to an Authorized User Session on page 25](#)
- [Understanding Server Fail Fallback and Authentication on EX Series Switches on page 28](#)
- [Authentication Process Flow for EX Series Switches on page 29](#)
- [Understanding Authentication Session Timeout on page 31](#)
- [Understanding NetBIOS Snooping on page 32](#)
- [Understanding Centralized Network Access Control and EX Series Switches on page 33](#)
- [Understanding Central Web Authentication on page 35](#)

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 144](#).

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 10](#)
- [Understanding 802.1X and VoIP on EX Series Switches on page 21](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 18](#)
- [Understanding 802.1X and RADIUS Accounting on EX Series Switches on page 16](#)
- [Understanding Guest VLANs for 802.1X on EX Series Switches on page 16](#)
- [Understanding Dynamic Filters Based on RADIUS Attributes on page 23](#)
- [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.

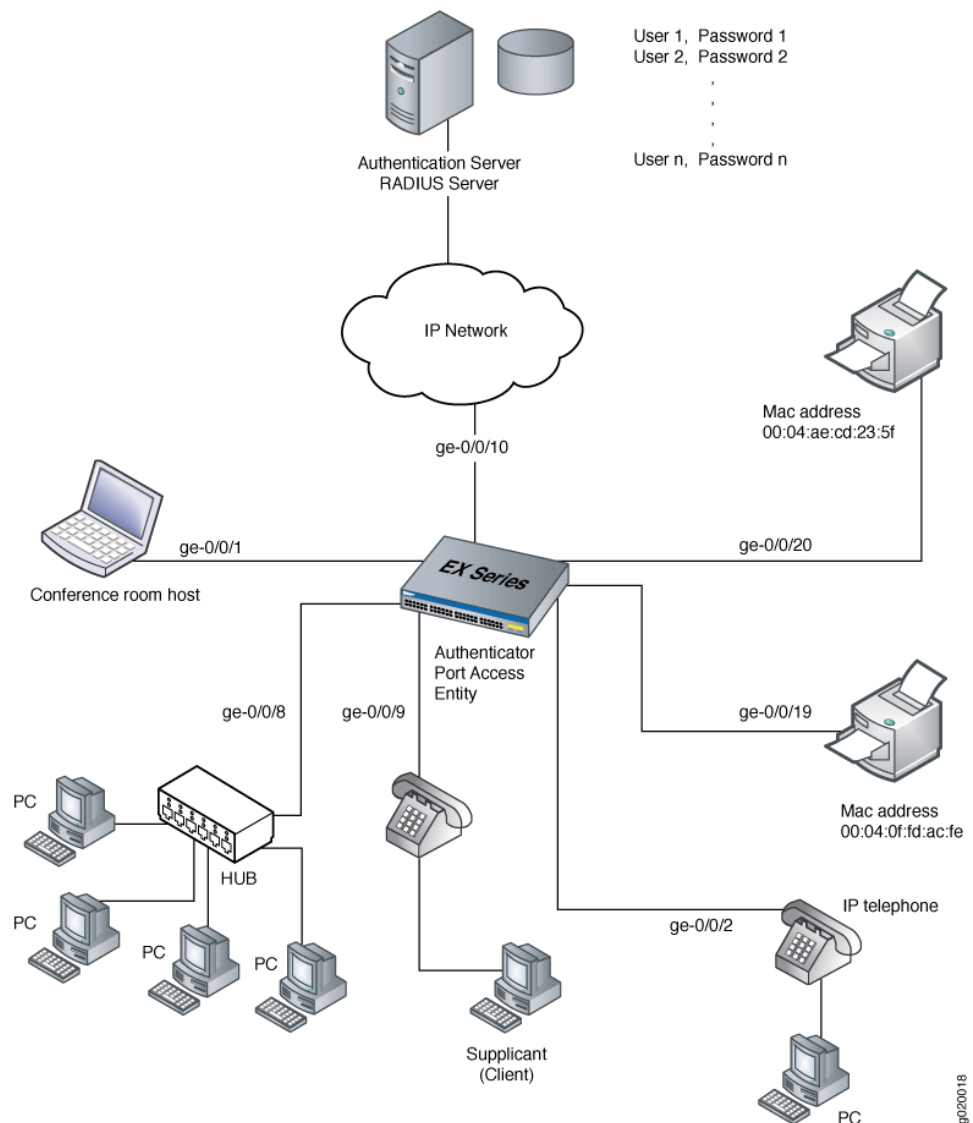
This topic covers:

- [Sample Authentication Topology on page 10](#)
- [802.1X Authentication on page 11](#)
- [MAC RADIUS Authentication on page 13](#)
- [Captive Portal Authentication on page 13](#)
- [Static MAC Bypass of Authentication on page 14](#)
- [Fallback of Authentication Methods on page 15](#)

Sample Authentication Topology

[Figure 1 on page 11](#) 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 126](#).

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 107](#) 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 29](#).

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 147](#).



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 7](#)
- [Authentication Process Flow for EX Series Switches on page 29](#)
- [Example: Setting Up 802.1X for Single-Suplicant or Multiple-Suplicant Configurations on an EX Series Switch on page 50](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 126](#)
- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 146](#)

- [Configuring Captive Portal Authentication \(CLI Procedure\) on page 151](#)
- [Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication \(CLI Procedure\) on page 149](#)
- [Controlling Authentication Session Timeouts \(CLI Procedure\) on page 155](#)

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 45](#)
- [Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 24](#)
- [Understanding Authentication on EX Series Switches on page 10](#)

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 16](#)
- [Supported RADIUS Attributes on page 17](#)

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 3 on page 18](#) list the RADIUS attributes supported for Accounting-Request packets.

Table 3: 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. <i>NOTE:</i> 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.
55	Event-Timestamp	Records the time an event occurred.

Related Documentation

- [802.1X for EX Series Switches Overview on page 7](#)
- [Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 130](#)

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 on page 56](#)
- [Configuring LLDP \(CLI Procedure\) on page 136](#)
- [Configuring LLDP-MED \(CLI Procedure\) on page 140](#)
- *Understanding PoE on EX Series Switches*

Understanding 802.1X and VoIP on EX Series Switches

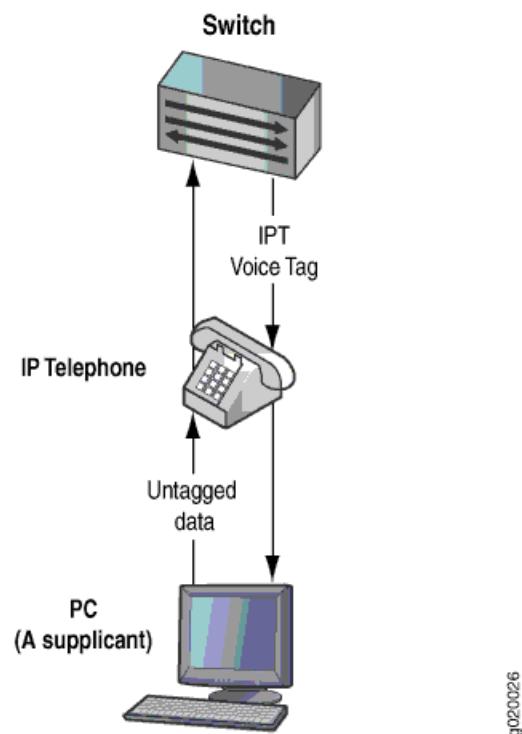
When you use VoIP, you can connect IP telephones to the switch and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. The 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.

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.

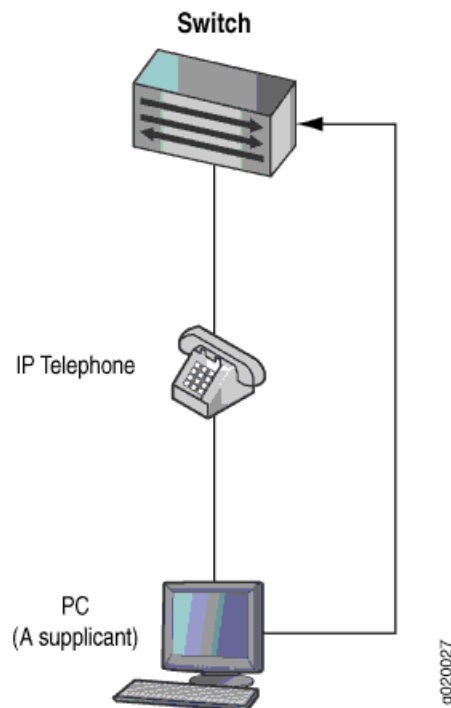
You can configure 802.1X authentication to work with VoIP in multiple supplicant or single supplicant mode. In *multiple supplicant* mode, the 802.1X process allows multiple supplicants to connect to the interface. Each supplicant is authenticated individually. For an example of a VoIP multiple supplicant topology, see [Figure 2 on page 22](#).

Figure 2: 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 3 on page 23](#).

Figure 3: 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 18](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56](#)
- [Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication on page 68](#)
- [Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 64](#)

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 10](#)
- [Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch on page 91](#)
- [Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 131](#)
- [Configuring Firewall Filters \(CLI Procedure\)](#)
- [Juniper-Switching-Filter VSA Match Conditions and Actions on page 142](#)

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 16](#)
- [Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 85](#)
- [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 45](#)

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 41](#).

- [Disconnect Messages on page 25](#)
- [Change of Authorization Messages on page 26](#)
- [Error-Cause Codes on page 26](#)

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 4 on page 27](#) for descriptions of error-cause codes that can be included in response messages sent from the NAS.

Table 4: 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.
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 23](#)
- [Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 24](#)

Understanding Server Fail Fallback and Authentication on EX Series Switches

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.

Juniper Networks EX Series 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.

A RADIUS server timeout occurs if no RADIUS authentication servers are reachable when an end device logs in and attempts to access the LAN. 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:

- *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.

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 that an end device be moved to a specified VLAN if the switch receives a RADIUS access-reject message. The configured VLAN name overrides any attributes sent by the server.

Related Documentation

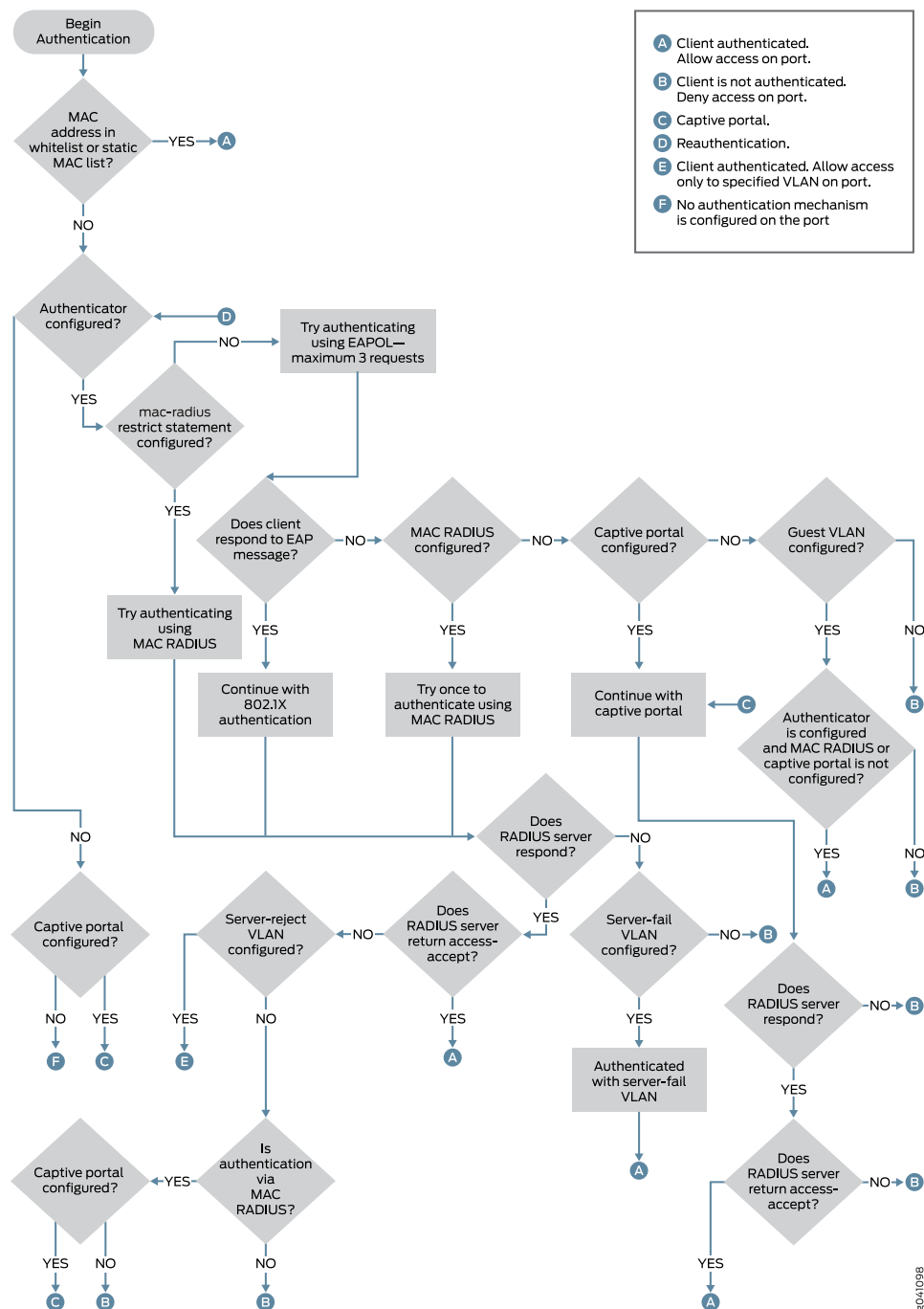
- [802.1X for EX Series Switches Overview on page 7](#)
- [Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 79](#)
- [Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 50](#)
- [Configuring RADIUS Server Fail Fallback \(CLI Procedure\) on page 144](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 126](#)

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 4 on page 30](#) illustrates the authentication process:

Figure 4: Authentication Process Flow for an EX Series Switch

**Related Documentation**

- [Understanding Authentication on EX Series Switches on page 10](#)
- [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 16](#)
- [Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 24](#)
- [Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102](#)

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 10](#)
- [Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 50](#)
- [Controlling Authentication Session Timeouts \(CLI Procedure\) on page 155](#)
- [Configuring MAC Table Aging \(CLI Procedure\)](#)

Understanding NetBIOS Snooping

NetBIOS snooping allows Juniper Networks EX Series Ethernet Switches to discover NetBIOS hosts that are connected to the switch.

- [What Is a NetBIOS Name? on page 32](#)
- [How NetBIOS Snooping Works on page 32](#)

What Is a NetBIOS Name?

A NetBIOS name is a key element in communications between NetBIOS resources. A NetBIOS name identifies a NetBIOS resource on the network. A NetBIOS name is either a unique (exclusive) name or a group (nonexclusive) name. When a NetBIOS resource communicates with one other NetBIOS resource, a unique name is used in that communication. When a NetBIOS resource communicates with multiple resources, a group name is used.

The NetBIOS name of each NetBIOS resource is stored on the NetBIOS Name Server (NBNS). The NetBIOS name of a NetBIOS resource is mapped to its IP address.

A NetBIOS name is a 16-byte address. The first 15 bytes contain the name and the last byte contains the name type.

The NetBIOS name service is supported over UDP port 137.

How NetBIOS Snooping Works

You can enable NetBIOS snooping on the switch so that the switch can identify NetBIOS resources that are connected to it.

When a host connected to the switch initializes itself, it attempts to register its NetBIOS name by sending a NetBIOS name registration request message. The host can opt for either a unique or a group NetBIOS name. For a unique NetBIOS name, the host either broadcasts a NetBIOS name query message on the local network or unicasts it to the NBNS to check whether the requested name is already being used by another host. If so, the host that previously registered the name or the NBNS responds with a negative name registration response. If the host receives no negative response, it broadcasts the NetBIOS name registration packet to confirm the name. For a NetBIOS group name, the host sends a NetBIOS name registration packet, which generates no responses from other hosts because multiple hosts can use the same group name at the same time.

The NetBIOS snooping-enabled switch extracts the host details from the NetBIOS name registration packet and stores the details in the LLDP neighbor database.

Related Documentation

- [Configuring NetBIOS Snooping \(CLI Procedure\) on page 156](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 18](#)

Understanding Centralized Network Access Control and EX Series Switches

Network access control (NAC) allows you to control who is admitted to the network and what resources—servers, applications, and stored data—those users are allowed to access. These controls include:

- Authentication—Pre-admission controls
- Authorization—Post-admission controls

You can use different methods to implement NAC on Juniper Networks EX Series Ethernet Switches.

This topic describes:

- [NAC Using Any RADIUS Server and Access Polices Defined on the Local Switch on page 33](#)
- [Centralized NAC Using Junos Pulse Access Control Service on page 33](#)
- [Captive Portal Authentication on page 34](#)

NAC Using Any RADIUS Server and Access Polices Defined on the Local Switch

For pre-admission controls, you can use the switch in combination with any RADIUS server as the *authentication server*. For additional information, see [“Understanding Authentication on EX Series Switches” on page 10](#).

For post-admission controls, you can configure firewall filters to limit access to specific resources. For additional information, see [Firewall Filters for EX Series Switches Overview](#).

Centralized NAC Using Junos Pulse Access Control Service

You can use Junos Pulse Access Control Service and the switches for a centralized end-to-end NAC system, including both pre-admission *authentication* and post-admission *authorization*.

When you configure such a system, the Juniper Networks MAG Series Junos Pulse Gateways or the Juniper Networks IC Series Unified Access Control Appliances NAC device functions as the authentication server. For messages relating to IEEE 802.1X and MAC RADIUS authentication, the NAC device communicates with the switch using the RADIUS protocol.

The Access Control Service also performs additional functions. It eliminates the need to configure firewall filters on each switch. Instead, you define resource access policies centrally on the NAC device. This centralized method is particularly helpful when you have multiple switches in your network.

The resource access policy on the Access Control Service defines which network resources are allowed and denied for a user, based upon the user's role. The NAC device distributes these policies to all connected switches. The NAC device thus functions as a centralized policy management server. For messages relating to access policies, the NAC device communicates with the switch using the Junos UAC Enforcer Protocol (JUEP). The switch

converts the resource access policies into filter definitions and applies these to the appropriate port.



NOTE: With this solution, the EX Series switch serves as an *Infranet Enforcer*, that is, a policy enforcement point for the Access Control Service. The Access Control Service sends auth table entries and resource access policies when an endpoint successfully completes 802.1X authentication or MAC authentication (unmanaged devices). Access for any endpoint is governed by the resource access policies that you configure on the Access Control Service. Because resource access policies are employed, firewall filters are not required for the switch configuration.

This integrated solution of Access Control Service and EX Series switches is easier to implement and much more efficient than previous versions of Access Control Service and the switches. As soon the switch connects to the MAG Series or IC Series NAC device, the Access Control Service pushes the role-based policies to the switch via JUEP. This enables the user to access the network more quickly than previous implementations, because the policy is already available on the switch and does not need to be pushed from the centralized device at the time of user authentication. Moreover, the policy push happens only once, which utilizes network bandwidth efficiently and makes this implementation suitable for scaled environments.

If you change policies, the Access Control Service automatically pushes the updated policies to the connected switch. The switch applies the policies dynamically without taking users through another authentication transaction.



NOTE: Do not configure firewall filters on the switch and do not use RADIUS server attributes for firewall filters if you are configuring the switch to use the Access Control Service. Instead, specify or deny access to resources by using the Access Control Service resource access policies.

You create policies on the NAC device's administrative interface to control access to resources and services. Access is based on successful authentication, the user's assigned role, and the security compliance of the endpoint device. For example, you can provide full access to protected resources employee role and limited access for a contractor role.

Captive Portal Authentication

Captive portal authentication allows you to authenticate users on the switches by redirecting Web browser requests to a login page that requires users to input a username and password before they are allowed access to the network. The details of configuring captive portal authentication differ depending on whether you are using the Access Control Service:

- If you have connected the switch to the Access Control Service, use the Access Control Service NAC device as an external captive portal server for redirecting Web browser requests. When users try to access a protected network resource that is connected to

the switch, the user must first sign in to the Access Control Service for authentication and endpoint security checking. The captive portal redirects the user to a login page located on the Access Control Service. When the sign-in page for the Access Control Service is displayed, the user signs in and the Access Control Service examines the endpoint for compliance with security policies. If the endpoint passes the security check, access is granted to the protected resource.

See [“Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service \(CLI Procedure\)”](#) on page 159. You can use the same Access Control Service as the external captive portal server for more than one switch.

- If you are not using the Access Control Service, you can use captive portal to redirect users to a login page that you configure on the local switch. See [“Designing a Captive Portal Authentication Login Page on an EX Series Switch”](#) on page 153 for information about designing a login page on your switch.

Related Documentation

- [Example: Configuring Centralized Access Control to Network Resources, with an EX Series Switch Connected to Junos Pulse Access Control Service](#) on page 111

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 35
- [Dynamic Firewall Filters for Central Web Authentication](#) on page 37
- [Redirect URL for Central Web Authentication](#) on page 37

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

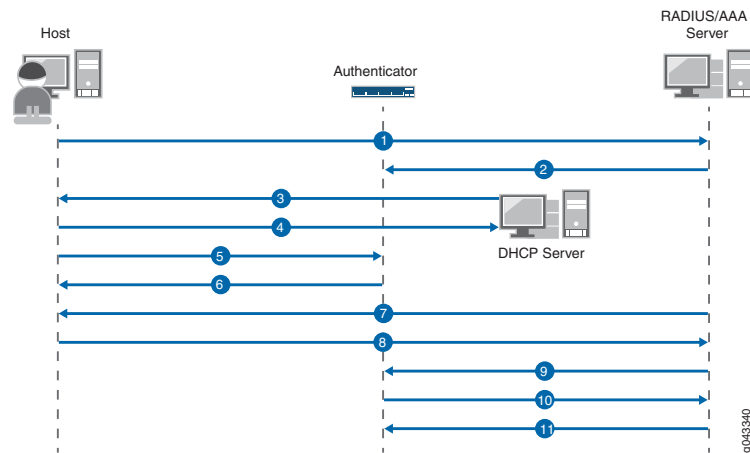
authentication. The switch applies the filter, which allows the host to receive an IP address, and uses the URL to redirect the host to the Web authentication page.

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 5 on page 37](#)):

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 5: 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 160](#).

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 160](#).

**Related
Documentation**

- [Understanding Dynamic Filters Based on RADIUS Attributes on page 23](#)
- [Understanding Dynamic VLAN Assignment Using RADIUS Attributes on page 24](#)
- [Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 131](#)

PART 2

Configuration

- [Configuration Examples on page 41](#)
- [Configuration Tasks on page 125](#)
- [Configuration Statements on page 165](#)

CHAPTER 3

Configuration Examples

- [Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41](#)
- [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 45](#)
- [Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 50](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56](#)
- [Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 64](#)
- [Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication on page 68](#)
- [Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 75](#)
- [Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 79](#)
- [Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 85](#)
- [Example: Applying a Firewall Filter to 802.1X-Authenticated Suplicants by Using RADIUS Server Attributes on an EX Series Switch on page 91](#)
- [Example: Applying Firewall Filters to Multiple Suplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on page 97](#)
- [Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102](#)
- [Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 107](#)
- [Example: Configuring Centralized Access Control to Network Resources, with an EX Series Switch Connected to Junos Pulse Access Control Service on page 111](#)

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 42](#)
- [Overview and Topology on page 42](#)
- [Configuration on page 44](#)
- [Verification on page 45](#)

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 6 on page 43](#) shows one EX4200 switch that is connected to the devices listed in [Table 5 on page 43](#).

Figure 6: Topology for Configuration

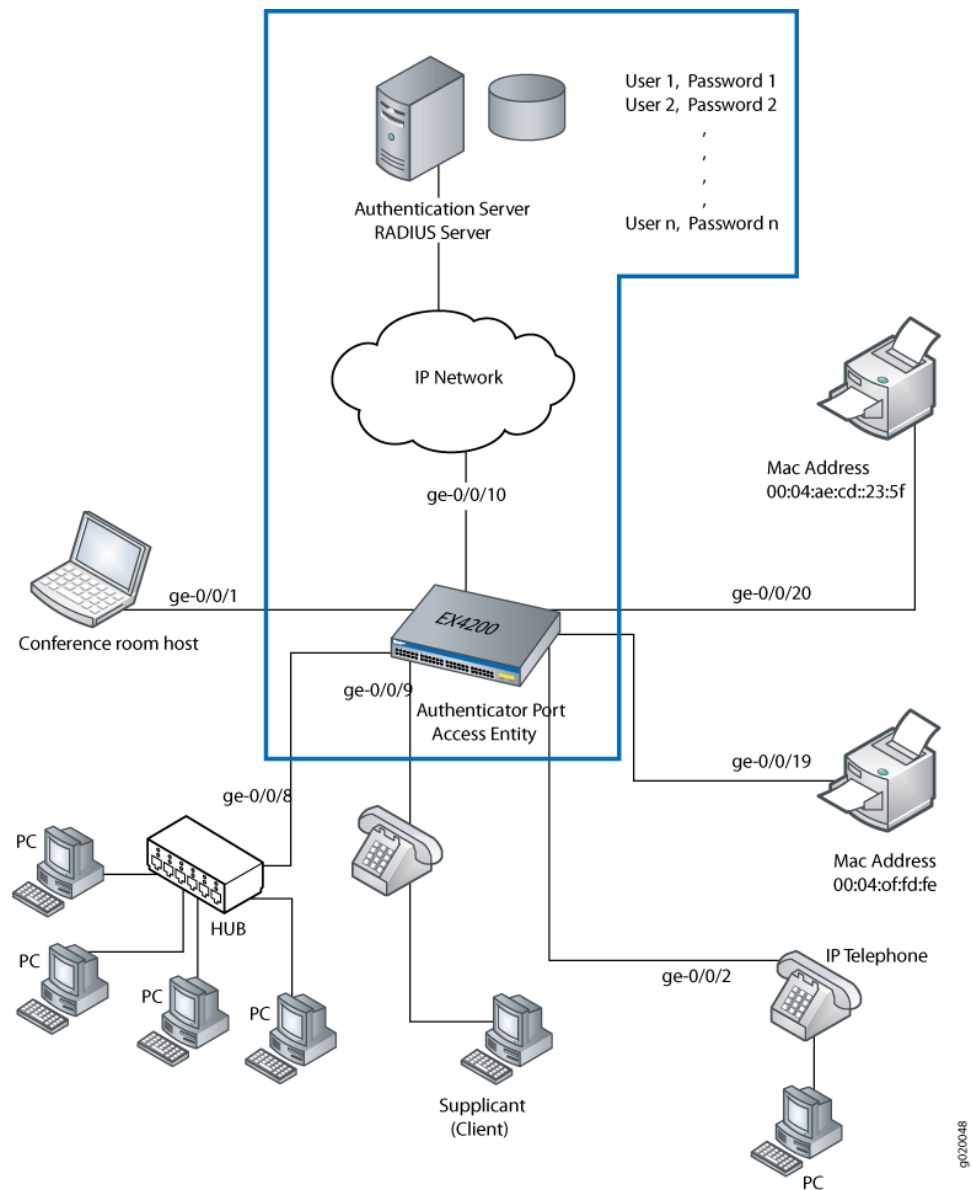


Table 5: Components of the Topology

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

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



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

Configuration

CLI Quick Configuration

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

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

Step-by-Step Procedure

To connect the RADIUS server to the switch:

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


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


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


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

Results

Display the results of the configuration:

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

Verification

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

- [Verify That the Switch and RADIUS Server Are Properly Connected on page 45](#)

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 50 • Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 45 • Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56 • Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 130 • Filtering 802.1X Suplicants by Using RADIUS Server Attributes on page 131

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 46](#)
- [Overview and Topology on page 46](#)
- [Configuration of a Guest VLAN That Includes 802.1X Authentication on page 48](#)
- [Verification on page 48](#)

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 7 on page 47](#) shows the conference room connected to the switch at interface ge-0/0/1.

Figure 7: Topology for Guest VLAN Example

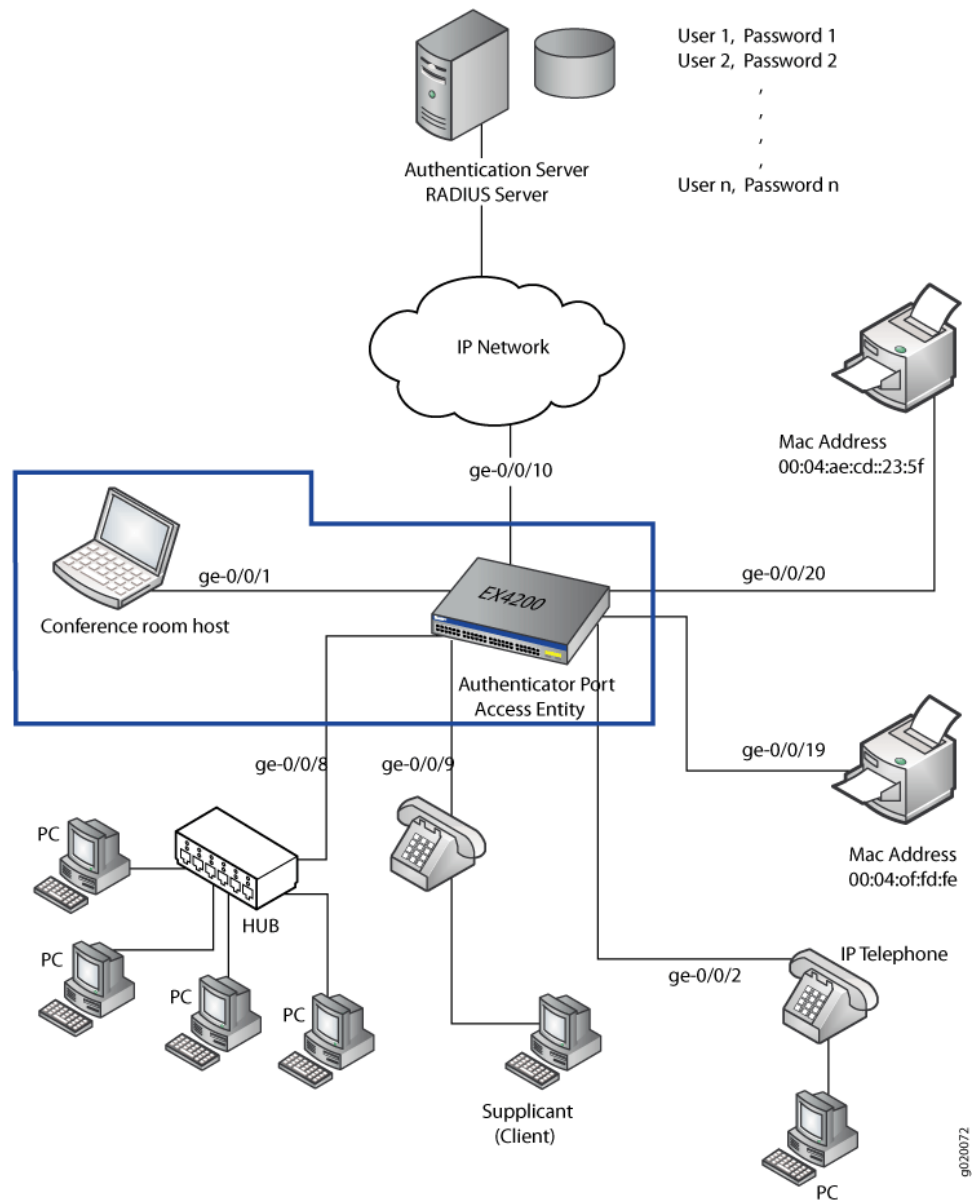


Table 6: Components of the Guest VLAN Topology

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 48](#)

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 41](#)
- [Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 50](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 126](#)

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 (suppliant) 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 suppliant 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 50](#)
- [Overview and Topology on page 51](#)
- [Configuration of 802.1X to Support Multiple Suppliant Modes on page 53](#)
- [Verification on page 54](#)

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 (suplicants) 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 8 on page 52](#), 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 8: Topology for Configuring Supplicant Modes

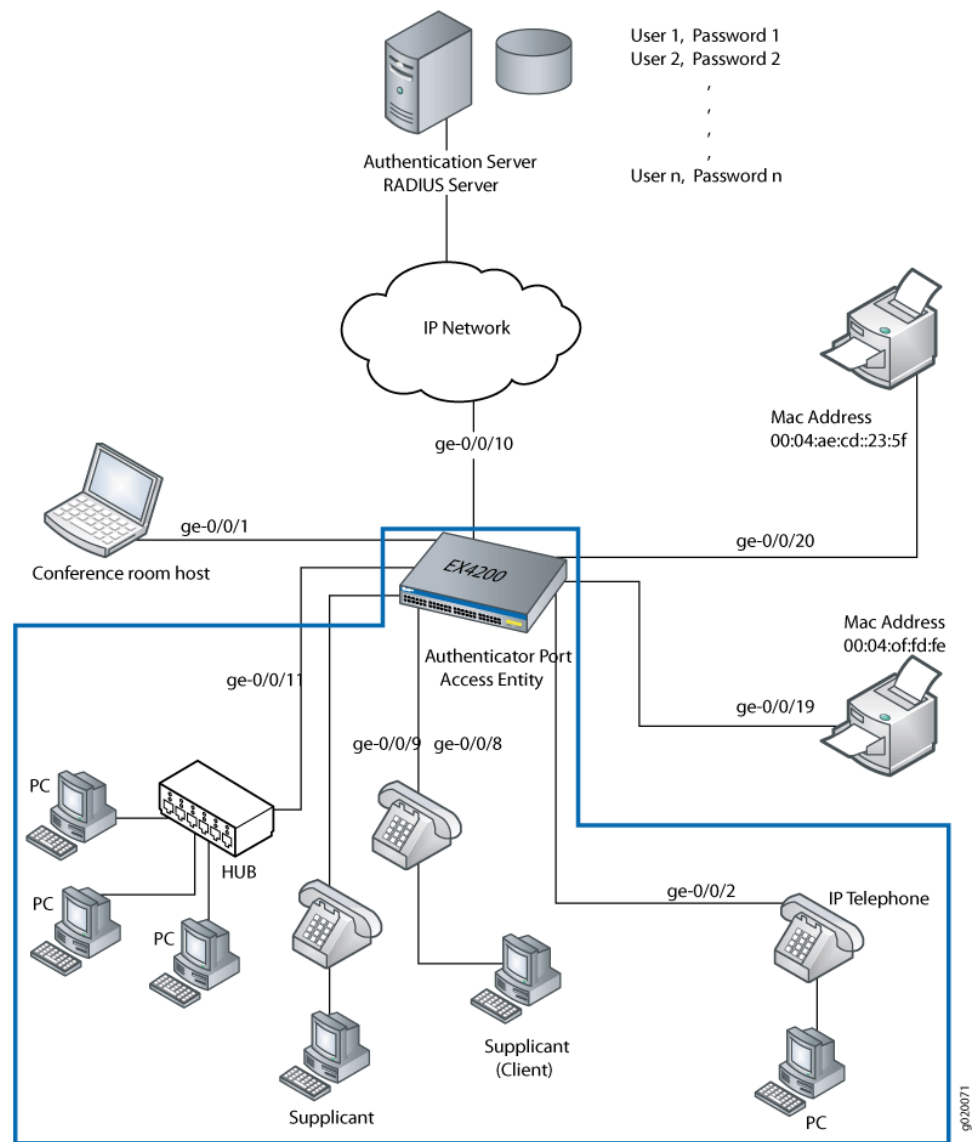


Table 7: Components of the Supplicant Mode Configuration Topology

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

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

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

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

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

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

Configuration of 802.1X to Support Multiple Supplicant Modes

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

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

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

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

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

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

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

Results

Check the results of the configuration:

```
[edit]
user@access-switch> show configuration
protocols {
  dot1x {
    authenticator {
      interface {
        ge-0/0/8.0 {
```

```
        supplicant single;  
    )  
    ge-0/0/9.0 {  
        supplicant single-secure;  
    }  
    ge-0/0/11.0 {  
        supplicant multiple;  
    }  
}  
}  
}
```

Verification

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

- [Verifying the 802.1X Configuration on page 54](#)

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 155](#)
- [Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41](#)
- [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 45](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 130](#)
- [Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 131](#)
- [Understanding Authentication on EX Series Switches on page 10](#)

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch

You can configure voice over IP (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 the LLDP-MED protocol and 802.1X authentication:

- [Requirements on page 56](#)
- [Overview and Topology on page 57](#)
- [Configuration on page 59](#)
- [Verification on page 61](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An Avaya 9620 IP telephone that supports LLDP-MED and 802.1X

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See *Installing and Connecting an EX3200 Switch*.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (J-Web 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 41](#).
- (Optional) Configured interface **ge-0/0/2** for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see *Configuring PoE on EX Series Switches (CLI Procedure)*.



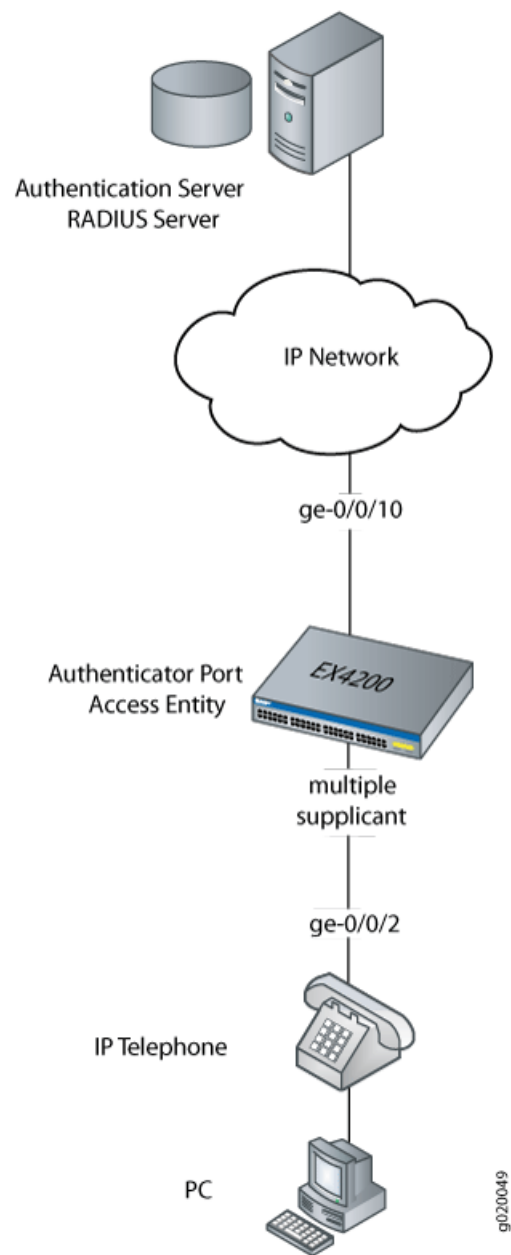
NOTE: If the IP address isn't configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the **voip** statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN 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 EX4200 switch is connected to an Avaya 9620 IP telephone. Avaya phones have a built-in bridge that allows you to connect a desktop PC to the phone, so the desktop and phone in a single office require only one interface on the switch. The EX Series switch is connected to a RADIUS server on interface **ge-0/0/10** (see [Figure 9 on page 58](#)).

Figure 9: 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 8 on page 58](#) describes the components used in this VoIP configuration example.

Table 8: Components of the VoIP Configuration Topology

Property	Settings
Switch hardware	EX4200 switch

Table 8: Components of the VoIP Configuration Topology (*continued*)

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

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

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



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

Configuration

To configure VoIP, LLDP-MED, and 802.1X authentication:

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 interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set ethernet-switching-options voip interface ge-0/0/2.0 vlan voice-vlan
set ethernet-switching-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2.0
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 interface ge-0/0/2.0
```

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


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


```
[edit ethernet-switching-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-0/0/2.0
```
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 {
        port-mode access;
        vlan {
          members data-vlan;
        }
      }
    }
  }
}
protocols {
  lldp-med {
    interface ge-0/0/2.0;
  }
  dot1x {
    authenticator {
      interface {
        ge-0/0/2.0 {
          supplicant multiple;
        }
      }
    }
  }
}
```

```
}
vpls {
  data-vlan {
    vlan-id 77;
    interface {
      ge-0/0/2.0;
    }
  }
  voice-vlan {
    vlan-id 99;
  }
}
ethernet-switching 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 61](#)
- [Verifying 802.1X Authentication for IP Phone and Desktop PC on page 62](#)
- [Verifying the VLAN Association with the Interface on page 63](#)

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 Second(s)
Transmit delay : 2 Second(s)
Hold timer : 2 Second(s)
Config Trap Interval : 300 Second(s)
Connection Hold timer : 60 Second(s)

LLDP MED : Enabled
MED fast start count : 3 Packet(s)
```

Interface	LLDP	LLDP-MED	Neighbor count
all	Enabled	-	0
ge-0/0/2.0	-	Enabled	0

Interface	VLAN-id	VLAN-name
ge-0/0/0.0	0	default
ge-0/0/1.0	0	employee-vlan
ge-0/0/2.0	0	data-vlan
ge-0/0/2.0	99	voice-vlan
ge-0/0/3.0	0	employee-vlan
ge-0/0/8.0	0	employee-vlan
ge-0/0/10.0	0	default
ge-0/0/11.0	20	employee-vlan
ge-0/0/23.0	0	default

LLDP basic TLVs supported:

Chassis identifier, Port identifier, Port description, System name, System description, System capabilities, Management address.

LLDP 802 TLVs supported:

Power via MDI, Link aggregation, Maximum frame size, Port VLAN tag, Port VLAN name.

LLDP MED TLVs supported:

LLDP MED capabilities, Network policy, Endpoint location, Extended power Via MDI.

Meaning The **show lldp detail** output shows that both LLDP and LLDP-MED are configured on the **ge-0/0/2.0** interface. The end of the output shows the list of supported LLDP basic TLVs, 802.3 TLVs, and LLDP-MED TLVs that are supported.

Verifying 802.1X Authentication for IP Phone and Desktop PC

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

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

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

Verifying the VLAN Association with the Interface

Purpose Display the interface state and VLAN membership.

Action user@switch> `show ethernet-switching interfaces`
 Ethernet-switching table: 0 entries, 0 learned

user@switch> `show ethernet-switching interfaces`

Interface	State	VLAN members	Blocking
ge-0/0/0.0	down	default	unblocked
ge-0/0/1.0	down	employee-vlan	unblocked
ge-0/0/5.0	down	employee-vlan	unblocked
ge-0/0/3.0	down	employee-vlan	unblocked
ge-0/0/8.0	down	employee-vlan	unblocked
ge-0/0/10.0	down	default	unblocked
ge-0/0/11.0	down	employee-vlan	unblocked
ge-0/0/23.0	down	default	unblocked
ge-0/0/2.0	up	voice-vlan	unblocked
		data-vlan	unblocked

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

Related Documentation • [Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41](#)

- [Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 50](#)
- [Defining CoS Forwarding Classes \(CLI Procedure\)](#)
- [Defining CoS Forwarding Classes \(J-Web Procedure\)](#)
- [Configuring LLDP-MED \(CLI Procedure\) on page 140](#)

Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol is sometimes used with IP phones to forward VoIP parameters from the switch to the phone. However, not all IP phones support LLDP-MED.

This example describes how to configure VoIP on an EX Series switch without using LLDP-MED:

- [Requirements on page 64](#)
- [Overview on page 65](#)
- [Configuring VoIP Without LLDP-MED by Using a Voice VLAN on an Access Port on page 65](#)
- [Configuring VoIP Without LLDP-MED by Using a Trunk Port with Native VLAN Option on page 67](#)
- [Verification on page 68](#)

Requirements

This example uses the following hardware and software components:

- One EX4200 switch acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An IP phone that does not support LLDP-MED.
- Junos OS Release 9.1 or later for EX Series switches.

Before you configure VoIP, 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*.
- Configured the IP phone as a member of the voice VLAN.
- (Optional) Configured interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. See *Configuring PoE on EX Series Switches (CLI Procedure)*.

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 can also power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

EX Series switches can accommodate an IP telephone and end host connected to a single switch port. In such a scenario, voice and data traffic must be separated into different broadcast domains, or VLANs. One method for accomplishing this is by configuring a voice VLAN, which enables access ports to accept untagged data traffic as well as tagged voice traffic from IP phones, and associate each type of traffic with separate and distinct VLANs. Voice traffic (tagged) can then be treated differently, generally with a higher priority than data traffic (untagged).

The voice VLAN delivers the greatest benefit when used with IP phones that support LLDP-MED, but it is flexible enough that IP phones that do not support LLDP-MED can also use it effectively. However, in the absence of LLDP-MED, the voice VLAN ID must be set manually on the IP phone because LLDP-MED is not available to accomplish this dynamically. For information about setting up a voice VLAN for IP phones that support LLDP-MED, see [“Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch” on page 56](#).

Another method to separate voice (tagged) and data (untagged) traffic into different VLANs is to use a trunk port with the native VLAN ID option. The trunk port is added as a member of the voice VLAN, and processes only tagged voice traffic from that VLAN. The trunk port must also be configured with the native VLAN ID for the data VLAN so that it can process untagged data traffic from the data VLAN. This configuration also requires that the voice VLAN ID be set manually on the IP phone.

This example illustrates both methods. In this example, the interface ge-0/0/2 on the EX4200 switch is connected to a non-LLDP-MED IP phone.



NOTE: 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.

Configuring VoIP Without LLDP-MED by Using a Voice VLAN on an Access Port

CLI Quick Configuration	<p>To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:</p> <pre>[edit] set vlans data-vlan vlan-id 77 set vlans voice-vlan vlan-id 99 set vlans data-vlan interface ge-0/0/2.0 set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan</pre>
--------------------------------	---

```
set ethernet-switching-options voip interface ge-0/0/2.0 vlan voice-vlan
set ethernet-switching-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

Step-by-Step Procedure

1. Configure two VLANs: one for data traffic and one for voice traffic:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```



NOTE: The voice VLAN ID must be set manually on the IP phone.

2. Configure the VLAN **data-vlan** on the interface ge-0/0/2:

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

3. Configure the interface ge-0/0/2 as an access port belonging to the data VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode access
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan member data-vlan
```

4. Configure VoIP on the interface ge-0/0/2 and add this interface to the voice VLAN:

```
[edit ethernet-switching-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
```

5. Specify the assured-forwarding forwarding class to provide the most dependable class of service:

```
[edit ethernet-switching-options]
user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

Results Display the results of the configuration:

```
[edit]
user@switch> show configuration
interfaces {
  ge-0/0/2 {
    unit 0 {
      family ethernet-switching {
        port-mode access;
        vlan {
          members data-vlan;
        }
      }
    }
  }
}
vlans {
  data-vlan {
    vlan-id 77;
    interface {
      ge-0/0/2.0;
    }
  }
  voice-vlan {
    vlan-id 99;
  }
}
```

```

}
ethernet-switching options {
  voip {
    interface ge-0/0/2.0 {
      vlan voice-vlan;
      forwarding-class assured-forwarding;
    }
  }
}

```

Configuring VoIP Without LLDP-MED by Using a Trunk Port with Native VLAN Option

CLI Quick Configuration To quickly configure VoIP, 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 interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members voice-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan

```

Step-by-Step Procedure 1. Configure two VLANs: one for data traffic and one for voice traffic:

```

[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99

```



NOTE: The voice VLAN ID must be set manually on the IP phone.

2. Configure interface ge-0/0/2 as a trunk port that includes only the voice VLAN:

```

[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode trunk
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan member voice-vlan

```

3. Configure the native VLAN ID for the data VLAN on the trunk port:

```

[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan

```

Results Display the results of the configuration:

```

[edit]
user@switch> show configuration
interfaces {
  ge-0/0/2 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members voice-vlan;
        }
        native-vlan-id data-vlan;
      }
    }
  }
}

```

```

}
vlans {
  data-vlan {
    vlan-id 77;
  }
  voice-vlan {
    vlan-id 99;
  }
}

```

Verification

To confirm that the configuration is working properly, perform the following task:

- [Verifying the VLAN Association With the Interface on page 68](#)

Verifying the VLAN Association With the Interface

Purpose Display the interface state and VLAN membership.

Action user@switch> [show ethernet-switching interfaces](#)
Ethernet-switching table: 0 entries, 0 learned

```

user@switch> show ethernet-switching interfaces
Interface  State  VLAN members  Blocking
ge-0/0/0.0 down  default       unblocked
ge-0/0/1.0 down  employee-vlan unblocked
ge-0/0/5.0 down  employee-vlan unblocked
ge-0/0/3.0 down  employee-vlan unblocked
ge-0/0/8.0 down  employee-vlan unblocked
ge-0/0/10.0 down default       unblocked
ge-0/0/11.0 down employee-vlan unblocked
ge-0/0/23.0 down default       unblocked
ge-0/0/2.0 up    voice-vlan    unblocked
              data-vlan    unblocked

```

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

- Related Documentation**
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56](#)
 - [Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication on page 68](#)
 - [Understanding 802.1X and VoIP on EX Series Switches on page 21](#)
 - [Understanding LLDP and LLDP-MED on EX Series Switches on page 18](#)

Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication

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 using static MAC bypass of authentication:

- [Requirements on page 69](#)
- [Overview on page 70](#)
- [Configuration on page 70](#)
- [Verification on page 72](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches
- An 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 41](#).
- (Optional) Configured interface **ge-0/0/2** for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see *Configuring PoE on EX Series Switches (CLI Procedure)*.



NOTE: If the IP address isn't 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 EX4200 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

To configure VoIP without 802.1X authentication:

CLI Quick Configuration

To quickly configure VoIP, 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 interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set ethernet-switching-options voip interface ge-0/0/2.0 vlan voice-vlan
set ethernet-switching-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2.0
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:

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 interface ge-0/0/2.0
```
3. Configure the interface as an access interface, configure support for Ethernet switching, and add the **data-vlan** VLAN:

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

```
[edit ethernet-switching-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-0/0/2.0
```
6. Set the authentication profile (see [“Configuring 802.1X Interface Settings \(CLI Procedure\)” on page 126](#) and [“Configuring 802.1X RADIUS Accounting \(CLI Procedure\)” on page 130](#)):
 

```
[edit protocols]
set dot1x authenticator authentication-profile-name auth-profile
```
  7. Add the MAC address of the phone to the static MAC bypass list:
 

```
[edit protocols]
set dot1x authenticator static 00:04:f2:11:aa:a7
```
  8. Set the supplicant mode to multiple:
 

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

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

```
[edit]
user@switch# show configuration
interfaces {
 ge-0/0/2 {
 unit 0 {
 family ethernet-switching {
 port-mode access;
 vlan {
 members data-vlan;
 }
 }
 }
 }
}
protocols {
 lldp-med {
 interface ge-0/0/2.0;
 }
 dot1x {
 authenticator {
 authentication-profile-name auth-profile;
 static {
 00:04:f2:11:aa:a7;
 }
 }
 interface {
 ge-0/0/2.0 {
 supplicant multiple;
 }
 }
 }
}
vlangs {
 data-vlan {
 vlan-id 77;
 interface {
 ge-0/0/2.0;
 }
 }
}
```

```
 }
 voice-vlan {
 vlan-id 99;
 }
}
ethernet-switching 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 72](#)
- [Verifying Authentication for the Desktop PC on page 73](#)
- [Verifying the VLAN Association with the Interface on page 74](#)

### 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 Second(s)
Transmit delay : 2 Second(s)
Hold timer : 2 Second(s)
Config Trap Interval : 300 Second(s)
Connection Hold timer : 60 Second(s)

LLDP MED : Enabled
MED fast start count : 3 Packet(s)

```

| Interface  | LLDP    | LLDP-MED | Neighbor count |
|------------|---------|----------|----------------|
| all        | Enabled | -        | 0              |
| ge-0/0/2.0 | -       | Enabled  | 0              |

| Interface   | VLAN-id | VLAN-name     |
|-------------|---------|---------------|
| ge-0/0/0.0  | 0       | default       |
| ge-0/0/1.0  | 0       | employee-vlan |
| ge-0/0/2.0  | 0       | data-vlan     |
| ge-0/0/2.0  | 99      | voice-vlan    |
| ge-0/0/3.0  | 0       | employee-vlan |
| ge-0/0/8.0  | 0       | employee-vlan |
| ge-0/0/10.0 | 0       | default       |
| ge-0/0/11.0 | 20      | employee-vlan |
| ge-0/0/23.0 | 0       | default       |

LLDP basic TLVs supported:

Chassis identifier, Port identifier, Port description, System name, System description, System capabilities, Management address.

LLDP 802 TLVs supported:

Power via MDI, Link aggregation, Maximum frame size, Port VLAN tag, Port VLAN name.

LLDP MED TLVs supported:

LLDP MED capabilities, Network policy, Endpoint location, Extended power Via MDI.

**Meaning** The `show lldp detail` output shows that both LLDP and LLDP-MED are configured on the `ge-0/0/2.0` interface. The end of the output shows the list of supported LLDP basic TLVs, 802.3 TLVs, and LLDP-MED TLVs that are supported.

### Verifying Authentication for the Desktop PC

**Purpose** Display the 802.1X configuration for the desktop PC connected to the VoIP interface through the IP phone.

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

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

---

### Verifying the VLAN Association with the Interface

---

**Purpose** Display the interface state and VLAN membership.

**Action** user@switch> `show ethernet-switching interfaces`  
Ethernet-switching table: 0 entries, 0 learned

user@switch> `show ethernet-switching interfaces`

| Interface   | State | VLAN members  | Blocking  |
|-------------|-------|---------------|-----------|
| ge-0/0/0.0  | down  | default       | unblocked |
| ge-0/0/1.0  | down  | employee-vlan | unblocked |
| ge-0/0/5.0  | down  | employee-vlan | unblocked |
| ge-0/0/3.0  | down  | employee-vlan | unblocked |
| ge-0/0/8.0  | down  | employee-vlan | unblocked |
| ge-0/0/10.0 | down  | default       | unblocked |
| ge-0/0/11.0 | down  | employee-vlan | unblocked |
| ge-0/0/23.0 | down  | default       | unblocked |
| ge-0/0/2.0  | up    | voice-vlan    | unblocked |
|             |       | data-vlan     | unblocked |

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

**Related Documentation**

- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56](#)

- [Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 64](#)
- [Understanding 802.1X and VoIP on EX Series Switches on page 21](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 18](#)

## 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 75](#)
- [Overview and Topology on page 76](#)
- [Configuration on page 77](#)
- [Verification on page 78](#)

### 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:

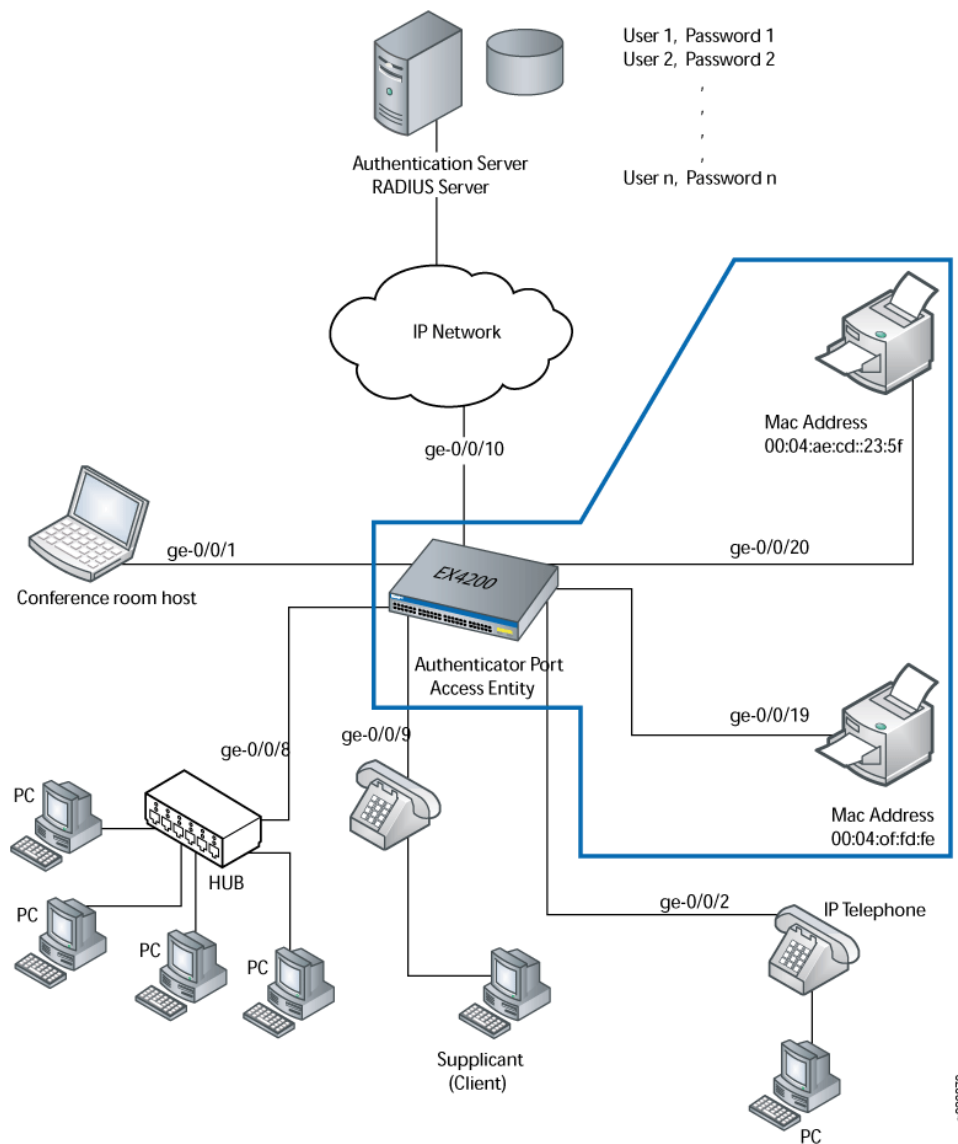
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN 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 41](#).

## 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 10 on page 76 shows the two printers connected to the EX4200.

Figure 10: Topology for Static MAC Bypass of Authentication Configuration



The interfaces shown in Table 9 on page 77 will be configured for static MAC bypass of authentication.

Table 9: 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                                                                                          |
| Connections to integrated printer/fax/copier machines (no PoE required) | ge-0/0/19, MAC address 00:04:0f:fd:ac:fe<br>ge-0/0/20, MAC address 00:04:ae:cd:23:5f             |

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

## Configuration

**CLI Quick Configuration** To quickly configure 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 78](#)

### 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 \(J-Web Procedure\) on page 127](#)
  - [Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication \(CLI Procedure\) on page 149](#)
  - [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 126](#)
  - [Understanding Authentication on EX Series Switches on page 10](#)

## 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 79](#)
- [Overview and Topology on page 80](#)
- [Configuration on page 82](#)
- [Verification on page 82](#)

### 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 41.
- 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 11 on page 81](#) 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 11: Topology for Configuring 802.1X Options

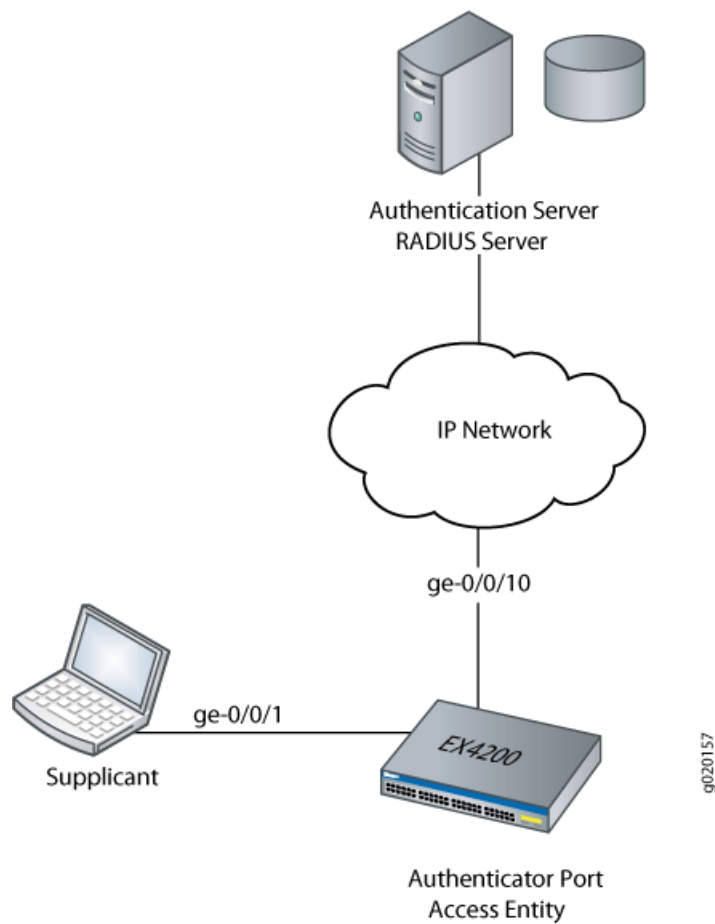


Table 10 on page 81 describes the components in this topology.

Table 10: 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        | <b>default</b> VLAN<br><b>vlan-sf</b> VLAN                                                             |
| Supplicant        | Supplicant attempting access on interface <b>ge-0/0/1</b>                                              |
| One RADIUS server | Backend database with an address of <b>10.0.0.100</b> connected to the switch at port <b>ge-0/0/10</b> |

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 83](#)

### 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 50](#)
- [Configuring RADIUS Server Fail Fallback \(CLI Procedure\) on page 144](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 130](#)
- [Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 131](#)
- [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 85](#)
- [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 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 41](#).

- 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 126](#).

## 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 12 on page 87](#) shows the two printers connected to the switch.

Figure 12: Topology for MAC RADIUS Authentication Configuration

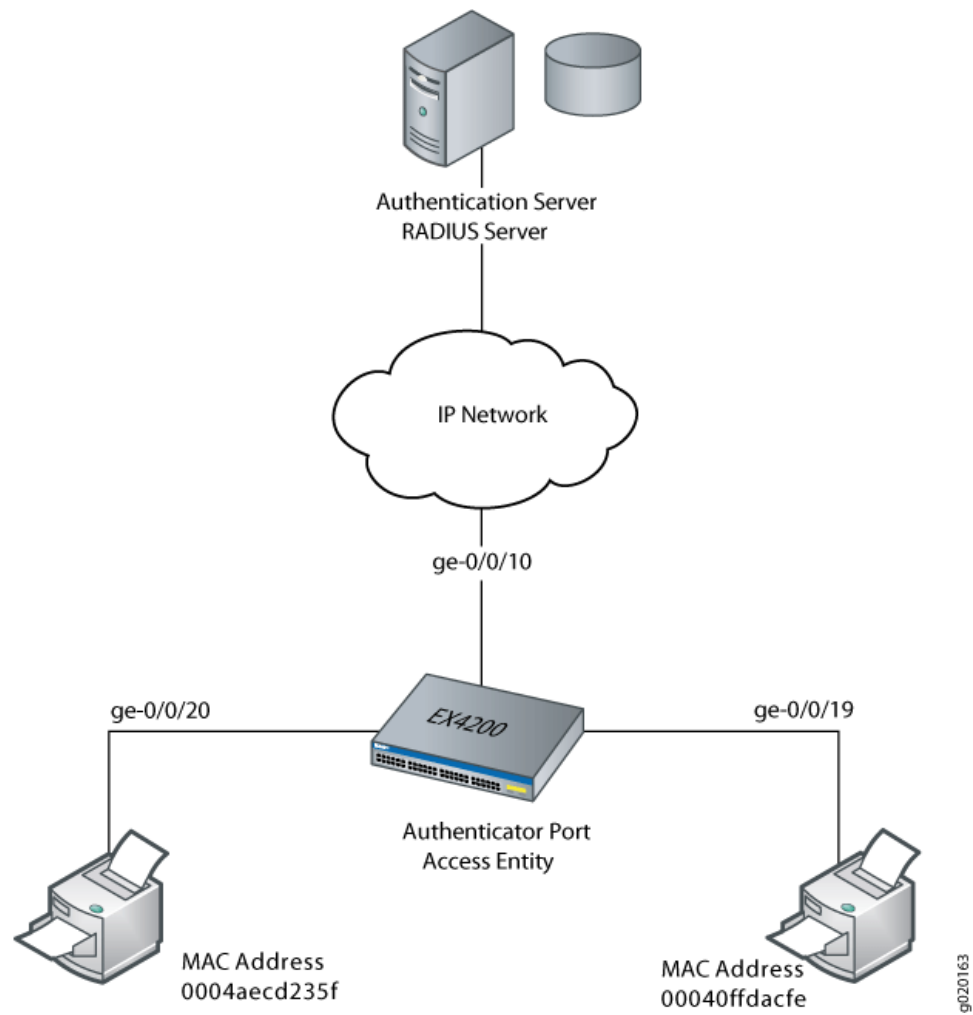


Table 11 on page 87 shows the components in the example for MAC RADIUS authentication.

Table 11: 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<br>ge-0/0/20, MAC address 0004aec235f |
| RADIUS server                             | Connected to the switch on interface <b>ge-0/0/10</b>                     |

The printer with the MAC address 00040ffdacfe is connected to access interface ge-0/0/19. A second printer with the MAC address 0004aec235f 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 0004aec235f as usernames and passwords:

```
[root@freeradius]#
edit /etc/raddb
vi users
00040ffdacfe Auth-type:=EAP, User-Password = "00040ffdacfe"
0004aec235f Auth-type:=EAP, User-Password = "0004aec235f"
```

**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 89](#)

### 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 146](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 126](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\) on page 127](#)
- [Understanding Authentication on EX Series Switches on page 10](#)

## 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 91](#)
- [Overview and Topology on page 92](#)
- [Configuring the Port Firewall Filter and Counters on page 94](#)
- [Applying the Port Firewall Filter to the Supplicant User Profiles on the RADIUS Server on page 95](#)
- [Verification on page 96](#)

## 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 41.
- 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 126 and [“Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch”](#) on page 50.
- 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 13 on page 93 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 13: Topology for Firewall Filter and RADIUS Server Attributes Configuration**

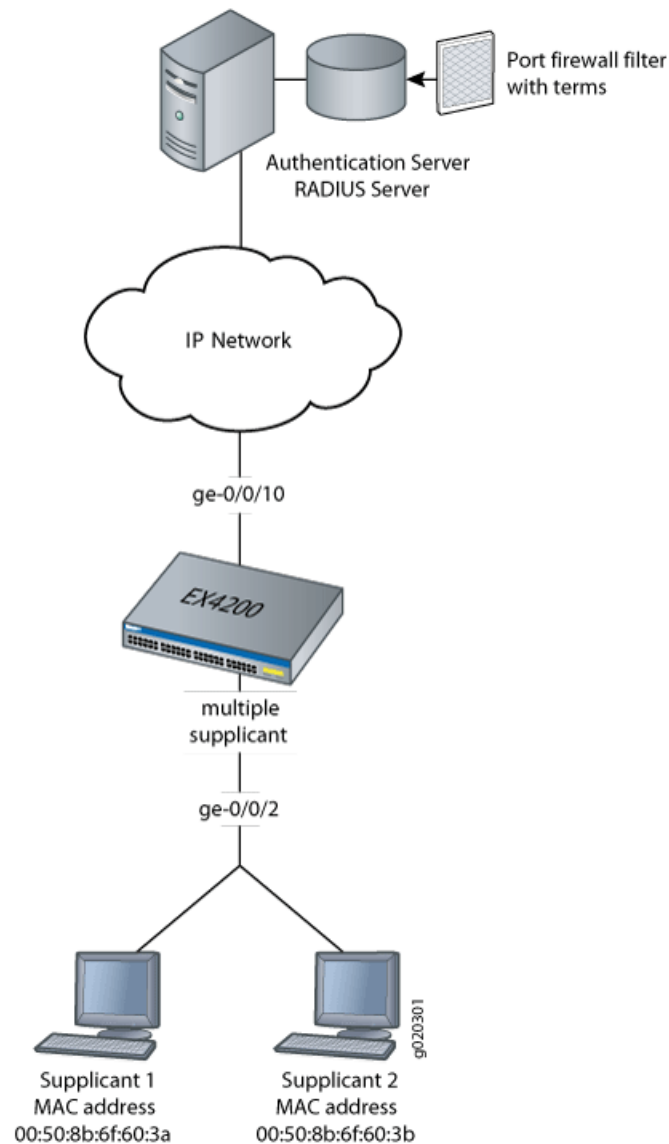


Table 12 on page 93 describes the components in this topology.

**Table 12: 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. |

Table 12: Components of the Firewall Filter and RADIUS Server Attributes Topology (*continued*)

| Property                                                                | Settings                                                                                                                                                                                   |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| One RADIUS server                                                       | Backend database with the address 10.0.0.100 connected to the switch at port <b>ge-0/0/10</b> .                                                                                            |
| 802.1X supplicants connected to the switch on interface <b>ge-0/0/2</b> | <ul style="list-style-type: none"> <li>• <b>Supplicant 1</b> has MAC address <b>00:50:8b:6f:60:3a</b>.</li> <li>• <b>Supplicant 2</b> has MAC address <b>00:50:8b:6f:60:3b</b>.</li> </ul> |
| Port firewall filter to be applied on the RADIUS server                 | <b>filter1</b>                                                                                                                                                                             |
| Counters                                                                | <b>counter1</b> counts packets from Supplicant 1, and <b>counter2</b> counts packets from Supplicant 2.                                                                                    |
| Policer                                                                 | <b>policer p1</b>                                                                                                                                                                          |
| User profiles on the RADIUS server                                      | <ul style="list-style-type: none"> <li>• Supplicant 1 has the user profile <b>supplicant1</b>.</li> <li>• Supplicant 2 has the user profile <b>supplicant2</b>.</li> </ul>                 |

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-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 50](#)
  - [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches](#)
  - [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 130](#)
  - [Understanding Authentication on EX Series Switches on page 10](#)
  - [Understanding Dynamic Filters Based on RADIUS Attributes on page 23](#)

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

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 98](#)
- [Overview and Topology on page 98](#)
- [Configuration on page 100](#)
- [Verification on page 102](#)

## Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.5 or later for EX Series switches
- One EX Series switch
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

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

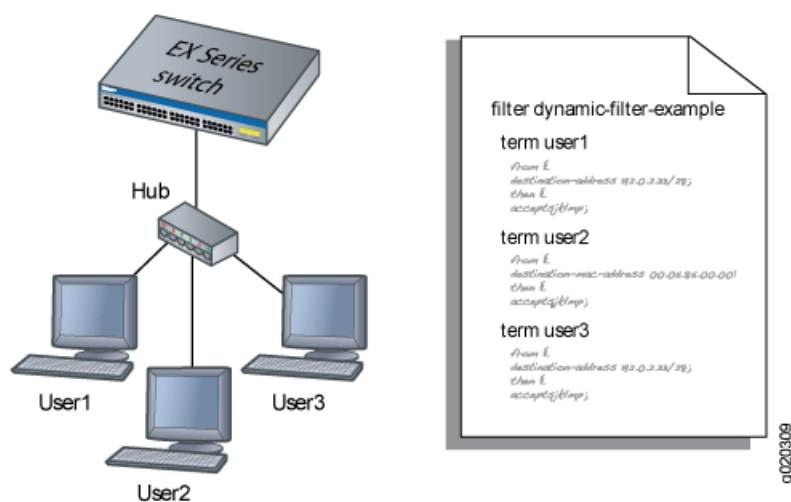
- Set up a connection between the switch and the RADIUS server. See [“Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch”](#) on page 41.
- Configured 802.1X authentication on the switch, with the authentication mode for interface **ge-0/0/2** set to **multiple**. See [“Configuring 802.1X Interface Settings \(CLI Procedure\)”](#) on page 126 and [“Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch”](#) on page 50.
- 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 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 14 on page 99](#), when User1 is authenticated by the EX Series switch, the system creates the firewall filter **dynamic-filter-example**. When User2 is authenticated, another term is added to the firewall filter, and so on.

Figure 14: Conceptual Model: Dynamic Filter Updated for Each New User



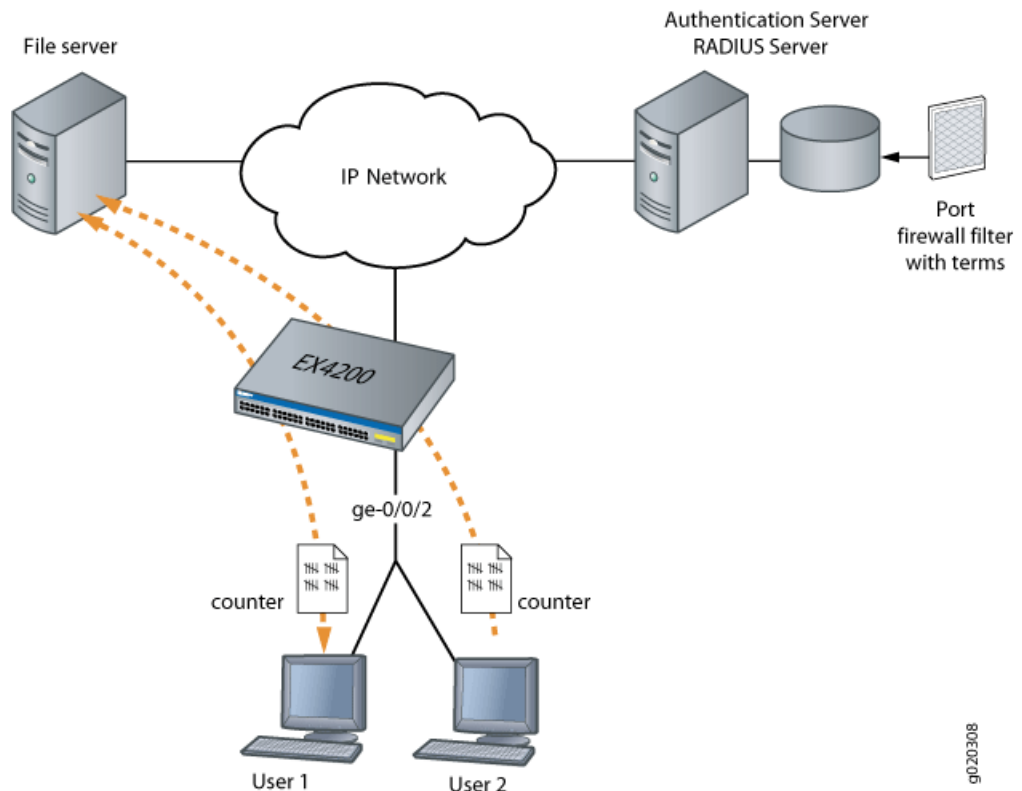
This is a conceptual model of the internal process—you cannot access or view the dynamic filter.



**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 15 on page 100](#) shows the network topology for this example.

Figure 15: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server



## Configuration

To configure firewall filters for multiple supplicants on 802.1X-enabled interfaces:

- [Configuring Firewall Filters on Interfaces with Multiple Supplicants on page 100](#)

### 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 protocols dot1x authenticator interface ge-0/0/2 supplicant multiple
set firewall family ethernet-switching filter filter1 term term1 from 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 1k
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. Configure interface **ge-0/0/2** for multiple supplicant mode authentication:
 

```
[edit protocols dot1x]
user@switch# set authenticator interface ge-0/0/2 supplicant multiple
```
2. Set policer definition:

```

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

```

3. 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 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 {
 destination-address {
 192.0.2.16/28;
 }
 }
 then count counter1;
 }
 term term2 {
 from {
 destination-address {
 192.0.2.16/28;
 }
 }
 then policer p1;
 }
 }
 }
}
policer p1 {
 if-exceeding {
 bandwidth-limit 1m;
 burst-size-limit 1k;
 }
 then discard;
}
}
protocols {
 dot1x {
 authenticator
 interface ge-0/0/2 {
 supplicant multiple;
 }
 }
}
}

```

## Verification

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

- [Verifying Firewall Filters on Interfaces with Multiple Supplicants on page 102](#)

---

### Verifying Firewall Filters on Interfaces with Multiple Supplicants

---

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>               | Verify that firewall filters are functioning on the interface with multiple supplicants.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Action</b>                | <ol style="list-style-type: none"><li>1. Check the results with one user authenticated on the interface. In this case, the user is authenticated on <b>ge-0/0/2</b>:<br/><br/>user@switch&gt; <b>show dot1x firewall</b><br/>Filter: dot1x_ge-0/0/2<br/>Counters<br/>counter1_dot1x_ge-0/0/2_user1 100</li><li>2. When a second user, User2, is authenticated on the same interface, <b>ge-0/0/2</b>, you can verify that the filter includes the results for both of the users authenticated on the interface:<br/><br/>user@switch&gt; <b>show dot1x firewall</b><br/>Filter: dot1x-filter-ge-0/0/0<br/>Counters<br/>counter1_dot1x_ge-0/0/2_user1 100<br/>counter1_dot1x_ge-0/0/2_user2 400</li></ol> |
| <b>Meaning</b>               | The results displayed by the <b>show dot1x firewall</b> command output reflect the dynamic filter created with the authentication of each new user. User1 accessed the file server located at the specified destination address 100 times, while User2 accessed the same file server 400 times.                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b> | <ul style="list-style-type: none"><li>• <a href="#">Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch on page 91</a></li><li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches</a></li><li>• <a href="#">Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 131</a></li></ul>                                                                                                                                                                                                                                                              |

---

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

---

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 103](#)
- [Overview and Topology on page 103](#)

- [Configuration on page 103](#)
- [Verification on page 105](#)
- [Troubleshooting on page 106](#)

## Requirements

This example uses the following hardware and software components:

- An EX Series switch that supports captive portal
- Junos OS Release 10.1 or later for EX Series switches

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 41](#).
- Designed your captive portal login page. See [“Designing a Captive Portal Authentication Login Page on an EX Series Switch” on page 153](#).

## 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 without going through captive portal, add its MAC address to the authentication whitelist. The MAC addresses in this list are permitted access on the interface without captive portal.

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 http
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 ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22
set custom-options post-authentication-url http://www.my-home-page.com
```

**Step-by-Step  
Procedure**

To configure captive portal on the switch:

1. Enable HTTP access on the switch:

```
[edit]
user@switch# set system services web-management http
```

2. To create a secure channel for Web access to the switch, configure captive portal for HTTPS:



**NOTE:** You can enable HTTP without enabling HTTPS, but we recommend HTTPS for security purposes.

- a. Associate the security certificate with the Web server and enable HTTPS access on the switch:

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

- b. Configure captive portal to use HTTPS:

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

3. Enable an interface for captive portal:

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

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



**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 authentication bypass will not be allowed.

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



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

5. (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 {
 http;
 https {
 local-certificate my-signed-cert;
 }
 }
 }
}
security {
 certificates {
 local {
 my-signed-cert {
 "-----BEGIN RSA PRIVATE KEY-----\nMIICXwIBAAKBgQDk8sUggnXdDUmr7T
 vLv63yJq/LRpDASfIDZlX3z9ZDe1Kfk5C9\nr/kyvzv
 ...
 Pt5YmvWDoGo0mSjoE/liH0BqYdh9YGqv3T2IEUfflSTQQHEOShS0ogWDHF\
 nnyOb1O/vQtjk20X9NVQg JHBwidssY9eRp\n-----END CERTIFICATE-----\n";
 ## SECRET-DATA
 }
 }
 }
}
services {
 captive-portal {
 interface {
 ge-0/0/10.0 {
 supplicant multiple;
 }
 }
 secure-authentication https;
 }
}
ethernet-switching-options {
 authentication-whitelist {
 00:10:12:e0:28:22/48;
 }
}
```

## Verification

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

- [Verifying That Captive Portal Is Enabled on the Interface on page 105](#)
- [Verify That Captive Portal Is Working Correctly on page 106](#)

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

**Purpose** Verify that captive portal is configured on 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 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 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 these tasks:

- [Troubleshooting Captive Portal on page 106](#)

---

### 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 Web page.

**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, 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 151](#)
  - [Designing a Captive Portal Authentication Login Page on an EX Series Switch on page 153](#)

## 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 107](#)
- [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 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 41](#).
- 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 16 on page 109](#) 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 16: EX Series Switch Connecting OAC to RADIUS Server Using EAP-TTLS Authentication

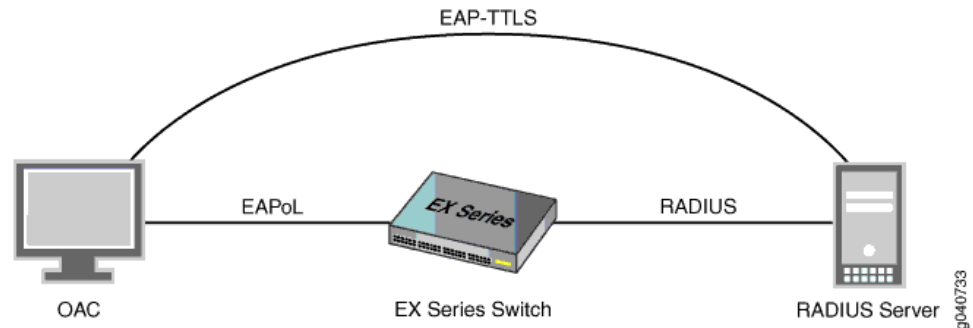


Table 13 on page 109 describes the components in this OAC deployment:

Table 13: Components of the OAC Deployment

| Property                         | Settings                                                                                            |
|----------------------------------|-----------------------------------------------------------------------------------------------------|
| Switch hardware                  | EX Series switch                                                                                    |
| VLANs                            | <b>default</b><br><b>server-reject-vlan:</b> VLAN name is <b>remedial</b> and VLAN ID is <b>700</b> |
| 802.1X interface                 | <b>ge-0/0/8</b>                                                                                     |
| 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 111](#)

### 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 10](#)

## Example: Configuring Centralized Access Control to Network Resources, with an EX Series Switch Connected to Junos Pulse Access Control Service

You can deploy an EX Series switch and Junos Pulse Access Control Service to control who is admitted to your network and what resources—servers, applications, stored data, and other devices—the user can access after being admitted to the network. Access Control Service provides both authentication and authorization:

With this combination of products, the switch serves as an *Infranet Enforcer*, that is, a policy enforcement point for Access Control Service. Access Control Service sends authentication entries and resource access policies when an endpoint successfully completes

802.1X or MAC authentication (unmanaged devices). Access for any endpoint is governed by the resource access policies that you configure on Access Control Service. The switch converts the resource access policies into filter definitions and applies these to the appropriate port. Because resource access policies are employed, firewall filters are not required for the switch configuration.

This example describes how to configure the switch to use Access Control Service for authentication and authorization and how to configure Access Control Service to use the switch as an Infranet Enforcer.



**NOTE:** This example configures the switch prior to configuring the Access Control Service. However, you can configure the Access Control Service first, if you prefer. The sequence does not matter.

The example also describes the requisite configuration procedures on Access Control Service for configuring user roles, user realms, and resource access policies:

- [Requirements on page 112](#)
- [Overview and Topology on page 113](#)
- [Configuring the EX Series Switch to Connect to the Junos Pulse Access Control Device on page 115](#)
- [Creating an Authentication Server Instance on the UAC NAC Device on page 117](#)
- [Configuring User Roles on the UAC NAC Device on page 118](#)
- [Configuring a User Realm on page 119](#)
- [Mapping User Roles to the User Realm on page 119](#)
- [Configuring Sign-In Policies on page 120](#)
- [Configuring a Location Group on page 120](#)
- [Configuring an EX Series Switch Infranet Enforcer Instance on the UAC NAC Device on page 120](#)
- [Configuring Resource Access Policies on the UAC NAC Device on page 121](#)
- [Verification on page 122](#)

## Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.2 or later for EX Series switches
- One EX Series switch acting as an Infranet Enforcer and an authenticator port access entity (PAE)
- Junos Pulse Access Control Service Release 4.2 or later
- Access Control Service IC Series device or MAG Series device

Before you configure the switch to use Access Control Service, be sure you have:

- Installed and set up the IC Series device or the MAG Series device.

- For information on the IC Series, see [http://www.juniper.net/techpubs/en\\_US/release-independent/uac/information-products/pathway-pages/unified-access-control/product/](http://www.juniper.net/techpubs/en_US/release-independent/uac/information-products/pathway-pages/unified-access-control/product/).
- For information on the MAG Series, see [http://www.juniper.net/techpubs/en\\_US/release-independent/mag/information-products/pathway-pages/mag-series/product/](http://www.juniper.net/techpubs/en_US/release-independent/mag/information-products/pathway-pages/mag-series/product/).
- The IP address and password of the IC Series or MAG Series device.



**NOTE:** Within the example, the IC Series or MAG Series device is referred to as a Network Access Control (NAC) device.

## Overview and Topology

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 Access Control Service as the user database for 802.1X authentication, as well as for MAC RADIUS authentication.

In addition, Access Control Service functions as a centralized policy management server. It eliminates the need to configure firewall filters on the individual switch. Instead, you define resource access policies centrally on Access Control Service. The resource access policy defines which network resources are allowed and denied for a user, based upon the user's role. Access Control Service NAC device distributes these policies to all connected switches. For messages relating to access policies, the NAC device communicates with the switch using the Junos UAC Enforcer Protocol (JUEP).

The Access Control Service IC Series device or MAG Series device acts as your centralized NAC device. Specific resources are allocated through resource access policies from the Access Control Service device. The ports on the switch form a control gate that blocks all traffic to and from supplicants until they are authenticated.

Limit access to protected resources by defining *user roles* and *user realms* with accompanying *resource access policies* in the UAC admin console.

In this example, we are configuring access control for a medical facility. Because we are using Access Control Service for centralized access control, we specify the permissions and limitations on the UAC NAC device.

To ensure patient privacy, the patient medical history files are accessible only to the medical staff (**med-staf**). The patient insurance information and payment records are available only to the accounts personnel (**accounts**). Other information pertaining to the patients is available to anyone of the general staff (**other**).

The switch acts as an Infranet Enforcer and an authenticator port access entity (PAE). It blocks all traffic and acts as a control gate until the supplicant (client) is authenticated by the server. All other users and devices are denied access.

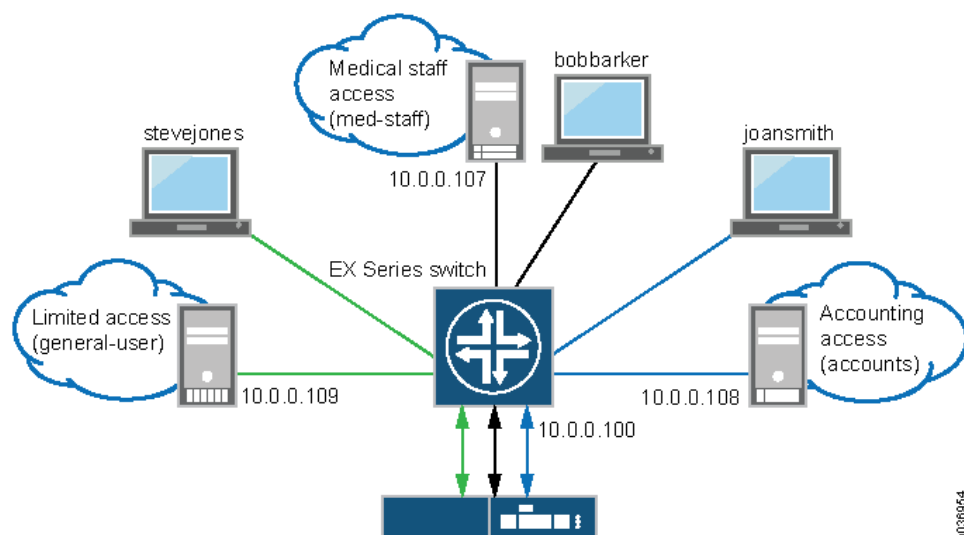
Table 14 on page 114 shows the configuration components used for the switch and the Access Control Service NAC device in this example.

**Table 14: Components of the Topology for Access Control Service and the EX Series Switch**

| Property                                                                          | Settings                 |
|-----------------------------------------------------------------------------------|--------------------------|
| Access Control Service NAC device properties that must be specified on the switch | IP address—10.204.88.148 |
|                                                                                   | hostname—my_nac          |
|                                                                                   | password—MyUACPassword   |
| Password to use for connecting the switch with the RADIUS server                  | <b>MySecret</b>          |
| Access profile, specified on the switch, to define the connection to the UAC      | <b>myuac_profile</b>     |
| Switch hostname                                                                   | <b>myswitch</b>          |
| User <b>roles</b> on the NAC device                                               | <b>med-staff</b>         |
|                                                                                   | <b>accounts</b>          |
|                                                                                   | <b>general-user</b>      |
| User <b>realm</b> on the NAC device                                               | <b>hospital-staff</b>    |
| Location <b>group</b> on the NAC device                                           | <b>medical-group</b>     |

Figure 17 on page 114 shows the topology used in this example.

**Figure 17: Centralized Access Control to Network Resources with an EX Series Switch Connected to Junos Pulse Access Control Service**



## Configuring the EX Series Switch to Connect to the Junos Pulse Access Control Device

**CLI Quick Configuration** To quickly connect the switch to Access Control Service, copy the following commands and paste them into the switch terminal window:



**NOTE:** This example uses the default values for **timeout**, **interval**, and **timeout-action**.

```
[edit]
set ethernet-switching-options uac-policy
set access profile myuac_profile authentication-order radius
set access profile myuac radius authentication-server 10.204.88.148
set access radius-server 10.204.88.148
set access radius-server secret MySecret
set services unified-access-control infranet-controller my_nacaddress 10.204.88.148
set services unified-access-control infranet-controller myswitch interface me0.0
set services unified-access-control infranet-controller myswitch password MyUACPassword
set protocols dot1x authenticator authentication-profile-name myuac_profile
set protocols dot1x authenticator interface ge-0/0/10.0
```

### Step-by-Step Procedure

To connect the switch to your UAC NAC device:

1. Configure the switch to use Access Control Service for authentication and authorization:
 

```
[edit ethernet-switching-options]
user@switch# set uac-policy
```
2. Configure the access profile to specify Access Control Service. The access profile contains the authentication and authorization configuration that aids in handling authentication and authorization requests, including the authentication method and sequence, and Access Control Service address:
  - a. Configure **radius** as the authentication method to be used when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches:
 

```
[edit access profile]
user@switch# set myuac_profile authentication-order radius
```
  - b. Define the access profile for connecting to the UAC by specifying the IP address of the authentication server:



**NOTE:** Specify the same IP address that you use for the RADIUS server and the NAC device.

- ```
[edit access profile]
user@switch# set myuac_profile radius authentication-server 10.204.88.148
```
3. Configure the RADIUS server to use the same IP address that you specified for the authentication server:


```
[edit access]
```

```
user@switch# set radius-server 10.204.88.148
```

4. Configure the password to use for connecting the switch with the RADIUS server:



NOTE: The password specified here is used for RADIUS communications between the switch and Access Control Service. It does not need to match the password that is specified on Access Control Service through the administrative interface on Access Control Service.

```
[edit access]
```

```
user@switch# set radius-server secret MySecret
```

5. Configure the address of Access Control Service NAC device:



NOTE: Specify the hostname and IP address of the NAC device. This is the same IP address that you used for specifying the authentication server.

```
[edit services united-access-control infranet-controller my_nac ]
```

```
user@switch# set address 10.204.88.148
```

6. Configure the switch's management Ethernet interface for the NAC device:

```
[edit services united-access-control infranet-controller myswitch]
```

```
user@switch# set interface me0.0
```

7. Configure the password for connecting the switch to the Access Control Service NAC device:



NOTE: This password must match the password specified on Access Control Service through its administrative interface. It is used for Junos UAC Enforcer Protocol (JUEP) communications between the switch and Access Control Service.

```
[edit services united-access-control infranet-controller myswitch]
```

```
user@switch# set password MyUACPassword
```

8. Specify the name of the access profile to use for 802.1X, MAC RADIUS, or captive portal authentication:



NOTE: Use the same access profile that you configured previously (step 2).

```
[edit protocols dot1x]
```

```
user@switch# set authenticator authentication-profile-name myuac_profile
```

9. Configure the 802.1X interface that the switch will use for communicating with Access Control Service:

```
[edit protocols dot1x]
```

```
user@switch# set authenticator interface ge-0/0/10.0
```

Results Display the results of the configuration:

```
user@switch> show configuration

services {
  unified-access-control {
    infranet-controller myuac {
      address 10.204.88.148;
      interface me0.0;
      password "$9$uOdBBRSvWxwYoreYoJGq.0BI"; ## SECRET-DATA
    }
  }
}
ethernet-switching-options {
  uac-policy;
}
protocols {
  dot1x {
    authenticator {
      authentication-profile-name myuac_profile;
      interface {
        ge-0/0/10.0;
      }
    }
  }
}
access {
  radius-server {
    10.204.88.148
    port 1812;
    secret "$9$38aJ6A0yIMXNb0BEyeK7Ns24oDkqm5Qz6k.ORSrLXJGDHPQ6/t"; ##
    SECRET-DATA
  }
}
profile myuac_profile {
  authentication-order radius;
  radius {
    authentication-server 10.204.88.148;
  }
}
```

Creating an Authentication Server Instance on the UAC NAC Device

Step-by-Step Procedure Access Control Service supports a variety of user authentication and authorization servers. To quickly set up user authentication, you can use local authentication on the Access Control Service NAC device. This example uses the preconfigured local authentication server, System Local.

To set up local user authentication on the NAC device:

1. In the NAC device admin console, select **Authentication > Auth. Servers**.
2. Click **System Local**.
3. Select the **Users** tab.
4. Click **New**.

5. In the dialog box for **New Local User**, enter information into the text boxes of the following fields:

- **Username**
- **Full Name**
- **Password**



NOTE: All other fields are optional.

6. Click **Save Changes**.
7. Repeat this procedure for each user that you want to include in the device database. For example, we created three users: **bobbarker**, **joansmith**, and **stevejones**

Results The users **bobbarker**, **joansmith**, and **stevejones** are available in the NAC device database and can be associated with a role.

Configuring User Roles on the UAC NAC Device

Step-by-Step Procedure To set up the user roles:



NOTE: In this example, either Odyssey Access Client or the Junos Pulse client is installed on the client.

1. In the NAC device admin console, select **Users > User Roles**.
2. Click **New Role** and then enter the **Name** of the role that allows users with compliant endpoints to access the protected resources. You can also enter additional information about this role into the **Description** text box.
3. Click **Save Changes**.
4. Repeat these steps to create the additional user roles. For example, we created three roles: **med-staff**, **accounts**, and **general-user**

Results The roles, **med-staff**, **accounts**, and **general-user**, are available in the NAC database.

Configuring a User Realm

Step-by-Step Procedure To configure a user realm within the authentication server instance.



NOTE: Only one user realm is required.

1. In the NAC device admin console, select **Users > User Realms**.
2. In the dialog box **User Authentication Realms**, click **New**.
3. In **New Authentication Realm**, :
 - Enter information into the text boxes:
 - **Name**—Name of the realm. For this example, we are using **hospital-staff**.
 - **Description**—(Optional) Any additional information that you wish to provide.
 - Under **Servers**:
 - **Authentication**—Select **System Local**.
 - **Directory/Attribute**—Select **None**.
 - **Accounting**—Select **None**.
4. Click **Save Changes**.

Results The new user realm can be associated with the roles you have created.

Mapping User Roles to the User Realm

Step-by-Step Procedure To map each user role to a rule within the user authentication realm.

1. In the NAC device admin console, select **Users > User Realms > Role Mapping hospital-staff**.
2. Click **New Rule**.
3. In the Role Mapping Rule dialog box, for a rule based on username, enter the information for the appropriate fields:
 - Under **Rule: If username**, is———**bobbarker**.
 - Under **then assign these roles**, select **med-staff** role and then click **Add**.
4. Create additional role mapping rules for additional users. For example, create a role mapping rule to associate user joansmith with accounts, and a role mapping rule to associate user stevejones with medical-staff.
5. Click **Save Changes**.

Results Each user is associated with a role.

Configuring Sign-In Policies

- Step-by-Step Procedure** To create a user sign-in policy:
1. In the admin console, select **Authentication > Signing in > Sign-in Policies**.
 2. To create a new sign-in policy, click **New URL** and select **Users**.
 3. In the **Sign-in URL** field, enter the URL that you want to associate with the policy. Use the format `<host>/<path>` where `<host>` is the hostname of the NAC device, and `<path>` is any string users must enter. For example `*/testsite/`.
 4. (Optional) Enter a **Description** for the policy.
 5. In the **Sign-in Page** list, select **Default Sign-in Page**.
 6. Under **Available realms**, select the hospital-staff that you created.
 7. Under **Authentication protocol set**, select **802.1X**.
 8. Click **Save Changes**.
- Results** A sign-in URL is available for users.

Configuring a Location Group

- Step-by-Step Procedure** You must create a location group to associate with an Infranet Enforcer instance.
1. In the admin console, select **Network Access > Location Group**.
 2. Select **New Location Group**.
 3. For **Name**, type `medical-group`.
 4. Add an optional description.
 5. Leave the default sign-in policy.
 6. Click **Save Changes**.

Results A location group that can be assigned to the EX Series switch is created.

Configuring an EX Series Switch Infranet Enforcer Instance on the UAC NAC Device

- Step-by-Step Procedure** To configure Junos Pulse Access Control Service to accept a connection from the switch:
1. On the left navigation bar in the NAC device admin console, select **UAC > Infranet Enforcer > Connection**.
 2. Click **New Enforcer**. The New Infranet Enforcer dialog box appears. By default, the new ScreenOS Enforcer page is displayed.
 3. Select the **Junos EX** option button. The New Infranet Enforcer page is displayed.
 4. Enter the name of the switch in the **Name** box.

5. Enter the password for the switch. This password is a shared secret that administrators of both the switch and Junos Pulse Access Control Service can use for connectivity between the two devices.
6. Enter the serial number of the switch.
7. For **Location Group**, select **medical-group**.
8. Click **Save Changes**.

Results Junos Pulse Access Control Service and the EX switch can be connected.

Configuring Resource Access Policies on the UAC NAC Device

Step-by-Step Procedure

To create a resource access policy:

1. In the Infranet Enforcer admin console, select **UAC > Infranet Enforcer > Resource Access**.
2. Click **New Policy**.
3. On the **New Policy** page:
 - a. For **Name** and **Description**, enter any name and description for this policy, such as **MedicalServer**.
 - b. For **Resources**, specify the protocol, IP address, network mask, and port of each resource (or range of addresses) for which this Infranet Enforcer resource access policy applies, one per line. You cannot specify a hostname in an Infranet Enforcer resource access policy. You can specify only an IP address. You can use TCP, UDP, or ICMP.

For example, type:10.204.91.20 to specify the med-staff protected resources on the switch.
 - c. In the **Infranet Enforcer** box, add the switch you created to selected Enforcers.
 - d. In the **Roles** box, select **Policy applies to SELECTED roles**, select **med-staff**, and click **Add** to apply this resource access policy to users who are mapped to the med-staff role.
 - e. In the **Action** box, select **Allow** access.
4. Click **Save Changes**.
5. Complete two additional resource access policies:
 - Allow role accounts with the IP address 10.204.91.21.
 - Allow role general-access with the IP address 10.204.91.22.

Results Individual users, through their assigned roles, are provided access to the proper protected assets.

Verification

The following procedures verify the connections between the switch and the NAC device.

- [Verifying That the Switch Is Connected to Access Control Service on page 122](#)
- [Verifying the Configuration of Resource Access Policies on page 122](#)
- [Verifying the Mapping of Roles to Resources on page 123](#)

Verifying That the Switch Is Connected to Access Control Service

Purpose Verify that the switch is connected to Access Control Service.

Action Confirm the status of the connection to Access Control Service.

```
user@switch> show services unified-access-control status
```

Host	Address	Port	Interface	State
ic	10.204.88.148	11123	vlan.60	connected

Meaning Confirm that the **State** indicates that the Access Control Service is connected.

Verifying the Configuration of Resource Access Policies

Purpose After you have configured the access resource policies on the UAC device admin console, verify that they have been deployed to the switch.

Action Confirm that resource access policies for the switch have been configured on Access Control Service .

```

user@switch> show services unified-access-control policies detail
Identifier: 1
  Resource: 10.204.91.20:*
  Action: allow
  Apply: selected
  Role identifier      Role name
    0000000001.000005.0 med-staff
Identifier: 2
  Resource: 10.204.91.21:*
  Action: allow
  Apply: selected
  Role identifier      Role name
    1331203933.456038.0 accounts
Identifier: 3
  Resource: 10.204.91.23:*
  Action: allow
  Apply: selected
  Role identifier      Role name
    1318918961.643263.0 general-user
Identifier: 4
  Resource: 10.204.88.148:*
  Resource: udp://*:53,67
  Action: allow
  Apply: all
Total: 4

```



NOTE: There must always be a resource access policy to allow traffic to the Access Control Service.

Meaning The results show the resource access policies that were configured in this example. The policy with identifier 4 is the policy that allows traffic to the Access Control Service. It lists the IP address of the Access Control Service and an additional resource for **udp** indicating that it allows dhcp/dns traffic, too.

Verifying the Mapping of Roles to Resources

Purpose Display the content of the authentication table in a user role firewall implementation. The table, pushed from a supporting Access Control Service device, provides the user roles associated with incoming traffic.

Action Display the contents of the authentication table to show the mapping of roles to resources.

```
user@switch> show services unified-access-control authentication-table detail
Identifier: 6
Source: 00-50-56-a4-5a-4c/10.204.90.61
Username: bobbarker
Age: 0
Role identifier      Role name
0000000001.000005.0 med-staff
Total: 1
```

Meaning This output shows the mapping for username **bobbarker**. The output shows only one user, because only this user is connected at the time that the command is issued. If additional users were connected, the other users would also be displayed.

Related Documentation

- [Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service \(CLI Procedure\) on page 159](#)
- [Understanding Centralized Network Access Control and EX Series Switches on page 33](#)

CHAPTER 4

Configuration Tasks

- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 126](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\) on page 127](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 130](#)
- [Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 131](#)
- [Configuring LLDP \(CLI Procedure\) on page 136](#)
- [Configuring LLDP \(J-Web Procedure\) on page 139](#)
- [Configuring LLDP-MED \(CLI Procedure\) on page 140](#)
- [Juniper-Switching-Filter VSA Match Conditions and Actions on page 142](#)
- [Configuring RADIUS Server Fail Fallback \(CLI Procedure\) on page 144](#)
- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 146](#)
- [Configuring Flexible Authentication Order on page 147](#)
- [Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication \(CLI Procedure\) on page 149](#)
- [Specifying RADIUS Server Connections on an EX Series Switch \(CLI Procedure\) on page 150](#)
- [Configuring Captive Portal Authentication \(CLI Procedure\) on page 151](#)
- [Designing a Captive Portal Authentication Login Page on an EX Series Switch on page 153](#)
- [Controlling Authentication Session Timeouts \(CLI Procedure\) on page 155](#)
- [Configuring NetBIOS Snooping \(CLI Procedure\) on page 156](#)
- [Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control \(CLI Procedure\) on page 157](#)
- [Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service \(CLI Procedure\) on page 159](#)
- [Configuring Central Web Authentication on page 160](#)

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 149.
- 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 150.

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 \(J-Web Procedure\) on page 127](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56](#)
- [Monitoring 802.1X Authentication on page 313](#)
- [Verifying 802.1X Authentication on page 314](#)
- [Configuring LLDP \(CLI Procedure\) on page 136](#)
- [Understanding Authentication on EX Series Switches on page 10](#)

Configuring 802.1X Authentication (J-Web Procedure)



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

To configure 802.1X settings on an EX Series switch using the J-Web interface:

1. Select **Configure > Security > 802.1X**.

The 802.1X screen displays a list of interfaces, whether 802.1X security has been enabled, and the assigned port role.

When you select an interface, the **Details of 802.1x configuration on port** section displays 802.1X details for that interface.



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

2. Click one of the following options:

- **RADIUS Servers**—Specifies the RADIUS server to be used for authentication. Select the check box to specify a server. Click **Add** or **Edit** to add or modify the RADIUS server settings. Enter information as specified in [Table 15 on page 128](#).
- **Exclusion List**—Excludes hosts from the 802.1X authentication list by specifying the MAC address. Click **Add** or **Edit** in the Exclusion list screen to include or modify the MAC addresses. Enter information as specified in [Table 16 on page 128](#).
- **Edit**—Specifies 802.1X settings for the selected interface
 - **Apply 802.1X Profile**—Applies an 802.1X profile based on the port role. If a message appears asking whether you want to configure a RADIUS server, click **Yes**.
 - **802.1X Configuration**—Configures custom 802.1X settings for the selected interface. If a message appears asking if you want to configure a RADIUS server, click **Yes**. Enter information as specified in [Table 15 on page 128](#). To configure 802.1X settings, enter information as specified in [Table 17 on page 129](#).
- **Delete**—Deletes 802.1X authentication configuration on the selected interface.

Table 15: RADIUS Server Settings

Field	Function	Your Action
IP Address	Specifies the IP address of the server.	Enter the IP address in dotted decimal notation.
Password	Specifies the login password.	Enter the password.
Confirm Password	Verifies the login password for the server.	Reenter the password.
Server Port Number	Specifies the port with which the server is associated.	Type the port number.
Source Address	Specifies the source address of the switch using which the switch can communicate with the server.	Type the IP address in dotted decimal notation.
Retry Attempts	Specifies the number of login retries allowed after a login failure.	Type the number.
Timeout	Specifies the time interval to wait before the connection to the server is closed.	Type the interval in seconds.

Table 16: 802.1X Exclusion List

Field	Function	Your Action
MAC Address	Specifies the MAC address to be excluded from 802.1X authentication.	Enter the MAC address.
Exclude if connected through the port	Specifies that the host can bypass authentication if it is connected through a particular interface.	Select to enable the option. Select the port through which the host is connected.
Move the host to the VLAN	Specifies moving the host to a specific VLAN once the host is authenticated.	Select to enable the option. Select the VLAN from the list.

Table 17: 802.1X Port Settings

Field	Function	Your Action
Supplicant Mode		
Supplicant Mode	Specifies the mode to be adopted for supplicants: <ul style="list-style-type: none"> • Single—allows only one host for authentication. • Multiple—allows multiple hosts for authentication. Each host is checked before being admitted to the network. • Single authentication for multiple hosts—Allows multiple hosts but only the first is authenticated. 	Select a mode.
Authentication		
Enable re-authentication	Specifies enabling reauthentication on the selected interface.	1. Select to enable reauthentication. 2. Enter the timeout for reauthentication in seconds.
Action on authentication failure	Specifies the action to be taken in case the host does not respond, leading to an authentication failure.	Select one: <ul style="list-style-type: none"> • Move to the Guest VLAN—Select the VLAN to move the interface to. • Deny—The host is not permitted access.
Timeouts	Specifies timeout values for each action.	Enter the value in seconds for: <ul style="list-style-type: none"> • Port waiting time after an authentication failure • EAPOL retransmitting interval • Max. EAPOL requests • Maximum number of retries • Port timeout value for the response from the supplicant • Port timeout value for the response from the RADIUS server

- Related Documentation**
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 126](#)
 - [Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 50](#)
 - [Understanding Authentication on EX Series Switches on page 10](#)

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/122.69.1.250
[root@freeradius 122.69.1.250]# ls
```

```
detail-20071214
```

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

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

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

- Related Documentation**
- [Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41](#)
 - [Understanding 802.1X and RADIUS Accounting on EX Series Switches on page 16](#)

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 132](#)
2. [Applying a Locally Configured Firewall Filter from the RADIUS Server on page 135](#)

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 142 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 a1and
Exp
$
#  VENDOR      Juniper      2636
BEGIN-VENDOR   Juniper
ATTRIBUTE      Juniper-Local-User-Name      1      string
ATTRIBUTE      Juniper-Allow-Commands       2      string
ATTRIBUTE      Juniper-Deny-Commands        3      string
ATTRIBUTE      Juniper-Allow-Configuration  4      string
ATTRIBUTE      Juniper-Deny-Configuration   5      string
ATTRIBUTE      Juniper-Switching-Filter      48     string
<-
```

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

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

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

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

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

- To deny access based on a destination IP address:

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

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

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

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

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

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

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



.....

NOTE: For the `forwarding-class` option to be applied, the forwarding class must be configured on the switch 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/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 91](#)
 - [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches](#)
 - [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 126](#)
 - [Understanding Dynamic Filters Based on RADIUS Attributes on page 23](#)

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 136](#)
- [Adjusting LLDP Advertisement Settings on page 137](#)
- [Adjusting SNMP Notification Settings of LLDP Changes on page 137](#)
- [Specifying a Management Address for the LLDP Management TLV on page 138](#)
- [Configuring LLDP Power Negotiation on page 138](#)

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 and EX4200 (except EX4200-24P and EX4200-48P models) switches.

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

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

- [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 \(J-Web Procedure\) on page 139](#)
- [Configuring LLDP-MED \(CLI Procedure\) on page 140](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 18](#)

Configuring LLDP (J-Web Procedure)



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

Use the LLDP Configuration page to configure LLDP global and port settings for an EX Series switch on the J-Web interface.

To configure LLDP:

1. Select **Configure > Switching > LLDP**.

The LLDP Configuration page displays LLDP Global Settings and Port Settings.

The second half of the screen displays operational details for the selected port.



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

2. For an EX8200 Virtual Chassis configuration, select the member and the slot (FPC) from the list.
3. To modify LLDP Global Settings, click **Global Settings**.
Enter information as described in [Table 18 on page 140](#).
4. To modify Port Settings, click **Edit** in the Port Settings section.

Enter information as described in [Table 19 on page 140](#).

Table 18: Global Settings

Field	Function	Your Action
Advertising interval	Specifies the frequency of outbound LLDP advertisements. You can increase or decrease this interval.	Type the number of seconds.
Hold multiplier	Specifies the multiplier factor to be used by an LLDP-enabled switch to calculate the time-to-live (TTL) value for the LLDP advertisements it generates and transmits to LLDP neighbors.	Type the required number in the field.
Fast start count	Specifies the number of LLDP advertisements sent in the first second after the device connects. The default is 3. Increasing this number results in the port initially advertising LLDP-MED at a faster rate for a limited time.	Type the Fast start count.

Table 19: Edit Port Settings

Field	Function	Your Action
LLDP Status	Specifies whether LLDP has been enabled on the port.	Select one: Enabled , Disabled , or None .
LLDP-MED Status	Specifies whether LLDP-MED has been enabled on the port.	Select Enable from the list.

Related Documentation

- [Configuring LLDP \(CLI Procedure\) on page 136](#)
- [Configuring LLDP-MED \(CLI Procedure\) on page 140](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 18](#)

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 140](#)
- [Configuring Location Information Advertised by the Switch on page 141](#)
- [Configuring a Fast Start for LLDP-MED on page 141](#)

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) on page 139
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56

- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
- [Configuring LLDP \(CLI Procedure\) on page 136](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 18](#)

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 20 on page 142](#) 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 20: Match Conditions

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

Table 20: Match Conditions (*continued*)

Option	Description
ip-protocol <i>protocol-id</i>	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)
source-port <i>port</i>	TCP or User Datagram Protocol (UDP) source port field. Normally, you specify this match statement in conjunction with the ip-protocol match statement to determine which protocol is being used on the port. In place of the numeric field, you can specify one of the text options listed under destination-port .
destination-port <i>port</i>	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), mobileip-mn (435), msdp (639), netbios-dgm (138), netbios-ns (137), netbios-ssn (139), nfsd (2049), nntp (119), ntalk (518), ntp (123), pop3 (110), pptp (1723), printer (515), radacct (1813), radius (1812), rip (520), rkinit (2108), smtp (25), snmp (161), snmptrap (162), snpp (444), socks (1080), ssh (22), sunrpc (111), syslog (514), telnet (23), tacacs-ds (65), talk (517), tftp (69), timed (525), who (513), xmcp (177), zephyr-clt (2103), zephyr-hm (2104)

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 21 on page 143](#) shows the actions that you can specify in a term.

Table 21: Actions for VSAs

Option	Description
(allow deny)	Accept a packet or discard a packet silently without sending an Internet Control Message Protocol (ICMP) message.
forwarding-class <i>class-of-service</i>	(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
loss-priority (low medium high)	(Optional) Set the packet loss priority (PLP) to low , medium , or high . Specify both the forwarding class and the loss priority.

Related Documentation • [Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 131](#)

- [Understanding Dynamic Filters Based on RADIUS Attributes on page 23](#)
- [Understanding Vendor-Specific Attributes \(VSAs\)](#)

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.



.....

NOTE: Server fail fallback and the server reject fallback are not supported for VLAN-tagged traffic. If a VoIP client starts authentication by sending untagged data traffic to a VLAN while server fail or 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 fail or server reject fallback is in effect, the VoIP client is denied access to the fallback VLAN.

.....

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

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

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

- Configure an interface to prevent traffic flow from an end device to the LAN (as if the end device had failed authentication and had been 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
```

- 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:

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

Related Documentation

- [Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 79](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\) on page 127](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 126](#)
- [Monitoring 802.1X Authentication on page 313](#)
- [Understanding Server Fail Fallback and Authentication on EX Series Switches on page 28](#)

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 41](#).

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 85](#)
 - [Verifying 802.1X Authentication on page 314](#)
 - [Understanding Authentication on EX Series Switches on page 10](#)

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 144](#) 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 10](#)
 - [Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 85](#)

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 75](#)
 - [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 126](#)
 - [Configuring 802.1X Authentication \(J-Web Procedure\) on page 127](#)

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 126](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\) on page 127](#)
- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 146](#)
- [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 130](#)

Configuring Captive Portal Authentication (CLI Procedure)

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 41.
- Designed your captive portal login page. See “[Designing a Captive Portal Authentication Login Page on an EX Series Switch](#)” on page 153.

This topic includes the following tasks:

- [Configuring Secure Access for Captive Portal on page 151](#)
- [Enabling an Interface for Captive Portal on page 152](#)
- [Configuring Bypass of Captive Portal Authentication on page 152](#)

Configuring Secure Access for Captive Portal

To configure secure access for captive portal:

1. Enable HTTP access on the switch:

```
[edit]
```

```
user@switch# set system services web-management http
```

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

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



NOTE: You can enable HTTP without HTTPS, but we recommend HTTPS for security purposes.

3. 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 captive portal:

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

For example, to enable captive portal on the interface ge-0/0/10:

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

Configuring Bypass of Captive Portal Authentication

To allow specific clients to bypass captive portal:

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

For example, to allow specific clients to bypass captive portal:

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



NOTE: Optionally, you can use `set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22 interface ge-0/0/10.0` 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 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 authentication bypass will not be allowed.

Related Documentation

- [Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102](#)
- [Understanding Authentication on EX Series Switches on page 10](#)

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 18 on page 153 shows an example of a captive portal login page:

Figure 18: Example of a Captive Portal Login Page

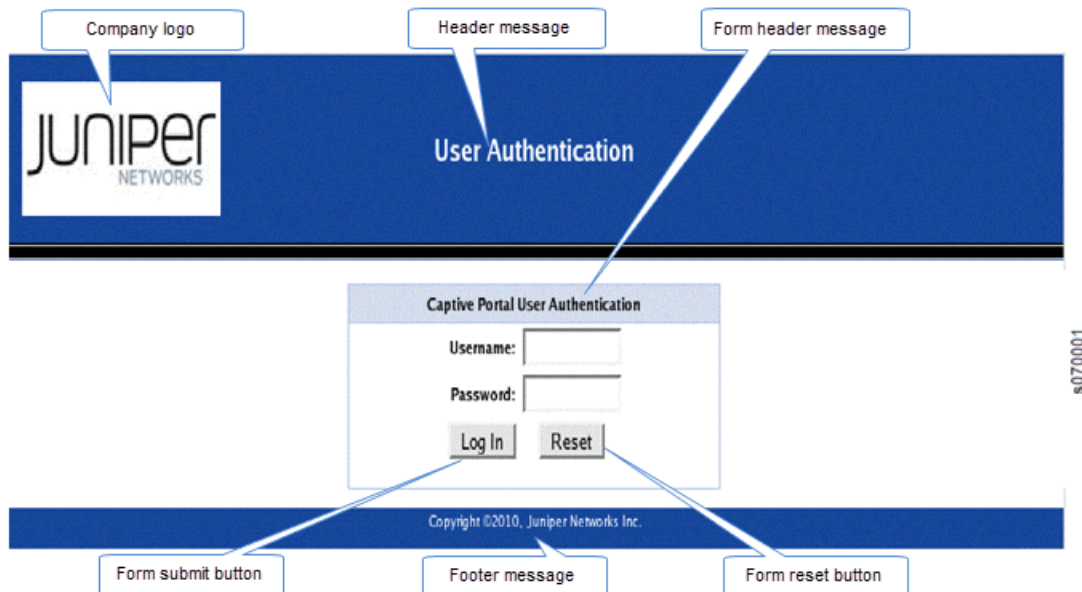


Table 22 on page 153 summarizes the configurable elements of a captive portal login page.

Table 22: 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.

Table 22: Configurable Elements of a Captive Portal Login Page (*continued*)

Element	CLI Statement	Description
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:

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

```
user@switch> file copy ftp://username:prompt@ftp.hostname.net/var/tmp/my-logo.jpeg
```
- 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 on page 102](#)
- [Understanding Authentication on EX Series Switches on page 10](#)
- [captive-portal on page 206](#)

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 150](#).
- Configure 802.1X authentication on the switch. See [“Configuring 802.1X Interface Settings \(CLI Procedure\)” on page 126](#).

To configure the authentication session time on all interfaces:

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

To configure the authentication session time on a single interface:

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

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

To remove the binding:

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

**Related
Documentation**

- [Configuring MAC Table Aging \(CLI Procedure\)](#)
- [Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 50](#)
- [Understanding Authentication on EX Series Switches on page 10](#)
- [Understanding Authentication Session Timeout on page 31](#)

Configuring NetBIOS Snooping (CLI Procedure)

NetBIOS snooping enables an EX Series switch to learn information about NetBIOS hosts that are connected to the switch.

This topic describes:

- [Enabling NetBIOS Snooping on page 156](#)
- [Disabling NetBIOS Snooping on page 156](#)

Enabling NetBIOS Snooping

To enable NetBIOS snooping:

```
[edit protocols lldp]
user@switch# set netbios-snooping
```

Disabling NetBIOS Snooping

To disable NetBIOS snooping:

```
[edit protocols lldp]
user@switch# delete netbios-snooping
```

**Related
Documentation**

- [show lldp neighbors on page 351](#)
- [Understanding NetBIOS Snooping on page 32](#)

Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)

You can connect the switch to Junos Pulse Access Control Service to set up a centralized, end-to-end network access control (NAC) system, which allows you to control who is admitted to the network and what resources those users are allowed to access.

The Access Control Service functions both as an *authentication server* (RADIUS server) and as a *centralized policy management server*.

Before you begin configuring the switch to connect to the Access Control Service:

- Configure a resource access policy. See *Configuring Resource Access Policies*.
- Obtain the password of the Access Control Service.
- Obtain the IP address of the Access Control Service.



NOTE: Specify the same IP address for the authentication server, the RADIUS server, and the infranet controller (NAC device). These components refer to the same Access Control Service.

To configure the switch to work with the Access Control Service:

1. Configure the switch to use the Access Control Service for authentication and authorization:


```
[edit ethernet-switching-options]
user@switch# set uac-policy
```
2. Configure the access profile to specify the Access Control Service. The access profile contains the authentication and authorization configuration that aids in handling authentication and authorization requests, including the authentication method and sequence, and the Access Control Service address:

- a. Configure **radius** as the authentication method to be used when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches:

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

- b. Specify the IP address of the authentication server:



NOTE: Specify the same IP address that you use for the RADIUS server and the NAC device.

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

3. Configure the RADIUS server to use the same IP address that you specified for the authentication server:

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

4. Configure the password to use for connecting the switch with the RADIUS server:



NOTE: The password specified here is used for RADIUS communications between the switch and the Access Control Service. It does not need to match the password that is specified on the Access Control Service through the administrative interface on the Access Control Service.

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

5. Configure the address of the Access Control Service MAG Series or the IC Series NAC device:



NOTE: Specify the hostname and IP address of the NAC device. This is the same IP address that you used for specifying the authentication server.

```
[edit services united-access-control infranet-controller hostname]
user@switch# set address ip-address
```

6. Configure the switch's management Ethernet interface for the NAC device:

```
[edit services united-access-control infranet-controller hostname]
user@switch# set interface me0.0
```

7. Configure the password for connecting the switch to the Access Control Service NAC device:



NOTE: This password must match the password specified on the Access Control Service through its administrative interface. It is used for Junos UAC Enforcer Protocol (JUEP) communications between the switch and the Access Control Service.

```
[edit services united-access-control infranet-controller hostname]
user@switch# set password password
```

8. Configure the amount of time that switch waits to receive a response from the Access Control Service:

```
[edit services united-access-control]
user@switch# set timeout seconds
```

9. Specify the time between continuity-check messages for the switch's connection with the Access Control Service:

```
[edit services united-access-control]
user@switch# set interval seconds
```

10. Specify an action for the switch to take if a timeout occurs for the connection between the switch and the Access Control Service:

```
[edit services united-access-control]
user@switch# set timeout-action action
```

11. Specify the name of the access profile to use for 802.1X, MAC RADIUS, or captive portal authentication:



NOTE: Use the same access profile that you configured previously (step 2).

```
[edit protocols dot1x]
```

```
user@switch# set authenticator authentication-profile-name profile-name
```

12. Configure the 802.1X interface that the switch will use for communicating with the Access Control Service:

```
[edit protocols dot1x]
```

```
user@switch# set authenticator interface interface-name
```

Related Documentation

- [Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service \(CLI Procedure\) on page 159](#)
- [Understanding Centralized Network Access Control and EX Series Switches on page 33](#)

Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure)

If you have connected the EX Series switch to the Junos Pulse Access Control Service and you want to use the captive portal user authentication feature, configure the Access Control Service network access control (NAC) device as an external captive portal server. The captive portal feature is required only for user authentication. Unmanaged devices, such as printers or phones, can be authenticated through 802.1X and MAC address authentication.

When users try to access a protected network resource that is connected to the switch, the user must first sign in to the Access Control Service for authentication and endpoint security checking. The captive portal redirects the user to a login page located on the Access Control Service.

When the sign-in page for the Access Control Service is displayed, the user signs in and the Access Control Service examines the endpoint for compliance with security policies. If the endpoint passes the security check, access is granted to the protected resource.

Before you begin, be sure you have:

- Configured access between the switch and the Access Control Service. See [“Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control \(CLI Procedure\)” on page 157](#).
- Designed your captive portal login page on the Access Control Service. See [About Sign-In Policies](#).

To configure the switch to use the Access Control Service for captive portal:

1. Configure captive portal to authenticate clients connected to the switch for access to use the authentication profile that directs the client to the Access Control Service:



NOTE: The access profile name specified here must match the access profile name that you specified for the Access Control Service in “Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)” on page 157.

[edit]

user@switch# **set services captive-portal authentication-profile-name** *access-profile-name*

2. Enable an interface for use with captive portal authentication:

[edit]

user@switch# **set services captive-portal interface** *interface-name* **supplicant** *multiple*

3. (Optional) Specify which clients are to bypass captive portal authentication:

[edit]

user@switch# **set ethernet-switching-options authentication-whitelist** *mac-address*



NOTE: You can use **set ethernet-switching-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 captive portal authentication by using the **clear captive-portal mac-address** *mac-address* command after adding its MAC address to the authentication 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.

Related Documentation

- [Understanding Centralized Network Access Control and EX Series Switches on page 33](#)
- [Understanding Authentication on EX Series Switches on page 10](#)

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 161](#)
- [Configuring the Redirect URL for Central Web Authentication on page 161](#)
- [Guidelines for Configuring Central Web Authentication on page 162](#)

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 35](#)

CHAPTER 5

Configuration Statements

- [\[edit access\] Configuration Statement Hierarchy on EX Series Switches on page 169](#)
- [\[edit ethernet-switching-options\] Configuration Statement Hierarchy on EX Series Switches on page 172](#)
- [\[edit protocols\] Configuration Statement Hierarchy on EX Series Switches on page 176](#)
- [\[edit protocols dot1x\] Configuration Statement Hierarchy on EX Series Switches on page 177](#)
- [\[edit protocols lldp\] Configuration Statement Hierarchy on EX Series Switches on page 179](#)
- [\[edit protocols lldp-med\] Configuration Statement Hierarchy on EX Series Switches on page 180](#)
- [access on page 182](#)
- [accounting \(Access Profile\) on page 183](#)
- [accounting on page 184](#)
- [accounting-port \(RADIUS Server\) on page 185](#)
- [accounting-port on page 186](#)
- [accounting-server on page 187](#)
- [accounting-session-id-format on page 188](#)
- [accounting-stop-on-access-deny on page 189](#)
- [accounting-stop-on-failure on page 190](#)
- [address \(Access Address Pool\) on page 191](#)
- [address \(Access Control Service\) on page 191](#)
- [address-pool on page 192](#)
- [address-range on page 192](#)
- [advertisement-interval on page 193](#)
- [attributes on page 194](#)
- [authentication-order \(Access Profile\) on page 195](#)
- [authentication-order \(Authenticator\) on page 196](#)
- [authentication-profile-name on page 198](#)
- [authentication-protocol on page 199](#)

- [authentication-server](#) on page 200
- [authentication-whitelist](#) on page 201
- [authenticator](#) on page 202
- [block-interval](#) on page 203
- [ca-type](#) on page 204
- [ca-value](#) on page 205
- [captive-portal](#) on page 206
- [certificate-verification](#) on page 207
- [civic-based](#) on page 208
- [country-code](#) on page 209
- [custom-options](#) on page 210
- [destination \(Accounting\)](#) on page 212
- [disable \(802.1X\)](#) on page 213
- [disable \(LLDP\)](#) on page 214
- [disable \(LLDP-MED\)](#) on page 214
- [disable \(LLDP Power Negotiation\)](#) on page 215
- [dot1x](#) on page 216
- [elin](#) on page 217
- [eapol-block](#) on page 218
- [ethernet-port-type-virtual](#) on page 218
- [ethernet-switching-options](#) on page 219
- [events](#) on page 222
- [exclude \(RADIUS\)](#) on page 223
- [fast-start \(LLDP-MED\)](#) on page 227
- [forwarding-class \(VoIP\)](#) on page 228
- [guest-vlan](#) on page 229
- [hold-multiplier](#) on page 230
- [ignore](#) on page 231
- [immediate-update](#) on page 232
- [infranet-controller](#) on page 232
- [interface \(802.1X\)](#) on page 233
- [interface \(Access Control Service\)](#) on page 234
- [interface \(Captive Portal\)](#) on page 235
- [interface \(LLDP\)](#) on page 236
- [interface \(LLDP-MED\)](#) on page 237
- [interface \(Static MAC Bypass\)](#) on page 238
- [interface \(VoIP\)](#) on page 239

- [interface-description-format](#) on page 240
- [interval \(Access Control Service\)](#) on page 241
- [lldp](#) on page 242
- [lldp-configuration-notification-interval](#) on page 244
- [lldp-med \(Ethernet Switching\)](#) on page 245
- [lldp-med-bypass](#) on page 246
- [lldp-priority](#) on page 246
- [location \(LLDP-MED\)](#) on page 247
- [mac-radius](#) on page 248
- [management-address](#) on page 249
- [maximum-requests](#) on page 250
- [nas-identifier](#) on page 250
- [nas-port-extended-format](#) on page 251
- [netbios-snooping](#) on page 252
- [no-mac-table-binding \(802.1X\)](#) on page 252
- [no-reauthentication](#) on page 253
- [no-tagging](#) on page 253
- [options](#) on page 254
- [order](#) on page 256
- [password \(Access Control Service\)](#) on page 257
- [port](#) on page 257
- [port \(Access Control Service\)](#) on page 258
- [port \(RADIUS Server\)](#) on page 259
- [port \(TACACS+ Server\)](#) on page 259
- [power-negotiation](#) on page 260
- [profile](#) on page 261
- [ptopo-configuration-maximum-hold-time](#) on page 262
- [ptopo-configuration-trap-interval](#) on page 262
- [quiet-period](#) on page 263
- [quiet-period \(Captive Portal\)](#) on page 263
- [radius \(Access Profile\)](#) on page 264
- [radius \(System\)](#) on page 266
- [radius](#) on page 267
- [radius-options \(Protocols 802.1X\)](#) on page 268
- [radius-server](#) on page 269
- [radius-server \(System\)](#) on page 270
- [reauthentication](#) on page 271

- [redirect-url on page 272](#)
- [retries on page 273](#)
- [retries \(Captive Portal\) on page 274](#)
- [retry on page 275](#)
- [retry \(RADIUS\) on page 276](#)
- [revert-interval on page 277](#)
- [routing-instance on page 277](#)
- [secret on page 278](#)
- [secret on page 279](#)
- [secure-authentication on page 279](#)
- [server \(RADIUS Accounting\) on page 280](#)
- [server \(TACACS+ Accounting\) on page 281](#)
- [server-fail on page 282](#)
- [server-reject-vlan on page 283](#)
- [server-timeout on page 284](#)
- [server-timeout \(Captive Portal\) on page 285](#)
- [session-expiry on page 286](#)
- [single-connection on page 287](#)
- [source-address on page 287](#)
- [source-address \(NTP, RADIUS, System Logging, or TACACS+\) on page 288](#)
- [static \(Protocols 802.1X\) on page 289](#)
- [statistics \(Access Profile\) on page 290](#)
- [supplicant on page 291](#)
- [supplicant-timeout on page 292](#)
- [tacplus on page 293](#)
- [timeout \(System\) on page 294](#)
- [timeout \(Access Control Service\) on page 295](#)
- [timeout \(RADIUS\) on page 296](#)
- [timeout-action \(Access Control Service\) on page 297](#)
- [traceoptions \(802.1X\) on page 298](#)
- [traceoptions \(LLDP\) on page 300](#)
- [transmit-delay on page 302](#)
- [transmit-period on page 303](#)
- [uac-policy on page 303](#)
- [uac-service on page 304](#)
- [unified-access-control on page 305](#)
- [update-interval on page 306](#)

- [vlan-assignment on page 307](#)
- [vlan-nas-port-stacked-format on page 308](#)
- [voip on page 308](#)
- [what on page 309](#)

[\[edit access\]](#) 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 command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see [Feature Explorer](#).

This topic lists:

- [Supported Statements in the \[edit access\] Hierarchy Level on page 169](#)
- [Unsupported Statements in the \[edit access\] Hierarchy Level on page 171](#)

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 percentage;
    abated-utilization-v6 percentage;
    high-utilization percentage;
    high-utilization-v6 percentage;
    pool pool-name {
      family inet {
        dhcp-attributes {
          boot-file filename;
          boot-server hostname;
          domain-name domain-name;
          grace-period seconds;
          maximum-lease-time (seconds | infinite);
          name-server {
            address;
          }
        }
        netbios-node-type (b-node | h-node | m-node | p-node);
        option option-index (array (byte | flag | integer | ip-address | short | string |
          unsigned-integer | unsigned-short) [ type-values ] | byte 8-bit-value |
          flag (false | off | on | true) | integer signed-32-bit-value | ip-address address |
          short signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
          unsigned-short 16-bit-value);
        router {

```

```

        address;
    }
    server-identifier ipv4-address;
    tftp-server hostname;
    wins-server {
        address;
    }
}
host hostname {
    hardware-address mac-address;
    ip-address ip-address;
}
network ip-prefix </prefix-length>;
range name {
    high upper-limit;
    low lower-limit;
}
}
link pool-name;
}
}
address-pool pool-name {
    address address-or-prefix;
    address-range <low lower-limit > <high upper-limit>;
}
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);
    }
}
authentication-order (Access Profile) (ldap | password | radius);
client client-name {
    chap-secret chap-secret;
    firewall-user {
        password password;
    }
    no-rfc2486;
    pap-password password;
}
radius {
    accounting-server server-address;
    attributes {
        exclude [exclude-options];
        ignore [ignore-options];
    }
    authentication-server server-address;
}
radius-options {
    revert-interval interval;
}
session-options {

```

```

        client-idle-timeout minutes;
        client-session-timeout minutes;
    }
    radius-options {
        revert-interval interval;
    }
    radius-server server-address {
        port port-number;
        retry attempts;
        routing-instance instance-name;
        secret password;
        source-address address;
        timeout minutes;
    }
}

```

Unsupported Statements in the [edit access] Hierarchy Level

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

Table 23: Unsupported [edit access] Configuration Statements on EX Series Switches

Statement	Hierarchy Level
NOTE: Variables, such as <i>filename</i> , are not shown in the statements or hierarchies.	
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]

Table 23: Unsupported [edit access] Configuration Statements on EX Series Switches (*continued*)

Statement	Hierarchy Level
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]
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 41](#)
 - [Configuring 802.1X RADIUS Accounting \(CLI Procedure\) on page 130](#)
 - [Security Features for EX Series Switches Overview on page 3](#)

[edit ethernet-switching-options] Configuration Statement Hierarchy on EX Series Switches

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

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

This topic lists:

- [Supported Statements in the \[edit ethernet-switching-options\] Hierarchy Level on page 173](#)
- [Unsupported Statements in the \[edit ethernet-switching-options\] Hierarchy Level on page 175](#)

Supported Statements in the [edit ethernet-switching-options] Hierarchy Level

The following hierarchy shows the **[edit ethernet-switching-options]** configuration statements supported on EX Series switches:

```
ethernet-switching-options {
  analyzer (Port Mirroring) {
    name {
      input {
        egress {
          interface (all | interface-name);
        }
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
      }
    }
    loss-priority priority;
    output {
      interface interface-name;
      vlan (vlan-id | vlan-name);
    }
    ratio number;
  }
}
authentication-whitelist {
  interface;
  vlan-assignment;
}
bpdu-block {
  disable-timeout timeout;
  interface (all | [interface-name]) {
    (disable | drop | shutdown);
  }
}
dot1q-tunneling {
  ether-type (0x8100 | 0x88a8 | 0x9100);
}
interfaces interface-name {
  no-mac-learning;
}
mac-lookup-length number-of-entries;
}
mac-notification {
  notification-interval seconds;
}
}
mac-table-aging-time seconds;
port-error-disable {
```

```

        disable-timeout timeout;
    }
    redundant-trunk-group {
        group name {
            description;
            interface interface-name {
                primary;
            }
            preempt-cutover-timer seconds;
        }
    }
    secure-access-port {
        dhcp-snooping-file {
            location local_pathname | remote_URL;
            timeout seconds;
            write-interval seconds;
        }
        interface (all | interface-name) {
            allowed-mac {
                mac-address-list;
            }
            (dhcp-trusted | no-dhcp-trusted );
            fcoe-trusted;
            mac-limit limit action action;
            no-allowed-mac-log;
            static-ip ip-address {
                mac mac-address;
                vlan vlan-name;
            }
        }
    }
    uac-policy;
}
vlan (all | vlan-name) {
    (arp-inspection | no-arp-inspection );
    dhcp-option82 {
        disable;
        circuit-id {
            prefix hostname;
            use-interface-description;
            use-vlan-id;
        }
        remote-id {
            prefix (hostname | mac | none);
            use-interface-description;
            use-string string;
        }
        vendor-id [string];
    }
    (examine-dhcp | no-examine-dhcp);
    examine-fip {
        fc-map fc-map-value;
    }
    (ip-source-guard | no-ip-source-guard);
    mac-move-limit limit action action;
}
}

```

```

static {
    vlan vlan-id {
        mac mac-address next-hop interface-name;
    }
}
storm-control {
    action-shutdown;
    interface (all | interface-name) {
        bandwidth bandwidth;
        multicast;
        no-broadcast;
        no-multicast;
        no-registered-multicast;
        no-unknown-unicast;
        no-unregistered-multicast;
    }
}
traceoptions {
    file filename <files number> <no-stamp> <replace> <size size> <world-readable |
        no-world-readable>;
    flag flag <disable>;
}
unknown-unicast-forwarding {
    vlan (all | vlan-name) {
        interface interface-name;
    }
}
voip {
    interface (all | [interface-name | access-ports]) {
        forwarding-class (assured-forwarding | best-effort | expedited-forwarding |
            network-control);
        vlan vlan-name;
    }
}
}

```

Unsupported Statements in the [edit ethernet-switching-options] Hierarchy Level

All statements in the [edit ethernet-switching-options] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

Related Documentation

- *Example: Setting Up Q-in-Q Tunneling on EX Series Switches*
- *Example: Configuring Redundant Trunk Links for Faster Recovery*
- *Configuring MAC Table Aging (CLI Procedure)*
- *Configuring MAC Notification (CLI Procedure)*
- *Configuring Q-in-Q Tunneling (CLI Procedure)*
- *Configuring Redundant Trunk Links for Faster Recovery (CLI Procedure)*
- *Configuring Nonstop Bridging on EX Series Switches (CLI Procedure)*

[\[edit protocols\]](#) Configuration Statement Hierarchy on EX Series Switches

Each of the following topics lists the statements at a subhierarchy of the **[edit protocols]** hierarchy:

- [\[edit protocols bfd\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols bgp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols connections\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols dcbx\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols dot1x\]](#) Configuration Statement Hierarchy on EX Series Switches on page 177
- [\[edit protocols igmp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols igmp-snooping\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols isis\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols lacp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols link-management\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols lldp\]](#) Configuration Statement Hierarchy on EX Series Switches on page 179
- [\[edit protocols lldp-med\]](#) Configuration Statement Hierarchy on EX Series Switches on page 180
- [\[edit protocols mld\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols mld-snooping\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols mpls\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols msdp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols mstp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols mvrp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols neighbor-discovery\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols oam\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols ospf\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols ospf3\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols pim\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols rip\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols ripng\]](#) Configuration Statement Hierarchy on EX Series Switches

- [\[edit protocols router-advertisement\] Configuration Statement Hierarchy on EX Series Switches](#)
- [\[edit protocols router-discovery\] Configuration Statement Hierarchy on EX Series Switches](#)
- [\[edit protocols rstp\] Configuration Statement Hierarchy on EX Series Switches](#)
- [\[edit protocols rsvp\] Configuration Statement Hierarchy on EX Series Switches](#)
- [\[edit protocols sflow\] Configuration Statement Hierarchy on EX Series Switches](#)
- [\[edit protocols stp\] Configuration Statement Hierarchy on EX Series Switches](#)
- [\[edit protocols uplink-failure-detection\] Configuration Statement Hierarchy on EX Series Switches](#)
- [\[edit protocols vrrp\] Configuration Statement Hierarchy on EX Series Switches](#)
- [\[edit protocols vstp\] Configuration Statement Hierarchy on EX Series Switches](#)

**Related
Documentation**

- [EX Series Switch Software Features Overview](#)
- [EX Series Virtual Chassis Software Features 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 177](#)
- [Unsupported Statements in the \[edit protocols dot1x\] Hierarchy Level on page 178](#)

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);
      }
    }
  }
}
```


- [Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 75](#)
- [802.1X for EX Series Switches Overview on page 7](#)
- [\[edit protocols\] Configuration Statement Hierarchy on EX Series Switches on page 176](#)

[\[edit protocols lldp\] Configuration Statement Hierarchy on EX Series Switches](#)

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

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

This topic lists:

- [Supported Statements in the \[edit protocols lldp\] Hierarchy Level on page 179](#)
- [Unsupported Statements in the \[edit protocols lldp\] Hierarchy Level on page 180](#)

Supported Statements in the **[edit protocols lldp]** Hierarchy Level

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

```
protocols {
  lldp {
    advertisement-interval seconds;
    disable;
    hold-multiplier seconds;
    interface (all | interface-name) {
      disable;
      power-negotiation {
        disable;
      }
    }
  }
  lldp-configuration-notification-interval seconds;
  management-address;
  netbios-snooping;
  ptopo-configuration-maximum-hold-time seconds;
  ptopo-configuration-trap-interval seconds;
  traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
      no-world-readable>;
    flag flag <disable>;
  }
}
```

```
        transmit-delay seconds;  
    }  
}
```

Unsupported Statements in the [edit protocols lldp] Hierarchy Level

All statements in the **[edit protocols lldp]** hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

Related Documentation

- [\[edit protocols\] Configuration Statement Hierarchy on EX Series Switches on page 176](#)

[edit protocols lldp-med] Configuration Statement Hierarchy on EX Series Switches

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

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

This topic lists:

- [Supported Statements in the \[edit protocols lldp-med\] Hierarchy Level on page 180](#)
- [Unsupported Statements in the \[edit protocols lldp-med\] Hierarchy Level on page 181](#)

Supported Statements in the [edit protocols lldp-med] Hierarchy Level

The following hierarchy shows the **[edit protocols lldp-med]** configuration statements supported on EX Series switches:

```
protocols {  
  lldp-med {  
    disable;  
    fast-start number;  
    interface (all | interface-name) {  
      disable;  
      location {  
        civic-based {  
          ca-type {  
            index {  
              ca-value value;  
            }  
          }  
        }  
        country-code code;  
        what value;  
      }  
    }  
  }  
}
```

```
elin number;  
}  
}  
}
```

Unsupported Statements in the [edit protocols lldp-med] Hierarchy Level

All statements in the [edit protocols lldp-med] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

Related Documentation

- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56](#)
- [show lldp on page 344](#)
- [Configuring LLDP-MED \(CLI Procedure\) on page 140](#)
- [\[edit protocols\] Configuration Statement Hierarchy on EX Series Switches on page 176](#)

access

Syntax	<pre> access { address-assignment pool <i>pool-name</i> address-pool <i>pool-name</i> profile <i>profile-name</i> { accounting (Access Profile) { accounting-stop-on-access-deny; accounting-stop-on-failure; (authentication-order (Access Profile) (ldap radius none); order (radius none); } radius { accounting-server [<i>server-addresses</i>]; authentication-server [<i>server-addresses</i>]; } } } </pre>
Hierarchy Level	[edit]
Release Information	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p>
Description	<p>Configure authentication, authorization, and accounting (AAA) services.</p> <p>The statements are explained separately.</p>
	<div>  <p>NOTE: The [edit access] hierarchy is not available on QFabric systems.</p> </div>
Default	Not enabled
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 130

accounting (Access Profile)

Syntax	<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>
Hierarchy Level	[edit access profile <i>profile-name</i>]
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p>
Description	<p>Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i> • <i>Configuring Per-Subscriber Session Accounting</i> • <i>Understanding RADIUS Accounting Duplicate Reporting</i>

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-port (RADIUS Server)

Syntax	accounting-port <i>port-number</i> ;
Hierarchy Level	[edit system accounting destination radius <i>server</i> <i>server-address</i>], [edit system <i>radius-server</i> <i>server-address</i>]
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 14.1X53-D20 for the OCX Series.
Description	Configure the accounting port number on which to contact the RADIUS server.
Options	<i>number</i> —Port number on which to contact the RADIUS server. Default: 1813
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Authentication</i>• <i>Configuring RADIUS System Accounting</i>

accounting-port

Syntax	<code>accounting-port <i>port-number</i>;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
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.

Options	<i>port-number</i> —Port number on which to contact the RADIUS accounting server. Most RADIUS servers use port 1813, as specified in RFC 2866. Default: 1813
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring RADIUS System Accounting</i>• <i>Configuring Router or Switch Interaction with RADIUS Servers</i>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>• <i>Configuring RADIUS Authentication for L2TP</i>

accounting-server

Syntax	<code>accounting-server[server-addresses];</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Description	Configure the Remote Authentication Dial-In User Service (RADIUS) server for authentication. To configure multiple RADIUS servers, include multiple server addresses. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.
Default	Not enabled
Options	<i>server-addresses</i> —One or more addresses of RADIUS authentication servers.



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

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • show network-access aaa statistics authentication on page 362 • Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41 • Understanding 802.1X and RADIUS Accounting on EX Series Switches on page 16 • Understanding RADIUS Accounting

accounting-session-id-format

Syntax	accounting-session-id-format (decimal description);
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
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 format the router or switch uses to identify the accounting session.
Default	decimal
Options	decimal —Use the decimal format. description —Use the generic format, in the form: jnpr <i>interface-specifier:subscriber-session-id</i> .
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Options for Subscriber Access</i>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

accounting-stop-on-access-deny


Syntax	accounting-stop-on-access-deny;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Description	Configure the authentication order for authentication, authorization, and accounting (AAA) services to send an Acct-Stop message if the AAA server denies access to a supplicant.



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

Default	Not enabled
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41 • Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 130 • show network-access aaa statistics authentication on page 362 • Configuring RADIUS Accounting

accounting-stop-on-failure

Syntax	accounting-stop-on-failure;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Description	Configure authentication order for authentication, authorization, and accounting (AAA) services to send an Acct-Stop message if a supplicant fails AAA authorization, but the RADIUS server grants access. For example, a supplicant might fail AAA authentication because of an internal error such as a timeout.
<div> NOTE: The [edit access] hierarchy is not available on QFabric switches.</div>	
Default	Not enabled
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41• Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 130• Understanding 802.1X and RADIUS Accounting on EX Series Switches on page 16• Configuring RADIUS Accounting• Understanding RADIUS Accounting

address (Access Address Pool)

Syntax	<code>address <i>address-or-prefix</i>;</code>
Hierarchy Level	[edit access address-pool <i>pool-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the IP address or prefix value for clients.
Options	<i>address-or-prefix</i> —An address or prefix value.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the Address Pool for L2TP Network Server IP Address Allocation

address (Access Control Service)

Syntax	<code>address <i>ip-address</i>;</code>
Hierarchy Level	[edit services unified-access-control infranet-controller]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Specify the address through which the switch will connect to the Junos Pulse Access Control Service.
Options	<i>ip-address</i> —Specify the IP address of the NAC device.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 157

address-pool

Syntax	<pre>address-pool <i>pool-name</i> { address <i>address-or-prefix</i>; address-range <low <i>lower-limit</i>> <high <i>upper-limit</i>>; }</pre>
Hierarchy Level	[edit access]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Allocate IP addresses for clients.



NOTE: This statement is not supported for L2TP LNS on MX Series routers.

Options	<p><i>pool-name</i>—Name assigned to an address pool.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the Address Pool for L2TP Network Server IP Address Allocation</i>

address-range

Syntax	<pre>address-range <low <i>lower-limit</i>> <high <i>upper-limit</i>>;</pre>
Hierarchy Level	[edit access address-pool <i>pool-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the address range.
Options	<ul style="list-style-type: none">• high <i>upper-limit</i>—Upper limit of an address range.• low <i>lower-limit</i>—Lower limit of an address range.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the Address Pool for L2TP Network Server IP Address Allocation</i>

advertisement-interval

Syntax	<code>advertisement-interval seconds;</code>
Hierarchy Level	[edit protocols lldp], [edit routing-instances <i>routing-instance-name</i> protocols lldp]
Release Information	Statement introduced in Junos OS Release 9.6 for MX Series and T Series routers. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Description	(MX Series and T Series routers only) Configure an interval for LLDP advertisement.
Options	seconds —Interval between LLDP advertisement. Default: 30 Range: 5 through 32768
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring LLDP</i> • show lldp on page 344 • Configuring LLDP (CLI Procedure) on page 136 • Understanding LLDP and LLDP-MED on EX Series Switches on page 18 • transmit-delay on page 302 • <i>Understanding LLDP</i>

attributes

Syntax	<pre>attributes { exclude { ... } ignore { framed-ip-netmask; input-filter; logical-system-routing-instance; output-filter; } }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i> radius]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Specify how the router or switch processes RADIUS attributes. 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	<ul style="list-style-type: none">• <i>Configuring How RADIUS Attributes Are Used for Subscriber Access</i>

authentication-order (Access Profile)

Syntax	authentication-order [(none ldap password radius secureid)];
Hierarchy Level	[edit access profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	(EX and QFX Series only) Configure the order of authentication, authorization, and accounting (AAA) methods to use while sending authentication messages.
Default	Not enabled
Options	<p>none—No authentication for specified subscribers.</p> <p>ldap—Lightweight Directory Access Protocol.</p> <p>password—Locally configured password in access profile.</p> <p>radius—RADIUS authentication.</p> <p>secureid—RSA SecurID authentication.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41 • Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 130

authentication-order (Authenticator)

Syntax	<code>authentication-order [dot1x mac-radius captive-portal];</code>
Hierarchy Level	[edit protocols <code>dot1x authenticator interface interface-name</code>]
Release Information	Statement introduced in Junos OS Release 15.1R3 for EX Series switches.
Description	<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 authentication-order 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 [mac-radius dot1x], 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 interface all 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 10](#)
- [Configuring Flexible Authentication Order on page 147](#)

authentication-profile-name

Syntax	authentication-profile-name <i>access-profile-name</i> ;
Hierarchy Level	[edit protocols dot1x authenticator], [edit services captive-portal]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Added to [edit services captive-portal] hierarchy in Junos OS Release 10.1 for EX Series switches.
Description	Specify the name of the access profile to be used for 802.1X, MAC RADIUS, or captive portal authentication.
Default	No access profile is specified.
Options	<i>access-profile-name</i> —Name of the access profile. The access profile is configured at the [edit access profile] hierarchy level and contains the RADIUS server IP address and other information used for authentication.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41• Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 85• Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102• Configuring 802.1X Interface Settings (CLI Procedure) on page 126• Configuring 802.1X Authentication (J-Web Procedure) on page 127• Configuring Captive Portal Authentication (CLI Procedure) on page 151

authentication-protocol

Syntax	authentication-protocol (eap-md5 pap);
Hierarchy Level	[edit protocols dot1x authenticator interface <i>interface-name</i> 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	<p>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.</p> <p>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.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Authentication on EX Series Switches on page 10 • Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 130

authentication-server

Syntax	<code>authentication-server [<i>server-addresses</i>];</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Description	Configure the RADIUS server for authentication. To configure multiple RADIUS servers, include multiple server addresses. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.
Options	<i>server-addresses</i> —Configure one or more RADIUS server addresses.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41• show network-access aaa statistics authentication on page 362

authentication-whitelist

Syntax	<pre>authentication-whitelist { mac-address { interface <i>interface-name</i>; vlan-assignment (<i>vlan-id</i> <i>vlan-name</i>); } }</pre>
Hierarchy Level	<pre>[edit ethernet-switching-options]; [edit switch-options]</pre>
Release Information	<p>Statement introduced in Junos OS Release 10.1 for EX Series switches.</p> <p>The [edit switch-options] hierarchy level was introduced in Junos OS Release 13.2X50-D10 for EX Series switches (ELS).</p>
Description	<p>Configure MAC addresses for which RADIUS authentication is to be bypassed.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102 • Example: Setting Up Captive Portal Authentication on an EX Series Switch • Configuring Captive Portal Authentication (CLI Procedure) on page 151 • Configuring Captive Portal Authentication (CLI Procedure)

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 {
        interface interface-names;
        static mac-address;
    }
    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 statements are explained separately.



NOTE: You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.

Default No static MAC address or VLAN is configured.

Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring 802.1X Interface Settings (CLI Procedure) on page 126 • Specifying RADIUS Server Connections on an EX Series Switch (CLI Procedure) on page 150 • Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 75

block-interval

Syntax	<code>block-interval <i>block-interval</i>;</code>
Hierarchy Level	[edit protocols dot1x authenticator interface (all [<i>interface-names</i>]) server-reject-vlan (<i>vlan-id</i> <i>vlan-name</i>)], [edit protocols dot1x authenticator interface (all [<i>interface-names</i>]) server-reject-vlan]
Release Information	Statement introduced in Junos OS Release 11.2 for EX Series switches.
Description	Specify the amount of time that the 802.1X interface ignores Extensible Authentication Protocol (EAP) start messages from the client when an EAPoL block has been enabled on the 802.1X interface.
Options	<i>block-interval</i> —The number of seconds for the interval. Range: 120 through 65,535
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • eapol-block on page 218 • Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 107

ca-type

Syntax	<pre>ca-type { number { ca-value value; } }</pre>
Hierarchy Level	[edit protocols lldp-med interface (all <i>interface-name</i> location civic-based)]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>For Link Layer Discovery Protocol–Media Endpoint Device (LLDP-MED), configure the address elements. These elements are included in the location information to be advertised from the switch to the MED. This information is used during emergency calls to identify the location of the MED.</p> <p>For further information about the values that can be used to comprise the location,, refer to RFC 4776, <i>Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information</i>. A subset of those values is provided below.</p> <p>The ca-value statement is explained separately.</p>
Default	Disabled.
Options	<p>value—Civic address elements that represent the civic or postal address. Values are:</p> <ul style="list-style-type: none">• 0—A code that specifies the language used to describe the location.• 16—The leading-street direction, such as “N”.• 17—A trailing street suffix, such as “SW”.• 18—A street suffix or type, such as “Ave” or “Platz”.• 19—A house number, such as “6450”.• 20—A house-number suffix, such as “A” or “1/2”.• 21—A landmark, such as “Stanford University”.• 22—Additional location information, such as “South Wing”.• 23—The name and occupant of a location, such as “Carrillo's Holiday Market”.• 24—A house-number suffix, such as “95684”.• 25—A building structure, such as “East Library”.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• show lldp on page 344

- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56](#)
- [Configuring LLDP-MED \(CLI Procedure\) on page 140](#)

ca-value

Syntax	<code>ca-value <i>value</i>;</code>
Hierarchy Level	<code>[edit protocols lldp-med interface (all <i>interface-name</i>) location civic-based ca-type <i>number</i>]</code>
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For Link Layer Discovery Protocol–Media Endpoint Device (LLDP-MED), configure location information, such as street address and city, that is indexed by the ca-type code. This information is advertised from the switch to the MED and is used during emergency calls to identify the location of the MED.
Default	Disabled.
Options	<i>value</i> —Specify a value that correlates to the ca-type . See ca-type for a list of codes and suggested values.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • show lldp on page 344 • Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56 • Configuring LLDP-MED (CLI Procedure) on page 140

captive-portal

Syntax	<pre> captive-portal { authentication-profile-name authentication-profile-name custom-options { banner-message string; footer-bgcolor color; footer-message string; footer-text-color color; form-header-bgcolor color; form-header-message string; form-header-text-color color; form-reset-label label name; form-submit-label label name; header-bgcolor color; header-logo filename; header-message string; header-text-color color; post-authentication-url url-string; } interface (all [interface-names]) { quiet-period seconds; retries number-of-retries; server-timeout seconds; session-expiry seconds; supplicant (multiple single single-secure); } secure-authentication (http https); } </pre>
Hierarchy Level	[edit services]
Release Information	Statement introduced in Junos OS Release 10.1 for EX Series switches.
Description	<p>Configure captive portal to authenticate clients connected to the switch for access to the network.</p> <p>The remaining statements are explained separately.</p>
Default	Captive portal is disabled.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102 • Designing a Captive Portal Authentication Login Page on an EX Series Switch on page 153 • Configuring Captive Portal Authentication (CLI Procedure) on page 151 • Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 157

- [Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service \(CLI Procedure\) on page 159](#)

certificate-verification

Syntax	certificate-verification (optional required warning);
Hierarchy Level	[edit services unified-access-control]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Specify certificate verification requirement for the connection from the switch to Junos Pulse Access Control service.
Default	warning
Options	<p>optional—The specification of a security certificate is optional.</p> <p>required—The specification of a security certificate is required.</p>



NOTE: Do not specify this option in Junos OS Release 12.2 for EX Series switches, because the specification of a security certificate ([ca-profile](#)) is not supported in this release.

warning—A warning is issue if a security certificate is not specified. Default.

Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 157 • Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 159 • Understanding Centralized Network Access Control and EX Series Switches on page 33

civic-based

Syntax	<pre>civic-based { what number; country-code code; ca-type { number { ca-value value; } } }</pre>
Hierarchy Level	[edit protocols lldp-med interface (all <i>interface-name</i>) location]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>For Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED), configure the geographic location to be advertised from the switch to the MED. This information is used during emergency calls to identify the location of the MED.</p> <p>The statements are explained separately.</p>
Default	Disabled.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• show lldp on page 344• Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56• Configuring LLDP-MED (CLI Procedure) on page 140

country-code

Syntax	<code>country-code code;</code>
Hierarchy Level	[edit protocols lldp-med (Ethernet Switching) interface (LLDP-MED) (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For Link Layer Discovery Protocol—Media Endpoint Device (LLDP-MED), configure the two-letter country code to include in the location information. Location information is advertised from the switch to the MED, and is used during emergency calls to identify the location of the MED. The country code is required when configuring LLDP-MED based on location.
Default	Disabled.
Options	code —Two-letter ISO 3166 country code in capital ASCII letters; for example, US or DE.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • show lldp on page 344 • Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56 • Configuring LLDP-MED (CLI Procedure) on page 140

custom-options

Syntax custom-options {
 banner-message *string*;
 footer-bgcolor *color*;
 footer-message *string*;
 footer-text-color *color*;
 form-header-bgcolor *color*;
 form-header-message *string*;
 form-header-text-color *color*;
 form-reset-label *label name*;
 form-submit-label *label name*;
 header-bgcolor *color*;
 header-logo *filename*;
 header-message *string*;
 header-text-color *color*;
 post-authentication-url *url-string*;
}

Hierarchy Level [edit services [captive-portal](#)]

Release Information Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description Specify the design elements of a captive portal login page.

Options **banner-message**—The first screen displayed before the captive portal login page is displayed—for example, a disclaimer message.

Range: 1–2047 characters

footer-bgcolor —The hexadecimal color code for the color of the footer bar across the bottom of the captive portal login page—for example, #2E8B57 (sea green).

Values: # symbol followed by six characters.

footer-message—Text message displayed in the footer bar across the bottom of the captive portal login page.

Range: 1–2047 characters

Default: Copyright ©2010, Juniper Networks Inc.

footer-text-color — Color of the text in the footer.

Default: The default color is white.

form-header-bgcolor —The hexadecimal color code for the background color of the header bar across the top of the form area of the captive portal login page.

Values: # symbol followed by six characters.

form-header-message—Text message displayed in the header bar across the top of the form area of the captive portal login page.

Range: 1–255 characters

Default: Captive Portal User Authentication

form-header-text-color—Color of the text in the form header.

Default: The default color is black.

form-reset-label—Label displayed in the button that the user can select to clear the username and password fields on the form.

Range: 1–255 characters

Default: Reset

form-submit-label —Label displayed in the button that the user selects to submit their login information—for example, **Log In** .

Range: 1–255 characters

Default: Log In

header-bgcolor—The hexadecimal color code for the color of the header bar across the top of the captive portal login page.

Values: # symbol followed by six characters.

header-logo—Filename of the file containing the image of the logo displayed at the top of the captive portal login page. The image file can be in GIF, JPEG, or PNG format.

Default: The Juniper Networks logo

header-message—Text displayed in the header bar across the bottom of the captive portal login page.

Range: 1–2047 characters

Default: User Authentication

header-text-color—Color of the text in the header.

Default: The default color is white.

post-authentication-url—URL to which the users are directed upon successful authentication—for example **www.mycafe.com**.

Range: 1–255 characters

Default: The page originally requested by the user.

**Required Privilege
Level**

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

**Related
Documentation**

- [Designing a Captive Portal Authentication Login Page on an EX Series Switch on page 153](#)
- [Configuring Captive Portal Authentication \(CLI Procedure\) on page 151](#)

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*

disable (802.1X)

Syntax	disable;
Hierarchy Level	[edit protocols dot1x authenticator interface (all [<i>interface-names</i>])]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Disable 802.1X authentication on a specified interface or all interfaces.
Default	802.1X authentication is disabled on all interfaces.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • show dot1x on page 331 • Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 50 • Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 45 • Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56 • Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 75 • Configuring 802.1X Interface Settings (CLI Procedure) on page 126 • Configuring 802.1X Authentication (J-Web Procedure) on page 127

disable (LLDP)

Syntax	disable;
Hierarchy Level	[edit protocols lldp], [edit protocols interface lldp]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Disable the LLDP configuration on the switch or on one or more interfaces.
Default	If you do not configure LLDP, it is disabled on the switch and on specific switch interfaces.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• show lldp on page 344• Configuring LLDP (CLI Procedure) on page 136• Understanding LLDP and LLDP-MED on EX Series Switches on page 18• <i>Configuring LLDP</i>• <i>Understanding LLDP</i>

disable (LLDP-MED)

Syntax	disable;
Hierarchy Level	[edit protocols lldp-med], [edit protocols lldp-med interface]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Disable the LLDP-MED configuration on the switch or on one or more interfaces.
Default	If you do not configure LLDP-MED, it is disabled on the switch and on specific switch interfaces.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• show lldp on page 344• Configuring LLDP (CLI Procedure) on page 136• Understanding LLDP and LLDP-MED on EX Series Switches on page 18

disable (LLDP Power Negotiation)

Syntax	disable;
Hierarchy Level	[edit protocols lldp interface (all <i>interface-name</i>) power-negotiation]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Disable Link Layer Discovery Protocol (LLDP) power negotiation, which negotiates with Power over Ethernet (PoE)-powered devices to allocate power.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring LLDP (CLI Procedure) on page 136• Configuring PoE on EX Series Switches (CLI Procedure)

dot1x

```
Syntax  dot1x {
        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 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;
            static mac-address {
                interface interface-names;
                vlan-assignment (vlan-id | vlan-name);
            }
        }
    }
```

Hierarchy Level [edit protocols]

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

Description Configure 802.1X authentication for Port-Based Network Access Control. 802.1X authentication is supported on interfaces that are members of private VLANs (PVLANS).

The remaining statements are explained separately.

Default 802.1X is disabled.

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

Related Documentation

- [show dot1x on page 331](#)
- [Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 50](#)

- [Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 45](#)
- [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56](#)
- [Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 75](#)
- [Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 85](#)
- [Configuring RADIUS Server Fail Fallback \(CLI Procedure\) on page 144](#)


elin

Syntax	<code>elin <i>number</i>;</code>
Hierarchy Level	<code>[edit protocols lldp-med (Ethernet Switching) interface (LLDP-MED) (all <i>interface-name</i> location (LLDP-MED))]</code>
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For Link Layer Discovery Protocol—Media Endpoint Discovery (LLDP-MED), configure the Emergency Line Identification Number (ELIN) as location information. Location information is advertised from the switch to the MED device and is used during emergency calls to identify the location of the MED device.
Default	Disabled.
Options	<i>number</i> —Configure a 10-digit number (area code and telephone number).
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • show lldp on page 344 • Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56 • Configuring LLDP-MED (CLI Procedure) on page 140

eapol-block

Syntax	eapol-block;
Hierarchy Level	[edit protocols dot1x authenticator interface (802.1X) (all [<i>interface-names</i>]) server-reject-vlan], [edit protocols dot1x authenticator interface (all [<i>interface-names</i>]) server-reject-vlan (<i>vlan-id</i> <i>vlan-name</i>)]
Release Information	Statement introduced in Junos OS Release 11.2 for EX Series switches.
Description	Enable an EAPoL block that causes the 802.1X interface to ignore Extensible Authentication Protocol (EAP) start messages from the client, which are attempts to restart the authentication procedure. When the 802.1X interface ignores the EAP start messages from the client, the switch allows the existing session that was established through the server-reject VLAN to remain open.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• block-interval on page 203• Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 107

ethernet-port-type-virtual

Syntax	ethernet-port-type-virtual;
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Specify the physical port type the router or switch uses to authenticate clients. The router or switch passes a port type of ethernet in RADIUS attribute 61 (NAS-Port-Type) by default. This statement specifies a port type of virtual .
<div> NOTE: This statement takes precedence over the nas-port-type statement if you include both statements in the same access profile.</div>	
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access• Configuring RADIUS Server Parameters for Subscriber Access

ethernet-switching-options

```

Syntax ethernet-switching-options {
    analyzer (Port Mirroring) {
        name {
            loss-priority priority;
            ratio number;
            input {
                ingress {
                    interface (all | interface-name);
                    vlan (vlan-id | vlan-name);
                }
                egress {
                    interface (all | interface-name);
                }
            }
        }
        output {
            interface interface-name;
            vlan (vlan-id | vlan-name) {
                no-tag;
            }
        }
    }
    bpdu-block {
        disable-timeout timeout;
        interface (all | [interface-name]) {
            (disable | drop | shutdown);
        }
    }
    dot1q-tunneling {
        ether-type (0x8100 | 0x88a8 | 0x9100);
    }
    interfaces interface-name {
        no-mac-learning;
    }
    mac-lookup-length number-of-entries;
}
    mac-notification {
        notification-interval seconds;
    }
    mac-table-aging-time seconds;
    nonstop-bridging;
    port-error-disable {
        disable-timeout timeout;
    }
    redundant-trunk-group {
        group name {
            interface interface-name <primary>;
            interface interface-name;
        }
    }
    secure-access-port {
        dhcp-snooping-file {

```

```

    location local_pathname | remote_URL;
    timeout seconds;
    write-interval seconds;
}
dhcpv6-snooping-file {
    location local_pathname | remote_URL;
    timeout seconds;
    write-interval seconds;
}
interface (all | interface-name) {
    allowed-mac {
        mac-address-list;
    }
    (dhcp-trusted | no-dhcp-trusted);
    fcoe-trusted;
    mac-limit limit action (drop | log | none | shutdown);
    no-allowed-mac-log;
    persistent-learning;
    static-ip ip-address {
        vlan vlan-name;
        mac mac-address;
    }
    static-ipv6 ip-address {
        vlan vlan-name;
        mac mac-address;
    }
}
vlan (all | vlan-name) {
    (arp-inspection | no-arp-inspection) [
        forwarding-class class-name;
    ]
    dhcp-option82 {
        circuit-id {
            prefix hostname;
            use-interface-description;
            use-vlan-id;
        }
        remote-id {
            prefix hostname | mac | none;
            use-interface-description;
            use-string string;
        }
        vendor-id [string];
    }
    (examine-dhcp | no-examine-dhcp) {
        forwarding-class class-name;
    }
    (examine-dhcpv6 | no-examine-dhcpv6) {
        forwarding-class class-name;
    }
    examine-fip {
        fc-map fc-map-value;
    }
    (ip-source-guard | no-ip-source-guard);
    (ipv6-source-guard | no-ipv6-source-guard);
    mac-move-limit limit action (drop | log | none | shutdown);

```

```

    }
    (neighbor-discovery-inspection | no-neighbor-discovery-inspection);
no-option-37;
static {
    vlan name {
        mac mac-address {
            next-hop interface-name;
        }
    }
}
storm-control {
    action-shutdown;
    interface (all | interface-name) {
        bandwidth bandwidth;
        level level;
        multicast;
        no-broadcast;
        no-multicast;
        no-registered-multicast;
        no-unknown-unicast;
        no-unregistered-multicast;
    }
}
traceoptions {
    file filename <files number> <no-stamp> <replace> <size size> <world-readable |
        no-world-readable>;
    flag flag <disable>;
}
unknown-unicast-forwarding {
    vlan (all | vlan-name) {
        interface interface-name;
    }
}
}
voip {
    interface (all | [interface-name | access-ports]) {
        vlan vlan-name;
        forwarding-class (assured-forwarding | best-effort | expedited-forwarding |
            network-control);
    }
}
}
}

```

Hierarchy Level [edit]

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

Description Configure Ethernet switching options.

The remaining statements are explained separately.

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

Related Documentation	<ul style="list-style-type: none">• <i>Understanding Port Mirroring on EX Series Switches</i>• <i>Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity</i>• <i>Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches</i>• <i>Understanding Redundant Trunk Links</i>• <i>Understanding Storm Control on EX Series Switches</i>• Understanding 802.1X and VoIP on EX Series Switches on page 21• <i>Understanding Q-in-Q Tunneling on EX Series Switches</i>• <i>Understanding Unknown Unicast Forwarding</i>• <i>Understanding MAC Notification on EX Series Switches</i>• <i>Understanding FIP Snooping</i>• <i>Understanding Nonstop Bridging on EX Series Switches</i>
------------------------------	---

events

Syntax	<code>events [events];</code>
Hierarchy Level	[edit system accounting]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the types of events to track and log.
Options	events —Event types; can be one or more of the following: <ul style="list-style-type: none">• change-log—Audit configuration changes.• interactive-commands—Audit interactive commands (any command-line input).• login—Audit logins.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring TACACS+ System Accounting</i>

exclude (RADIUS)

```
Syntax  exclude {
    acc-aggr-cir-id-asc [ access-request | accounting-start | accounting-stop ];
    acc-aggr-cir-id-bin [ access-request | accounting-start | accounting-stop ];
    acc-loop-cir-id [ access-request | accounting-start | accounting-stop ];
    accounting-authentic [ accounting-on | accounting-off ];
    accounting-delay-time [ accounting-on | accounting-off ];
    accounting-session-id [ access-request | accounting-on | accounting-off | accounting-stop
    ];
    accounting-terminate-cause [ accounting-off ];
    acct-tunnel-connection [ accounting-start | accounting-stop ];
    act-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    act-data-rate-up [ access-request | accounting-start | accounting-stop ];
    act-interlv-delay-dn [ access-request | accounting-start | accounting-stop ];
    act-interlv-delay-up [ access-request | accounting-start | accounting-stop ];
    att-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    att-data-rate-up [ access-request | accounting-start | accounting-stop ];
    called-station-id [ access-request | accounting-start | accounting-stop ];
    calling-station-id [ access-request | accounting-start | accounting-stop ];
    chap-challenge [ access-request ];
    chargeable-user-identity [ access-request ];
    class [ accounting-start | accounting-stop ];
    cos-shaping-rate [ accounting-start | accounting-stop ];
    dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
    dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
    dhcp-options [ access-request | accounting-start | accounting-stop ];
    downstream-calculated-qos-rate [ access-request | accounting-start | accounting-stop
    ];
    dsl-forum-attributes [ access-request | accounting-start | accounting-stop ];
    dsl-line-state [ access-request | accounting-start | accounting-stop ];
    dsl-type [ access-request | accounting-start | accounting-stop ];
    event-timestamp [ accounting-on | accounting-off | accounting-start | accounting-stop
    ];
    filter-id [ accounting-start | accounting-stop ];
    framed-ip-address [ accounting-start | accounting-stop ];
    framed-ip-netmask [ accounting-start | accounting-stop ];
    input-filter [ accounting-start | accounting-stop ];
    input-gigapackets [ accounting-stop ];
    input-gigawords [ accounting-stop ];
    interface-description [ access-request | accounting-start | accounting-stop ];
    l2tp-rx-connect-speed [ access-request | accounting-start | accounting-stop ];
    l2tp-tx-connect-speed [ access-request | accounting-start | accounting-stop ];
    max-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    max-data-rate-up [ access-request | accounting-start | accounting-stop ];
    max-interlv-delay-dn [ access-request | accounting-start | accounting-stop ];
    max-interlv-delay-up [ access-request | accounting-start | accounting-stop ];
    min-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    min-data-rate-up [ access-request | accounting-start | accounting-stop ];
    min-lp-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    min-lp-data-rate-up [ access-request | accounting-start | accounting-stop ];
    nas-identifier [ access-request | accounting-on | accounting-off | accounting-start |
    accounting-stop ];
    nas-port [ access-request | accounting-start | accounting-stop ];
```

```
nas-port-id [ access-request | accounting-start | accounting-stop ];
nas-port-type [ access-request | accounting-start | accounting-stop ];
output-filter [ accounting-start | accounting-stop ];
output-gigapackets [ accounting-stop ];
output-gigawords [ accounting-stop ];
pppoe-description [ access-request | accounting-start | accounting-stop ];
tunnel-assignment-id [ accounting-start | accounting-stop ];
tunnel-client-auth-id [ accounting-start | accounting-stop ];
tunnel-client-endpoint [ accounting-start | accounting-stop ];
tunnel-medium-type [ accounting-start | accounting-stop ];
tunnel-server-auth-id [ accounting-start | accounting-stop ];
tunnel-server-endpoint [ accounting-start | accounting-stop ];
tunnel-type [ accounting-start | accounting-stop ];
upstream-calculated-qos-rate [ access-request | accounting-start | accounting-stop ];
virtual-router [ access-request | accounting-start | accounting-stop ];
}
```

Hierarchy Level [edit access profile *profile-name* radius [attributes](#)]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
downstream-calculated-qos-rate, **dsl-forum-attributes**, and **upstream-calculated-qos-rate**
Options introduced in Junos OS Release 11.4.
cos-shaping-rate and **filter-id** Options introduced in Junos OS Release 13.2.
virtual-router Option introduced in Junos OS Release 14.1X51.
pppoe-description Option introduced in Junos OS Release 14.2.

Description Configure the router or switch to exclude the specified attributes from the specified type of RADIUS message.

Not all attributes are available in all types of RADIUS messages. By default, the router or switch includes the specified attributes in RADIUS Access-Request, Acct-On, Acct-Off, Acct-Start, and Acct-Stop messages.

Options RADIUS attribute type—RADIUS attribute or Juniper Networks VSA number and name.

- **acc-aggr-cir-id-asc**—Juniper Networks VSA 26-112, Acc-Aggr-Cir-Id-Asc.
- **accounting-delay-time**—RADIUS attribute 41, Acct-Delay-Time.
- **accounting-session-id**—RADIUS attribute 44, Acct-Session-Id.
- **accounting-terminate-cause**—RADIUS attribute 49, Acct-Terminate-Cause.
- **acct-tunnel-connection**—RADIUS attribute 68, Acct-Tunnel-Connection.
- **act-data-rate-dn**—Juniper Networks VSA 26-114, Act-Data-Rate-Dn
- **act-data-rate-up**—Juniper Networks VSA 26-113, Act-Data-Rate-Up
- **act-interlv-delay-dn**—Juniper Networks VSA 26-126, Act-Interlv-Delay-Dn
- **act-interlv-delay-up**—Juniper Networks VSA 26-124, Act-Interlv-Delay-Up
- **att-data-rate-dn**—Juniper Networks VSA 26-118, Att-Data-Rate-Dn
- **att-data-rate-up**—Juniper Networks VSA 26-117, Att-Data-Rate-Up
- **called-station-id**—RADIUS attribute 30, Called-Station-Id.
- **calling-station-id**—RADIUS attribute 31, Calling-Station-Id.
- **chap-challenge**—RADIUS attribute 60, CHAP-Challenge.
- **chargeable-user-identity**—RADIUS attribute 89, Chargeable-User-Identity.
- **class**—RADIUS attribute 25, Class.
- **cos-shaping-rate**—Juniper Networks VSA 26-177, Cos-Shaping-Rate.
- **dhcp-gi-address**—Juniper Networks VSA 26-57, DHCP-GI-Address.
- **dhcp-mac-address**—Juniper Networks VSA 26-56, DHCP-MAC-Address.
- **dhcp-mac-address**—Juniper VSA 26-56, DHCP-MAC-Address.
- **dhcp-options**—Juniper VSA 26-55, DHCP-Options.
- **downstream-calculated-qos-rate**—Juniper VSA 26-141
- **dsl-forum-attributes**—DSL Forum VSA as described in RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*
- **dsl-type**—Juniper Networks VSA 26-128, DSL-Type
- **event-timestamp**—RADIUS attribute 55, Event-Timestamp.
- **filter-id**—RADIUS attribute 11, Filter-Id.
- **framed-ip-address**—RADIUS attribute 8, Framed-IP-Address.
- **framed-ip-netmask**—RADIUS attribute 9, Framed-IP-Netmask.
- **input-filter**—Juniper Networks VSA 26-10, Ingress-Policy-Name.
- **input-gigapackets**—Juniper Networks VSA 26-42, Acct-Input-Gigapackets.
- **input-gigawords**—RADIUS attribute 52, Acct-Input-Gigawords.

- **interface-description**—Juniper Networks VSA 26-53, Interface-Desc.
- **l2tp-rx-connect-speed**—Juniper Networks VSA 26-163, Rx-Connect-Speed
- **l2tp-tx-connect-speed**—Juniper Networks VSA 26-162, Tx-Connect-Speed
- **max-data-rate-dn**—Juniper Networks VSA 26-120, Max-Data-Rate-Dn
- **max-data-rate-up**—Juniper Networks VSA 26-119, Max-Data-Rate-Up
- **max-interlv-delay-dn**—Juniper Networks VSA 26-125, Max-Interlv-Delay-Dn
- **framed-ip-address**—RADIUS attribute 8, Framed-IP-Address.
- **framed-ip-netmask**—RADIUS attribute 9, Framed-IP-Netmask.
- **input-filter**—Juniper VSA 26-10, Ingress-Policy-Name.
- **input-gigapackets**—Juniper VSA 26-42, Acct-Input-Gigapackets.
- **input-gigawords**—RADIUS attribute 52, Acct-Input-Gigawords.
- **interface-description**—Juniper VSA 26-53, Interface-Desc.
- **nas-identifier**—RADIUS attribute 32, NAS-Identifier.
- **nas-port**—RADIUS attribute 5, NAS-Port.
- **nas-port-id**—RADIUS attribute 87, NAS-Port-Id.
- **nas-port-type**—RADIUS attribute 61, NAS-Port-Type.
- **output-filter**—Juniper VSA 26-11, Egress-Policy-Name.
- **output-gigapackets**—Juniper VSA 25-43, Acct-Output-Gigapackets.
- **output-gigawords**—RADIUS attribute 53, Acct-Output-Gigawords.
- **tunnel-assignment-id**—RADIUS attribute 82, Tunnel-Assignment-ID.
- **tunnel-client-auth-id**—RADIUS attribute 90, Tunnel-Client-Auth-ID.
- **tunnel-client-endpoint**—RADIUS attribute 66, Tunnel-Client-Endpoint.
- **tunnel-medium-type**—RADIUS attribute 65, Tunnel-Medium-Type.
- **tunnel-server-auth-id**—RADIUS attribute 91, Tunnel-Server-Auth-ID.
- **tunnel-server-endpoint**—RADIUS attribute 67, Tunnel-Server-Endpoint.
- **tunnel-type**—RADIUS attribute 64, Tunnel-Type.
- **upstream-calculated-qos-rate**—Juniper Networks VSA 26-142

RADIUS message type

- **access-request**—RADIUS Access-Accept messages.
- **accounting-off**—RADIUS Accounting-Off messages.
- **accounting-on**—RADIUS Accounting-On messages.
- **accounting-start**—RADIUS Accounting-Start messages.
- **accounting-stop**—RADIUS Accounting-Stop messages.

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring How RADIUS Attributes Are Used for Subscriber Access</i>• <i>Configuring RADIUS Server Parameters for Subscriber Access</i>

fast-start (LLDP-MED)

Syntax	fast-start <i>count</i> ;
Hierarchy Level	[edit protocols lldp-med]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the number of Link Layer Discovery Protocol—Media Endpoint Discovery (LLDP-MED) advertisements sent from the switch in the first second after it has detected an LLDP-MED device (such as an IP telephone).
Options	count —Number of advertisements. Range: 1 through 10 Default: 3
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• show lldp on page 344• Configuring LLDP-MED (CLI Procedure) on page 140• Understanding LLDP and LLDP-MED on EX Series Switches on page 18

forwarding-class (VoIP)

Syntax	forwarding-class < assured-forwarding best-effort expedited-forwarding network-control >;
Hierarchy Level	[edit ethernet-switching-options voip interface <all <i>interface-name</i> access-ports>] [edit switch-options voip interface <all <i>interface-name</i> access-ports>]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For EX Series switches, configure the forwarding class used to handle packets on the VoIP interface.
Default	Disabled.
Options	<i>class</i> —Forwarding class: <ul style="list-style-type: none">• assured-forwarding—Assured forwarding (AF)—Provides a group of values you can define and includes four subclasses: AF1, AF2, AF3, and AF4, each with three drop probabilities: low, medium, and high.• best-effort—Provides no service profile. For the best effort forwarding class, loss priority is typically not carried in a class-of-service (CoS) value, and random early detection (RED) drop profiles are more aggressive.• expedited-forwarding—Provides a low loss, low latency, low jitter, assured bandwidth, end-to-end service.• network-control—Provides a typically high priority because it supports protocol control.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56• Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication on page 68• Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 64

guest-vlan

Syntax	<code>guest-vlan (vlan-id vlan-name);</code>
Hierarchy Level	[edit protocols dot1x authenticator interface (all [<i>interface-names</i>])]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the VLAN to which an interface is moved when no 802.1X supplicants are connected on the interface. The VLAN specified must already exist on the switch.
Default	None
Options	<p><i>vlan-id</i>—VLAN tag identifier of the guest VLAN.</p> <p><i>vlan-name</i>—Name of the guest VLAN.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 45 • Understanding Guest VLANs for 802.1X on EX Series Switches on page 16

hold-multiplier

Syntax	<code>hold-multiplier <i>number</i>;</code>
Hierarchy Level	[edit protocols lldp]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. Statement introduced in Junos OS Release 11.1 for QFX Series.
Description	Specify the multiplier used in combination with the advertisement-interval value to determine the length of time LLDP information is held before it is discarded. The default value is 4 (or 120 seconds).
Default	Disabled.
Options	<i>number</i> —A number used as a multiplier. Range: 2 through 10 Default: 4 (or 120 seconds)
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• show lldp on page 344• Configuring LLDP (CLI Procedure) on page 136• Understanding LLDP and LLDP-MED on EX Series Switches on page 18• Configuring LLDP• Understanding LLDP

ignore

Syntax	<pre>ignore { dynamic-iflset-name; framed-ip-netmask; input-filter; logical-system-routing-instance; output-filter; }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i> radius attributes]
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p>
Description	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.
Options	<p>dynamic-iflset-name—Ignore Interface-Set/Dynamic-Ifset-Name (VSA 26-130).</p> <p>framed-ip-netmask—Ignore Framed-IP-Netmask (RADIUS attribute 9).</p> <p>input-filter—Ignore Ingress-Policy-Name (VSA 26-10).</p> <p>logical-system-routing-instance—Ignore Virtual-Router (VSA 26-1).</p> <p>output-filter—Ignore Egress-Policy-Name (VSA 26-11).</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring How RADIUS Attributes Are Used for Subscriber Access</i> • <i>Configuring RADIUS Server Parameters for Subscriber Access</i>

immediate-update

Syntax	<code>immediate-update;</code>
Hierarchy Level	<code>[edit access profile <i>profile-name</i> accounting]</code>
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 router or switch to send an Acct-Update message to the RADIUS accounting server on receipt of a response (for example, an ACK or timeout) to the Acct-Start message.
Required Privilege Level	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Parameters for Subscriber Access• Configuring Per-Subscriber Session Accounting

infranet-controller

Syntax	<pre>infranet-controller <i>hostname</i> { address <i>ip-address</i>; interface <i>interface-name</i>; password <i>password</i>; port <i>port-number</i>; }</pre>
Hierarchy Level	<code>[edit services unified-access-control]</code>
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Configure the switch's connection to the Junos Pulse Access Control Service network access control (NAC) device. The remaining statements are explained separately.
Required Privilege Level	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 157• Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 159

interface (802.1X)

Syntax	<pre> interface (all [<i>interface-names</i>]) { disable; guest-vlan (<i>vlan-name</i> <i>vlan-id</i>); lldp-med-bypass; mac-radius <restrict>; maximum-requests <i>number</i>; no-reauthentication; quiet-period <i>seconds</i>; reauthentication { interval <i>seconds</i>; } retries <i>number</i>; server-fail (deny permit use-cache <i>vlan-id</i> <i>vlan-name</i>); server-reject-vlan (<i>vlan-id</i> <i>vlan-name</i>) { eapol-block; block-interval <i>block-interval</i>; } server-timeout <i>seconds</i>; supplicant (single single-secure multiple); supplicant-timeout <i>seconds</i>; transmit-period <i>seconds</i>; } </pre>
Hierarchy Level	[edit protocols dot1x authenticator]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure 802.1X authentication for Port-Based Network Access Control for all interfaces or for specific interfaces.
Options	<p>all—Configure all interfaces for 802.1X authentication.</p> <p>[<i>interface-names</i>]— List of names of interfaces to configure for 802.1X authentication.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • show dot1x on page 331 • Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 50 • Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 45 • Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56 • Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 85

- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 126](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\) on page 127](#)


interface (Access Control Service)

Syntax	<code>interface <i>interface-name</i>;</code>
Hierarchy Level	[edit services unified-access-control infranet-controller]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Specify the interface through which the switch will connect to the Junos Pulse Access Control Service.
Options	<i>interface-name</i> —Name of the interface that will connect the switch to the Access Control Service.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 157• Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 159

interface (Captive Portal)

Syntax	<pre>interface (all [<i>interface-names</i>]) { quiet-period <i>seconds</i>; retries <i>number-of-retries</i>; server-timeout <i>seconds</i>; session-expiry <i>seconds</i>; supplicant (multiple single single-secure); }</pre>
Hierarchy Level	[edit services captive-portal]
Release Information	Statement introduced in Junos OS Release 10.1 for EX Series switches.
Description	Configure captive portal authentication for all interfaces or for specific interfaces.
Options	<p>all—All interfaces to be configured for captive portal authentication.</p> <p>[<i>interface-names</i>]—List of names of interfaces to be configured for captive portal authentication.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing—control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102 • Configuring Captive Portal Authentication (CLI Procedure) on page 151

interface (LLDP)

Syntax	<pre>interface (all <i>interface-name</i>) { disable; power-negotiation { disable; } }</pre>
Hierarchy Level	[edit protocols lldp]
Release Information	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
Description	Configure Link Layer Discovery Protocol (LLDP) on all interfaces or on a specific interface.
<div>  <p>NOTE: On EX4300 switches, LLDP cannot be configured on the me0 or vme interface. Issuing the command <code>set protocols lldp interface me0</code> generates the following error message:</p> <pre>error: name: 'me0': Invalid interface error: statement creation failed: interface</pre> <p>Issuing the command <code>set protocols lldp interface vme</code> generates the following error message:</p> <pre>error: name: 'vme': Invalid interface error: statement creation failed: interface</pre> </div>	
Default	None
Options	<p>all—All interfaces on the switch.</p> <p><i>interface-name</i>—Name of a specific interface.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring LLDP (CLI Procedure) on page 136 • Understanding LLDP and LLDP-MED on EX Series Switches on page 18 • Configuring LLDP • Understanding LLDP

interface (LLDP-MED)

Syntax	<pre> interface (all <i>interface-name</i>) { disable; location (LLDP-MED) { elin <i>number</i>; civic-based { what <i>number</i>; country-code <i>code</i>; ca-type { number { ca-value <i>value</i>; } } } } } </pre>
Hierarchy Level	[edit protocols lldp-med (Ethernet Switching)]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) on all interfaces or on a specific interface.
Default	Not enabled
Options	<p>all—All interfaces on the switch.</p> <p><i>interface-name</i>—Name of a specific interface.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • show lldp on page 344 • Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56 • Configuring LLDP-MED (CLI Procedure) on page 140 • Understanding LLDP and LLDP-MED on EX Series Switches on page 18

interface (Static MAC Bypass)

Syntax	<code>interface [<i>interface-names</i>];</code>
Hierarchy Level	[edit protocols dot1x authenticator authentication-profile-name static mac-address], [edit ethernet-switching-options authentication-whitelist mac-address], [edit switch-options authentication-whitelist mac-address]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement added to the [edit ethernet-switching-options authentication-whitelist] hierarchy in Junos OS Release 10.1 for EX Series switches. Statement added to the [edit switch-options authentication-whitelist] hierarchy in Junos OS Release 13.2X50-D10 for EX Series switches (ELS).
Description	Configure interfaces on which the specified MAC addresses are allowed to bypass RADIUS authentication and allowed to connect to the LAN without authentication.
Options	<i>interface-names</i> —List of interfaces.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• show dot1x static-mac-address on page 338• Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 75• Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102• Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102• Configuring Captive Portal Authentication (CLI Procedure) on page 151

interface (VoIP)

Syntax	<pre>interface (all [<i>interface-name</i>] access-ports) { vlan <i>vlan-name</i> ; forwarding-class <assured-forwarding best-effort expedited-forwarding network-control>; }</pre>
Hierarchy Level	<ul style="list-style-type: none"> For platforms with ELS: [edit switch-options voip] For platforms without ELS: [edit ethernet-switching-options voip],
Release Information	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>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.)</p>
Description	Enable voice over IP (VoIP) on interfaces.
Options	<p>all—Enable VoIP on all interfaces.</p> <p>interface-name—Enable VoIP on a specific interface.</p> <p>all—(Switches without ELS only) Enable VoIP on all access ports.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56 Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication on page 68 Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 64

interface-description-format

Syntax	<pre>interface-description-format { exclude-adapter; exclude-sub-interface; }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches. Options exclude-adapter and exclude-sub-interface introduced in Junos OS Release 10.4.
Description	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.
Options	exclude-adapter —Exclude the adapter from the interface description. exclude-sub-interface —Exclude the subinterface from the interface description.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Options for Subscriber Access</i>• <i>RADIUS Server Options for Subscriber Access</i>

interval (Access Control Service)

Syntax	<code>interval seconds;</code>
Hierarchy Level	[edit services unified-access-control]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Configure the time between continuity check messages for the switch's connection with the Junos Pulse Access Control Service. The specified value must be less than the value specified for timeout .
Options	seconds —Time between continuity check messages, in seconds. Range: 1 through 9999 seconds Default: 30 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 157• Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 159

lldp

```
Syntax  lldp {
    advertisement-interval seconds;
    disable;
    hold-multiplier number;
    interface (all | [interface-name]) {
        disable;
        power-negotiation {
            disable;
        }
    }
    lldp-configuration-notification-interval seconds;
    management-address ip-management-address;
    netbios-snooping;
    no-tagging;
    ptopo-configuration-maximum-hold-time seconds;
    ptopo-configuration-trap-interval seconds;
    traceoptions {
        file filename <files number> <size size> <world-readable | no-world-readable>
        <no-stamp> <replace>;
        flag flag <disable>;
    }
    transmit-delay seconds;
}
```

Hierarchy Level [edit protocols]

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

Description Configure Link Layer Discovery Protocol (LLDP). The switch uses LLDP to advertise its identity and capabilities on a LAN, as well as to receive information about other network devices. LLDP is defined in the IEEE standard 802.1AB-2005.

The remaining statements are explained separately.



NOTE: The `transmit-delay` and `netbios-snooping` options are not available on QFabric systems.



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

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

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

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

.....

Default LLDP is enabled.

The following statements have default values:

- **advertisement-interval**—The default value is 30 seconds. The allowable range is from 5 through 32768 seconds.
- **hold-multiplier**—The default values is 4. The allowable range is from 2 through 10.
- **ptopo-configuration-maximum-hold-time**—The default value is 300 seconds. The allowable range is from 1 through 2147483647 seconds.
- **transmit-delay**—The default values is 2 seconds. The allowable range is from 1 through 8192 seconds.

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

Related Documentation

- [show lldp on page 344](#)
- [Configuring LLDP \(CLI Procedure\) on page 136](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 18](#)
- [Configuring LLDP](#)
- [Understanding LLDP](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 18](#)

lldp-configuration-notification-interval

Syntax	lldp-configuration-notification-interval <i>seconds</i> ;
Hierarchy Level	[edit protocols lldp]
Release Information	Statement introduced in Junos OS Release 9.6 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Specify how often SNMP trap notifications are generated as a result of LLDP database changes. If the interval value is 0, trap notifications of database changes are disabled.
Default	SNMP trap notifications of LLDP database changes are disabled.
Options	seconds —Interval between trap notifications about LLDP database changes. Range: 0 through 3600
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• show lldp on page 344

lldp-med (Ethernet Switching)

Syntax	<pre> lldp-med { disable; fast-start number; interface (all interface-name) { disable; location { elin number; civic-based { what number; country-code code; ca-type { number { ca-value value; } } } } } } </pre>
Hierarchy Level	[edit protocols]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<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>
Default	Disabled.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • show lldp on page 344 • Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56 • Configuring LLDP-MED (CLI Procedure) on page 140

lldp-med-bypass

Syntax	lldp-med-bypass;
Hierarchy Level	[edit protocols dot1x authenticator interface (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 12.3 for EX Series switches.
Description	Bypass the 802.1X authentication procedure for connecting multiple LLDP-MED end devices. Automatically add the learned MAC addresses of the end devices to the switch's static MAC bypass list, and allow the devices to access the network. You can enable lldp-med-bypass only when the interface is also configured for 802.1X authentication of <i>multiple</i> supplicants.
Default	Disabled
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• supplicant on page 291• Understanding Authentication on EX Series Switches on page 10

lldp-priority

Syntax	lldp-priority;
Hierarchy Level	[edit poe], [edit poe fpc (all <i>slot-number</i>)]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Configure the switch to assign interfaces the power priority provided by the powered device by using Link Layer Discovery Protocol (LLDP) power negotiation rather than the power priority configured on the switch interface.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring PoE on EX Series Switches (CLI Procedure)

location (LLDP-MED)

Syntax	<pre>location { elin number; civic-based { what number; country-code code; ca-type{ number { ca-value value; } } } }</pre>
Hierarchy Level	[edit protocols lldp-med interface (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>For Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED), configure the location information. Location information is advertised from the switch to the MED. This information is used during emergency calls to identify the location of the MED.</p> <p>The statements are explained separately.</p>
Default	Disabled.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • show lldp on page 344 • Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56 • Configuring LLDP-MED (CLI Procedure) on page 140

mac-radius

Syntax	<code>mac-radius <flap-on-disconnect> <restrict>;</code>
Hierarchy Level	[edit protocols dot1x authenticator interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.3 for EX Series switches. Option flap-on-disconnect introduced in Junos OS Release 9.4 for EX Series switches.
Description	<p>Configure MAC RADIUS authentication for specific interfaces. MAC RADIUS authentication allows LAN access to permitted MAC addresses. When a new MAC address appears on an interface, the switch consults the RADIUS server to check whether the MAC address is a permitted address. If the MAC address is configured on the RADIUS server, the device is allowed access to the LAN.</p> <p>If MAC RADIUS is configured, the switch first tries to get a response from the host for 802.1X authentication. If the host is unresponsive, the switch attempts to authenticate using MAC RADIUS.</p> <p>To restrict authentication to MAC RADIUS only, use the restrict option. In restrictive mode, all 802.1X packets are eliminated and the attached device on the interface is considered a nonresponsive host.</p>
Options	<p>flap-on-disconnect—(Optional) When the RADIUS server sends a disconnect message to a supplicant, the switch resets the interface on which the supplicant is authenticated. If the interface is configured for multiple supplicant mode, the switch resets all the supplicants on the specified interface. This option takes effect only when the restrict option is also set.</p> <p>restrict—(Optional) Restricts authentication to MAC RADIUS only. When mac-radius restrict is configured the switch drops all 802.1X packets. This option is useful when no other 802.1X authentication methods, such as guest VLAN, are needed on the interface, and eliminates the delay that occurs while the switch determines that a connected device is a non-802.1X-enabled host.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• show dot1x on page 331• Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 85• Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 50• Configuring MAC RADIUS Authentication (CLI Procedure) on page 146• Configuring 802.1X Interface Settings (CLI Procedure) on page 126• Understanding Authentication on EX Series Switches on page 10

management-address

Syntax	<code>management-address <i>ip-management-address</i>;</code>
Hierarchy Level	[edit protocols lldp]
Release Information	Statement introduced in Junos OS Release 9.5 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Specify the management address to be used in LLDP Management Address type, length, and value (TLV) messages. The Management Address TLV typically contains the IPv4 or IPv6 management addresses of the local system. Only out-of-band management addresses must be used for the management-address. Other remote managers can use this address to obtain information related to the local device.
Default	The LLDP Management Address TLV uses the IP address of the switch's management Ethernet interface (me0), or the IP address of the virtual management Ethernet (VME) interface if the switch is a Virtual Chassis member.
Options	<i>ip-management-address</i> —You can specify either an IPv4 or an IPv6 management address for the switch.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • show lldp on page 344 • Understanding LLDP and LLDP-MED on EX Series Switches on page 18 • EX Series Switches Interfaces Overview • Understanding LLDP

maximum-requests

Syntax	<code>maximum-requests <i>number</i>;</code>
Hierarchy Level	<code>[edit protocols dot1x authenticator interface (all [<i>interface-names</i>])]</code>
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For 802.1X authentication, configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out.
Default	Two retransmission attempts
Options	<i>number</i> —Number of retransmission attempts. Range: 1 through 10 Default: 2
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring 802.1X Interface Settings (CLI Procedure) on page 126• Configuring 802.1X Authentication (J-Web Procedure) on page 127

nas-identifier

Syntax	<code>nas-identifier <i>identifier-value</i>;</code>
Hierarchy Level	<code>[edit access profile <i>profile-name</i> radius options]</code>
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 value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests.
Options	<i>identifier-value</i> —String to use for authentication and accounting requests. Range: 1 through 64 characters
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access• Configuring RADIUS Server Parameters for Subscriber Access

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.

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Options for Subscriber Access</i>• <i>Configuring RADIUS Server Parameters for Subscriber Access</i>

netbios-snooping

Syntax	netbios-snooping;
Hierarchy Level	[edit protocols lldp]
Release Information	Statement introduced in Junos OS Release 11.1 for EX Series switches.
Description	Enable NetBIOS snooping on the switch.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring NetBIOS Snooping (CLI Procedure) on page 156

no-mac-table-binding (802.1X)

Syntax	no-mac-table-binding;
Hierarchy Level	[edit protocols dot1x authenticator]
Release Information	Statement introduced in Junos OS Release 11.1 for EX Series switches.
Description	For 802.1X authentication, disable the removal of the session from the authentication session table when the MAC address ages out of the Ethernet switching table.
Default	Not enabled
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Controlling Authentication Session Timeouts (CLI Procedure) on page 155

no-reauthentication

Syntax	no-reauthentication;
Hierarchy Level	[edit protocols dot1x authenticator interface (802.1X) (all [<i>interface-names</i>])]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For 802.1X authentication, disables reauthentication.
Default	Not disabled
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring 802.1X Interface Settings (CLI Procedure) on page 126 • Configuring 802.1X Authentication (J-Web Procedure) on page 127 • Understanding Authentication on EX Series Switches on page 10

no-tagging

Syntax	no-tagging;
Hierarchy Level	[edit protocols lldp]
Release Information	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Configure the switch to send LLDPDUs without including VLAN tags on interfaces for which VLAN tagging is enabled (tagged interfaces).
Default	Interfaces for which VLAN tagging is enabled include a VLAN tag (tag 0) in LLDPDUs if the no-tagging option is not configured.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Understanding LLDP and LLDP-MED on EX Series Switches on page 18

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 *profile-name* **radius**]

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 options used by RADIUS authentication and accounting servers.


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 Options for Subscriber Access*
- *RADIUS Server Options for Subscriber Access*

order

Syntax	<code>order (radius [<i>accounting-order-data-list</i>]);</code>
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Configure the order of authentication, authorization, and accounting (AAA) servers to use while sending accounting messages and updates.
Default	No order specified
Options	radius —RADIUS accounting for specified subscribers. [<i>accounting-order-data-list</i>]— Set of data listing the authentication order to be used, enclosed by brackets. This can be any combination of the authentication methods, up to and including a full list of the entire authentication order.
<div> NOTE: The [edit access] hierarchy is not available on QFabric systems.</div>	
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41• Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 130• Configuring RADIUS Accounting


password (Access Control Service)

Syntax	<code>password password;</code>
Hierarchy Level	<code>[edit services unified-access-control infranet-controller hostname]</code>
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Configure the password to connect the switch to the Junos Pulse Access Control Service network access control (NAC) device. This password must match the password specified on the Access Control Service through its administrative interface.
Options	password —A string of up to 200 alphanumeric characters bounded by quotation marks. Spaces are allowed, but special characters, such as <code>?</code> , are not allowed.
Required Privilege Level	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 157 • Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 159

port

Syntax	<code>port port-number;</code>
Hierarchy Level	<code>[edit access radius-server server-address],</code> <code>[edit access profile profile-name radius-server server-address]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the port number on which to contact the RADIUS server.
Options	port-number —Port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2865)
Required Privilege Level	<code>system</code> —To view this statement in the configuration. <code>system-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Router or Switch Interaction with RADIUS Servers • Configuring Authentication and Accounting Parameters for Subscriber Access

port (Access Control Service)

Syntax	<code>port <i>port-number</i>;</code>
Hierarchy Level	[edit services unified-access-control infranet-controller]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Configure the switch's connection to the security port on the Junos Pulse Access Control Service network access control (NAC) device.
<div> NOTE: Do not change this port setting.</div>	
Options	<code><i>port-number</i></code> —11123
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 157• Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 159

port (RADIUS Server)

Syntax	<code>port port-number;</code>
Hierarchy Level	[edit system radius-server <i>address</i>], [edit system accounting destination radius server <i>address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Configure the port number on which to contact the RADIUS server.
Options	<i>number</i> —Port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2865)



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

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


port (TACACS+ Server)

Syntax	<code>port port-number;</code>
Hierarchy Level	[edit system accounting destination tacplus server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the port number on which to contact the TACACS+ server.
Options	<i>number</i> —Port number on which to contact the TACACS+ server. Default: 49
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring TACACS+ System Accounting</i>

power-negotiation

Syntax	<code>power-negotiation { disable; }</code>
Hierarchy Level	[edit protocols <code>lldp interface</code> (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	<p>Configure Link Layer Discovery Protocol (LLDP) power negotiation, which negotiates with Power over Ethernet (PoE) powered devices to allocate power.</p> <p>LLDP power negotiation requires the PoE management option to be set to class.</p> <p>The remaining statement is explained separately.</p>
Default	LLDP power negotiation is enabled by default when the PoE management option is set to class .
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring LLDP (CLI Procedure) on page 136• Configuring PoE on EX Series Switches (CLI Procedure)

profile

Syntax	<pre> profile <i>profile-name</i> { accounting (Access Profile) { accounting-stop-on-access-deny; accounting-stop-on-failure; order (radius [<i>accounting-order-data-list</i>]); } authentication-order (Access Profile) [<i>authentication-method</i>]; radius { accounting-server [<i>server-addresses</i>]; authentication-server [<i>server-addresses</i>]; } } </pre>
Hierarchy Level	[edit access]
Release Information	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
Description	Configure an access profile. The access profile contains the entire authentication, authorization, and accounting (AAA) configuration that aids in handling AAA requests, including the authentication method and order, AAA server addresses, and AAA accounting.
Default	Not enabled
Options	<p><i>profile-name</i>—Profile name of up to 32 characters.</p> <p>The remaining statements are explained separately.</p>
<div>  NOTE: The [edit access] hierarchy is not available on QFabric systems. </div>	
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41 • Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 130 • Configuring RADIUS Accounting

ptopo-configuration-maximum-hold-time

Syntax	<code>ptopo-configuration-maximum-hold-time <i>seconds</i>;</code>
Hierarchy Level	[edit protocols lldp]
Release Information	Statement introduced in Junos OS Release 9.6 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Configure how long to maintain the physical topology database entries. The physical topology identifies the devices on the network and their physical interconnections.
Options	<i>seconds</i> —Time to maintain physical topology database entries. Default: 300 Range: 1 through 2147483647
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• show lldp on page 344• Understanding LLDP and LLDP-MED on EX Series Switches on page 18• Understanding LLDP

ptopo-configuration-trap-interval

Syntax	<code>ptopo-configuration-trap-interval <i>seconds</i>;</code>
Hierarchy Level	[edit protocols lldp]
Release Information	Statement introduced in Junos OS Release 9.6 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Specify how often SNMP trap notifications are sent regarding changes in physical topology global statistics.
Default	SNMP trap notifications of changes in physical topology global statistics are disabled.
Options	<i>seconds</i> —Interval between SNMP trap notifications about physical topology global statistics. Range: 0 through 3600
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

quiet-period

Syntax	<code>quiet-period seconds;</code>
Hierarchy Level	[edit protocols dot1x authenticator interface (802.1X) (all <i>[interface-names]</i>)]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For 802.1X authentication, configure the number of seconds the interface remains in the wait state following a failed authentication attempt by a supplicant before reattempting authentication.
Default	60 seconds
Options	seconds —Number of seconds the interface remains in the wait state. Range: 0 through 65,535 seconds Default: 60 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • show network-access aaa statistics authentication on page 362 • Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41

quiet-period (Captive Portal)

Syntax	<code>quiet-period seconds;</code>
Hierarchy Level	[edit services captive-portal interface (all <i>interface-names</i>)]
Release Information	Statement introduced in Junos OS Release 10.1 for EX Series switches.
Description	Configure time, in seconds, after a user exceeds the maximum number of retries before they can attempt to authenticate.
Options	seconds —Number of seconds. Range: 1–65535 Default: 60
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102 • Configuring Captive Portal Authentication (CLI Procedure) on page 151

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	<pre>radius { server { server-address { accounting-port port-number; secret password; source-address address; retry number; timeout seconds; } } }</pre>
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	<ul style="list-style-type: none">• <i>Configuring RADIUS System Accounting</i>

radius

Syntax	<pre>radius { accounting-server [server-addresses]; authentication-server [server-addresses]; }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i>]
Release Information	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
Description	<p>Configure the RADIUS servers for authentication and for accounting. To configure multiple RADIUS servers, include multiple radius statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.</p> <p>The statements are explained separately.</p>
<div style="display: flex; align-items: center;">  <div> <p>NOTE: The [edit access] hierarchy is not available on QFabric systems.</p> </div> </div>	
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41 • Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 130 • Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 131 • Configuring RADIUS Accounting

radius-options (Protocols 802.1X)

Syntax	<pre>radius-options { use-vlan-id; use-vlan-name; }</pre>
Hierarchy Level	[edit protocols dot1x authenticator]
Release Information	Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	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.
Options	<p>use-vlan-id—Include the VLAN ID in the packet sent to the RADIUS server to request authentication.</p> <p>use-vlan-name—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>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring 802.1X Interface Settings (CLI Procedure) on page 126• Specifying RADIUS Server Connections on an EX Series Switch (CLI Procedure) on page 150• authenticator on page 202


radius-server

Syntax	<pre>radius-server server-address { accounting-port port-number; accounting-retry number; accounting-timeout seconds; dynamic-request-port; port port-number; preauthentication-port port-number; preauthentication-secret password; retry attempts; routing-instance routing-instance-name; secret password; max-outstanding-requests value; source-address source-address; timeout seconds; }</pre>
Hierarchy Level	<p>[edit access],</p> <p>[edit access profile <i>profile-name</i>]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>dynamic-request-port option added in Junos OS Release 14.2R1 for MX Series routers.</p> <p>preauthentication-port and preauthentication-secret options added in Junos OS Release 14.1X51 for MX Series routers.</p>
Description	<p>Configure RADIUS for subscriber access management, L2TP, or PPP.</p> <p>To configure multiple RADIUS servers, include multiple radius-server statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.</p>
Options	<p>server-address—Address of the RADIUS authentication server.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring RADIUS Authentication for L2TP</i> • <i>Configuring the PPP Authentication Protocol</i> • <i>Configuring RADIUS Server Authentication</i> • <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i> • <i>show network-access aaa statistics</i> • <i>clear network-access aaa statistics</i>

radius-server (System)

Syntax	<pre>radius-server { server-address { accounting-port port-number; port number; retry number; secret password; source-address source-address; timeout seconds; } }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure a RADIUS server for Point-to-Point Protocol (PPP).</p> <p>To configure multiple RADIUS servers, include multiple radius-server statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.</p>
Options	<p>server-address—Address of the RADIUS authentication server.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Authentication</i>

reauthentication

Syntax	<code>reauthentication <i>interval</i>;</code>
Hierarchy Level	[edit protocols <code>dot1x authenticator interface</code> (all [<i>interface-names</i>])]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	The reauthentication statement is used to locally configure the number of seconds before the 802.1X authentication session times out and the client must reattempt authentication.
<div>  <p>NOTE: If the authentication server sends an authentication session timeout to the client, this takes priority over the value configured locally using the reauthentication statement. The session timeout value is sent from the server to the client as an attribute of the RADIUS Access-Accept message.</p> </div>	
Options	<p><i>interval</i>—Sets the periodic reauthentication time interval in seconds.</p> <p>Range: 1 through 4,294,967,296 seconds</p> <p>Default: 3600 seconds</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring 802.1X Interface Settings (CLI Procedure) on page 126

redirect-url

Syntax	<code>redirect-url url;</code>
Hierarchy Level	[edit protocols <code>dot1x authenticator interface interface-name</code>]
Release Information	Statement introduced in Junos OS Release 15.1R3 for EX Series switches.
Description	<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 redirect-url 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 “Configuring Central Web Authentication” on page 160.</p>
Default	Disabled. The redirect URL is not enabled for central Web authentication by default.
Options	<p>url—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">• <code>http://www.example.com</code>• <code>https://www.example.com</code>• <code>http://10.10.10.10</code>• <code>https://10.10.10.10</code>• <code>http://www.example.com/login.html</code>• <code>https://www.example.com/login.html</code>• <code>http://10.10.10.10/login.html</code>• <code>https://10.10.10.10/login.html</code>



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 160](#)

retries

Syntax `retries number;`

Hierarchy Level [edit protocols `dot1x authenticator interface (802.1X)` (all | [*interface-names*])]

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

Description For 802.1X authentication, configure the number of times the switch attempts to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt.

Options *number*—Number of retries.

Default: 3 retries

Range: 1 through 10

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


Related Documentation

- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 126](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\) on page 127](#)
- [Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 107](#)

retries (Captive Portal)

Syntax	<code>retries <i>number-of-tries</i>;</code>
Hierarchy Level	[edit services captive-portal interface (all <i>interface-names</i>)]]
Release Information	Statement introduced in Junos OS Release 10.1 for EX Series switches.
Description	Configure the number of times the user can attempt to submit authentication information.
Options	<i>number-of-tries</i> —Number of authentication attempts by user. Range: 1–65535 Default: 3
Required Privilege Level	routing—To view this statement in the configuration. routing—control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102• Configuring Captive Portal Authentication (CLI Procedure) on page 151

retry

Syntax	<code>retry attempts;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>]; [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
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 <i>accounting-retry</i> statement.
<div>  <p>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.</p> </div>	
Options	<p>attempts—Number of times that the router is allowed to attempt to contact a RADIUS server.</p> <p>Range: 1 through 30</p> <p>Default: 3</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i> • <i>Configuring Router or Switch Interaction with RADIUS Servers</i> • <i>Example: Configuring CHAP Authentication with RADIUS</i> • <i>Configuring RADIUS Authentication for L2TP</i> • timeout on page 296

retry (RADIUS)

Syntax	<code>retry number;</code>
Hierarchy Level	[edit system radius-server server-address], [edit system accounting destination radius server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Number of times the router or switch is allowed to try to contact a RADIUS authentication or accounting server.
Options	<i>number</i> —Number of retries allowed for contacting a RADIUS server. Range: 1 through 10 Default: 3
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Authentication</i>• <i>Configuring RADIUS System Accounting</i>• timeout on page 294

revert-interval

Syntax	<code>revert-interval <i>interval</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]; [edit access radius-options]
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 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.
Options	<i>interval</i> —Amount of time to wait. Range: 0 through 604,800 seconds Default: 60 seconds
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring RADIUS Server Options for Subscriber Access</i> • <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

routing-instance

Syntax	<code>routing-instance <i>routing-instance-name</i>;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the routing instance used to send RADIUS packets to the RADIUS server.
Options	<i>routing-instance-name</i> —Routing instance name.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring the PPP Authentication Protocol</i> • <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

secret

Syntax	<code>secret password;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius-server <i>server-address</i>], [edit access radius-disconnect <i>client-address</i>], [edit access radius-server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the password to use with the RADIUS server. The secret password used by the local router or switch must match that used by the server.
Options	password —Password to use; it can include spaces if the character string is enclosed in quotation marks.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>• <i>Configuring Router or Switch Interaction with RADIUS Servers</i>• <i>Example: Configuring CHAP Authentication with RADIUS</i>• <i>Configuring RADIUS Authentication for L2TP</i>• <i>Configuring the RADIUS Disconnect Server for L2TP</i>

secret

Syntax	<code>secret password;</code>
Hierarchy Level	[edit system accounting destination radius server <i>server-address</i>], [edit system accounting destination tacplus server <i>server-address</i>], [edit system radius-server <i>server-address</i>], [edit system tacplus-server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the password to use with the RADIUS or TACACS+ server. The secret password used by the local router or switch must match that used by the server.
Options	<i>password</i> —Password to use; can include spaces included in quotation marks.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring RADIUS Server Authentication • Configuring TACACS+ Authentication • Configuring TACACS+ System Accounting • Configuring RADIUS System Accounting

secure-authentication

Syntax	<code>secure-authentication (http https);</code>
Hierarchy Level	[edit services captive-portal]
Release Information	Statement introduced in Junos OS Release 10.1 for EX Series switches.
Description	Enable HTTP or HTTPS access on the captive portal interface.
Default	<code>http</code>
Options	<p><code>http</code>—Enables HTTP access on the captive portal interface.</p> <p><code>https</code>—Enables HTTPS access on the captive portal interface. HTTPS is recommended.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102 • Configuring Captive Portal Authentication (CLI Procedure) on page 151

server (RADIUS Accounting)

Syntax	<pre>server { server-address { accounting-port port-number; retry number secret password; source-address address; timeout seconds; } }</pre>
Hierarchy Level	[edit system accounting destination radius]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for the source-address-inet6 statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Configure RADIUS logging. 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	<ul style="list-style-type: none">• <i>Configuring RADIUS System Accounting</i>

server (TACACS+ Accounting)

Syntax server {
 server-address {
 port port-number;
 secret password;
 single-connection;
 timeout seconds;
 }
 }

Hierarchy Level [edit system accounting destination tacplus]

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

Description Configure TACACS+ logging.

 The remaining statements are explained separately.

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

Related Documentation • *Configuring TACACS+ System Accounting*

server-fail

Syntax	<code>server-fail (deny permit use-cache <i>vlan-id</i> <i>vlan-name</i>);</code>
Hierarchy Level	[edit protocols dot1x authenticator interface (802.1X) (all [<i>interface-names</i>])]
Release Information	Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	<p>For EX Series switches configured for 802.1X authentication, specify the server fail fallback action the switch takes when all RADIUS authentication servers are unreachable.</p> <p>When you specify the action <i>vlan-name</i> or <i>vlan-id</i>, the VLAN must already be configured on the switch.</p>
Default	Authentication is denied.
Options	<p>deny—Force fail the supplicant authentication. No traffic will flow through the interface.</p> <p>permit—Force succeed the supplicant authentication. Traffic will flow through the interface as if it were successfully authenticated by the RADIUS server.</p> <p>use-cache—Force succeed the supplicant authentication only if it was previously authenticated successfully. This action ensures that already authenticated supplicants are not affected.</p> <p>vlan-id—Move supplicant on the interface to the VLAN specified by this numeric identifier. This action is allowed only if it is the first supplicant connecting to the interface. If an authenticated supplicant is already connected, then the supplicant is not moved to the VLAN and is not authenticated.</p> <p>vlan-name—Move supplicant on the interface to the VLAN specified by this name. This action is allowed only if it is the first supplicant connecting to an interface. If an authenticated supplicant is already connected, then the supplicant is not moved to the VLAN and is not authenticated.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• show dot1x on page 331• Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 79• Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41• Configuring RADIUS Server Fail Fallback (CLI Procedure) on page 144• Understanding Server Fail Fallback and Authentication on EX Series Switches on page 28

server-reject-vlan

Syntax	<pre>server-reject-vlan (vlan-id vlan-name) { eapol-block; block-interval block-interval; }</pre>
Hierarchy Level	[edit protocols dot1x authenticator interface (802.1X) (all [<i>interface-names</i>])]
Release Information	Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	<p>For EX Series switches configured for 802.1X authentication, specify that when the switch receives an Extensible Authentication Protocol Over LAN (EAPoL) Access-Reject message during the authentication process between the switch and the RADIUS authentication server, supplicants attempting access to the LAN are granted access and moved to a specific VLAN. Any VLAN name or VLAN ID sent by a RADIUS server as part of the EAPoL Access-Reject message is ignored.</p> <p>When you specify the VLAN ID or VLAN name, the VLAN must already be configured on the switch.</p> <p>The remaining statements are explained separately.</p>
Default	None
Options	<p><i>vlan-id</i>—Numeric identifier of the VLAN to which the supplicant is moved.</p> <p><i>vlan-name</i>—Name of the VLAN to which the supplicant is moved.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • show dot1x on page 331 • Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41 • Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients • Configuring RADIUS Server Fail Fallback (CLI Procedure) on page 144 • Understanding Server Fail Fallback and Authentication on EX Series Switches on page 28


server-timeout

Syntax	<code>server-timeout <i>seconds</i>;</code>
Hierarchy Level	[edit protocols dot1x authenticator interface (802.1X) (all [<i>interface-name</i>])
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For 802.1X authentication, configure the amount of time a port will wait for a reply when relaying a response from the supplicant to the authentication server before timing out and invoking the server-fail action.
Default	30 seconds
Options	<i>seconds</i> —Number of seconds. Range: 1 through 60 seconds Default: 30 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• show dot1x on page 331• clear dot1x on page 320• Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41• 802.1X for EX Series Switches Overview on page 7

server-timeout (Captive Portal)

Syntax	<code>server-timeout <i>seconds</i>;</code>
Hierarchy Level	[edit services captive-portal interface (all <i>interface-names</i>)]]
Release Information	Statement introduced in Junos OS Release 10.1 for EX Series switches.
Description	Configure the time in seconds 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.
Options	<i>seconds</i> —Number of seconds. Range: 1–65535 Default: 20
Required Privilege Level	routing—To view this statement in the configuration. routing—control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102• Configuring Captive Portal Authentication (CLI Procedure) on page 151

session-expiry

Syntax	<code>session-expiry <i>seconds</i>;</code>
Hierarchy Level	[edit services captive-portal interface (all <i>interface-names</i>)]]
Release Information	Statement introduced in Junos OS Release 10.1 for EX Series switches.
Description	The session-expiry statement is used to locally configure the number of seconds before the captive portal authentication session times out and the client must reattempt authentication.
<div> NOTE: If the authentication server sends an authentication session timeout to the client, this takes priority over the value configured locally using the session-expiry statement. The session timeout value is sent from the server to the client as an attribute of the RADIUS Access-Accept message.</div>	
Options	<i>seconds</i> —Duration of session. Range: 1 through 65535 Default: 3600
Required Privilege Level	routing—To view this statement in the configuration. routing—control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102• Configuring Captive Portal Authentication (CLI Procedure) on page 151• Understanding Authentication Session Timeout on page 31

single-connection

Syntax	single-connection;
Hierarchy Level	[edit system accounting destination tacplus server <i>server-address</i>] [edit system tacplus-server <i>server-address</i>],
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring TACACS+ Authentication</i> • <i>Configuring TACACS+ System Accounting</i>

source-address

Syntax	source-address <i>source-address</i> ;
Hierarchy Level	[edit access <i>radius-server</i> <i>server-address</i>]; [edit access profile <i>profile-name</i> <i>radius-server</i> <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address.
Options	<i>source-address</i> —Valid IPv4 address configured on one of the router or switch interfaces. On M Series routers only, the source address can be an IPv6 address and the UDP source port is 514.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Router or Switch Interaction with RADIUS Servers</i> • <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i> • <i>Example: Configuring CHAP Authentication with RADIUS</i> • <i>Configuring RADIUS Authentication for L2TP</i>

source-address (NTP, RADIUS, System Logging, or TACACS+)

Syntax	<code>source-address <i>source-address</i>;</code>
Hierarchy Level	<code>[edit system accounting destination radius server <i>server-address</i>],</code> <code>[edit system accounting destination tacplus server <i>server-address</i>],</code> <code>[edit system ntp],</code> <code>[edit system radius-server <i>server-address</i>],</code> <code>[edit system syslog],</code> <code>[edit system tacplus-server <i>server-address</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify a source address for each configured TACACS+ server, RADIUS server, NTP server, or the source address to record in system log messages that are directed to a remote machine.
Options	<i>source-address</i> —A valid IP address configured on one of the router or switch interfaces. For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all host <i>hostname</i> statements at the [edit system syslog] hierarchy level, but not for messages directed to the other Routing Engine or to the TX Matrix router or TX Matrix Plus router in a routing matrix based on a TX Matrix router or TX Matrix Plus router.
Required Privilege Level	system —To view this statement in the configuration. system-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring RADIUS Authentication</i>• <i>Synchronizing and Coordinating Time Distribution Using NTP</i>• <i>Specifying an Alternative Source Address for System Log Messages</i>

static (Protocols 802.1X)

Syntax	<pre>static mac-address { interface interface-names; vlan-assignment (vlan-id vlan-name); }</pre>
Hierarchy Level	[edit protocols dot1x authenticator]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Configure MAC addresses to exclude from 802.1X authentication. The static MAC list provides an authentication bypass mechanism for supplicants connecting to a port, permitting devices such as printers that are not 802.1X-enabled to be connected to the network on 802.1X-enabled ports.</p> <p>Using this 802.1X authentication-bypass mechanism, the supplicant connected to the MAC address is assumed to be successfully authenticated and the port is opened for it. No further authentication is done for the supplicant.</p> <p>You can optionally configure the VLAN that the supplicant is moved to or the interfaces on which the MAC address can gain access from.</p>
Options	<p>mac-address —The MAC address of the device for which 802.1X authentication should be bypassed and the device permitted access to the port.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • show dot1x static-mac-address on page 338 • Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 75 • Configuring 802.1X Interface Settings (CLI Procedure) on page 126 • Configuring 802.1X Authentication (J-Web Procedure) on page 127 • Understanding Authentication on EX Series Switches on page 10

statistics (Access Profile)

Syntax	statistics (time volume-time);
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches. volume-time option added in Junos OS Release 9.4.
Description	Configure the router or switch to collect time statistics, or both volume and time statistics, for the sessions being managed by AAA.
Options	time —Collect uptime statistics only. volume-time —Collect both volume and uptime statistics.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

supplicant

Syntax	supplicant (multiple single single-secure);
Hierarchy Level	[edit protocols dot1x authenticator interface (802.1X) (all [interface-names])], [edit services captive-portal interface (all interface-names)]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement added to the [edit services captive-portal interface] hierarchy in Junos OS Release 10.1 for EX Series switches
Description	Configure the MAC-based method used to authenticate clients for 802.1X or captive portal authentication.
Default	single
Options	<p>single—Authenticates only the first client that connects to an authenticator port. All other clients connecting to the authenticator port after the first are permitted free access to the port without further authentication. If the first authenticated client logs out, all other supplicants are locked out until a client authenticates again.</p> <p>single-secure—Authenticates only one client to connect to an authenticator port. The host must be directly connected to the switch.</p> <p>multiple—Authenticates multiple clients individually on one authenticator port. You can configure the number of clients per port. If you also configure a maximum number of devices that can be connected to a port through port security settings, the lower of the configured values is used to determine the maximum number of clients allowed per port.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 50 • Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102 • Understanding Authentication on EX Series Switches on page 10 • Configuring Captive Portal Authentication (CLI Procedure) on page 151

supplicant-timeout

Syntax	supplicant-timeout <i>seconds</i> ;
Hierarchy Level	[edit protocols dot1x authenticator interface (802.1X) (all [<i>interface-name</i>])
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For 802.1X authentication, configure how long the port waits for a response when relaying a request from the authentication server to the supplicant before resending the request.
Default	30 seconds
Options	<i>seconds</i> —Number of seconds. Range: 1 through 60 seconds Default: 30 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• supplicant on page 291• Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 50• Understanding Authentication on EX Series Switches on page 10

tacplus

Syntax	<pre> tacplus { server { server-address { port port-number; secret password; single-connection; timeout seconds; } } } </pre>
Hierarchy Level	[edit system accounting destination]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the Terminal Access Controller Access Control System Plus (TACACS+).
Options	<p>server-address—Address of the TACACS+ authentication server.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring TACACS+ System Accounting</i>


timeout (System)

Syntax	<code>timeout seconds;</code>
Hierarchy Level	[edit system radius-server <i>server-address</i>], [edit system tacplus-server <i>server-address</i>], [edit system accounting destination radius server <i>server-address</i>], [edit system accounting destination tacplus server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the amount of time that the local router or switch waits to receive a response from a RADIUS or TACACS+ server.
Options	seconds —Amount of time to wait. Range: 1 through 90 seconds Default: 3 seconds
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Authentication</i>• <i>Configuring TACACS+ Authentication</i>• retry on page 276

timeout (Access Control Service)

Syntax	timeout <i>seconds</i> ;
Hierarchy Level	[edit services unified-access-control]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Configure the amount of time that the switch waits to receive a response from the Junos Pulse Access Control Service.
Options	<p><i>seconds</i>—Amount of time to wait.</p> <p>Range: 2 through 1000 seconds</p> <p>Default: 300 seconds</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 157• Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 159

timeout (RADIUS)

Syntax	<code>timeout seconds;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the 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> 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.</div>	
Options	seconds —Amount of time to wait. Range: 1 through 90 seconds Default: 3 seconds
Required Privilege Level	system —To view this statement in the configuration. system-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Router or Switch Interaction with RADIUS Servers</i>• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>• <i>Example: Configuring CHAP Authentication with RADIUS</i>• <i>Configuring RADIUS Authentication for L2TP</i>

timeout-action (Access Control Service)

Syntax	timeout-action (close no-change);
Hierarchy Level	[edit services unified-access-control]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Specify the action to be taken when the timeout is reached for the switch's connection with the Junos Pulse Access Control Service.
Options	<p>close—Remove existing sessions and block further traffic.</p> <p>no-change—Preserve existing connections, but block new sessions.</p> <p>Default: close</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• timeout (Access Control Service) on page 295• Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 157• Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 159

traceoptions (802.1X)

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable> <match <i>regex</i>>; flag <i>flag</i>; }</pre>
Hierarchy Level	[edit protocols dot1x]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for the dot1x-event and dot1x-ipc options introduced in Junos OS Release 13.2X50 for EX Series switches.
Description	Define tracing operations for the 802.1X protocol.
Default	Tracing operations are disabled.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size by using the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none">• all—All tracing operations.• config-internal—Trace internal configuration operations.• dot1x-event—(Switches with ELS only) Trace 802.1x events.• dot1x-debug—(Switches without ELS) Trace 802.1x events.• dot1x-ipc—(Switches with ELS only) Trace IPC interactions.• eapol—Trace EAPOL packets transmitted and received.• esw-if—(Switches without ELS) Trace ESW interactions.• general—Trace general operations.• normal—Trace normal operations.• parse—Trace reading of the configuration.• regex-parse—Trace regular-expression parsing operations.• state—Trace protocol state changes.

- **task**—Trace protocol task operations.
- **timer**—Trace protocol timer operations.
- **vlan**—Trace VLAN transactions.

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

no-world-readable—(Optional) Restrict file access to the user who created the file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files with the **files** option, you also must specify a maximum file size.

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

Range: 10 KB through 1 GB

Default: 128 KB

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

Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • show lldp on page 344 • Configuring 802.1X Interface Settings (CLI Procedure) on page 126 • 802.1X for EX Series Switches Overview on page 7

traceoptions (LLDP)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable> <no-stamp> <replace>; flag <i>flag</i> <disable>; } </pre>
Hierarchy Level	[edit protocols lldp]
Release Information	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
Description	Define tracing operations for the Link Layer Discovery Protocol (LLDP). You can trace messages under LLDP for LLDP and PTOPO MIBs.



NOTE: The traceoptions statement is not supported on the QFX3000 QFabric system.

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

- **vlan**—Trace VLAN update events.

no-stamp—(Optional) Do not timestamp the trace file.

Default: If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

no-world-readable—(Optional) Restrict file access to the user who created the file.

replace—(Optional) Replace an existing trace file if there is one rather than appending output to it.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **files** option.

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

Range: 10 KB through 1 GB

Default: 128 KB

Default: If you do not include this option, tracing output is appended to an existing trace file.

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



NOTE: The **traceoptions** statement is not supported on the QFX3000 QFabric system.

Required Privilege Level

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

Related Documentation

- [Configuring LLDP-MED \(CLI Procedure\) on page 140](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 18](#)
- [Configuring LLDP](#)
- [Understanding LLDP](#)

transmit-delay

Syntax	<code>transmit-delay <i>seconds</i>;</code>
Hierarchy Level	[edit protocols lldp]
Release Information	Statement introduced in Junos OS Release 11.1 for EX Series switches.
Description	<p>Specify the number of seconds the device delays before sending advertisements to neighbors after a change is made in a TLV (type, length, or value) element in the Link Layer Discovery Protocol (LLDP) or in 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.</p> <p>The advertisement-interval value must be greater than or equal to four times the transmit-delay value, or an error will be returned when you attempt to commit the configuration.</p>
Default	Enabled
Options	<p><i>seconds</i>—Delay after a change to the local TLVs or system state before LLDP advertisements are sent.</p> <p>Range: 1 through 8192 seconds</p> <p>Default:</p> <ul style="list-style-type: none">• 2 seconds if the advertisement-interval value is set to 8 seconds or more• 1 second if the advertisement-interval value is set to less than 8 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• show lldp on page 344• Configuring LLDP (CLI Procedure) on page 136• Understanding LLDP and LLDP-MED on EX Series Switches on page 18

transmit-period

Syntax	transmit-period <i>seconds</i> ;
Hierarchy Level	[edit protocols dot1x authenticator interface (802.1X) (all [<i>interface-name</i>])
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For 802.1X authentication, how long the port waits before retransmitting the initial EAPOL PDUs to the supplicant.
Default	30 seconds
Options	<i>seconds</i> —Number of seconds the port waits before retransmitting the initial EAPOL PDUs to the supplicant. Range: 1 through 65,535 seconds Default: 30 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring 802.1X Interface Settings (CLI Procedure) on page 126 • 802.1X for EX Series Switches Overview on page 7

uac-policy

Syntax	uac-policy;
Hierarchy Level	[edit ethernet-switching-options]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Configure Junos Pulse Access Control Service as the access policy to authenticate and authorize users connected to the switch for admission to the network and for access to protected network resources.
Default	The Access Control Service access policy is disabled.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 157 • Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 159


uac-service

Syntax	uac-service { timeout { timeout-action {
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Configure Junos Pulse Access Control Service as one of the system processes.
Default	Junos Pulse Access Control Service process is disabled.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 157• Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 159• Understanding Centralized Network Access Control and EX Series Switches on page 33

unified-access-control

Syntax	<pre> unified-access-control { infranet-controller <i>hostname</i> { address <i>ip-address</i>; interface <i>interface-name</i>; password <i>password</i>; port <i>port-number</i>; } </pre>
Hierarchy Level	[edit services]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	<p>Configure Junos Pulse Access Control Service to authenticate and authorize users connected to the switch for admission to the network and for access to protected network resources.</p> <p>The remaining statements are explained separately.</p>
Default	Junos Pulse Access Control Service is disabled.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) on page 157 • Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) on page 159

update-interval

Syntax	update-interval <i>minutes</i> ;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	<p>Enable interim accounting updates and configure the amount of time that the router or switch waits before sending a new accounting update.</p> <p>Interim accounting updates are included in the exchange of messages between the client and the accounting server. In RADIUS accounting, the client is the network access server (NAS), which can be the router or switch. The NAS sends Accounting-Request messages to the server, which acknowledges receipt of the requests with Accounting-Response messages. Interim accounting updates are sent in Accounting-Request packets with the Acct-Status-Type attribute set to Interim-Update.</p> <p>When a user is authenticated, the authentication server issues an Access-Accept message in response to a successful Access-Request message. The interval between interim updates can be configured directly on the server using the Acct-Interim-Interval attribute of the Access-Accept message. However, if the update interval is configured on the NAS using update-interval, then the locally configured value overrides the value found in an Access-Accept message from the server.</p> <div> NOTE: All information in an interim update message is cumulative from the beginning of the session, not from the last interim update message.</div>
Default	No interim updates are sent from the client to the accounting server.
Options	<p>minutes—Amount of time between updates, in minutes. All values are rounded to the next higher multiple of 10. For example, the values 811 through 819 are all accepted by the CLI, but are all rounded up to 820.</p> <p>Range: 10 through 1440 minutes</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><i>Configuring Authentication and Accounting Parameters for Subscriber Access</i><i>Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications</i>

vlan-assignment

Syntax	<code>vlan-assignment (vlan-id vlan-name);</code>
Hierarchy Level	<p>[edit protocols dot1x authenticator authentication-profile-name static (Protocols 802.1X) mac-address];</p> <p>[edit ethernet-switching-options authentication-whitelist];</p> <p>[edit switch-options authentication-whitelist]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement added to the [edit ethernet-switching-options authentication-whitelist] hierarchy in Junos OS Release 10.1 for EX Series switches.</p> <p>Statement added to the [edit switch-options authentication-whitelist] hierarchy in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	Configure the VLAN that is associated with the list of MAC addresses that are excluded from RADIUS authentication.
Options	<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.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • show dot1x static-mac-address on page 338 • Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 75 • Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102 • Understanding Authentication on EX Series Switches on page 10 • Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102 • Configuring Captive Portal Authentication (CLI Procedure) on page 151

vlan-nas-port-stacked-format

Syntax	<code>vlan-nas-port-stacked-format;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access• Configuring Authentication and Accounting Parameters for Subscriber Access

voip

Syntax	<pre>voip { interface (all [<i>interface-name</i> access-ports]) { vlan <i>vlan-name</i> ; forwarding-class <assured-forwarding best-effort expedited-forwarding network-control>; } }</pre>
Hierarchy Level	[edit ethernet-switching-options]; [edit switch-options]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure VoIP 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	<ul style="list-style-type: none">• Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56• Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication on page 68• Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 64

what

Syntax	<code>what <i>number</i>;</code>
Hierarchy Level	[edit protocols lldp-med (Ethernet Switching) interface (LLDP-MED) (all <i>interface-name</i>) location (LLDP-MED) civic-based]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Modified in Junos OS Release 9.2 for EX Series switches to display new default.
Description	<p>For Link Layer Discovery Protocol—Media Endpoint Device (LLDP-MED), configure the location to which the DHCP entry refers. This information is advertised, along with other location information, from the switch to the MED. It is used during emergency calls to identify the location of the MED.</p> <p>Options 0 and 1 should not be used unless it is known that the DHCP client is in close physical proximity to the server or network element.</p>
Default	1
Options	<p><i>number</i>—Location:</p> <ul style="list-style-type: none"> • 0—Location of the DHCP server. • 1—Location of a network element believed to be closest to the client. • 2—Location of the client.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • show lldp on page 344 • Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 56 • Configuring LLDP-MED (CLI Procedure) on page 140

PART 3

Administration

- [Routine Monitoring on page 313](#)
- [Operational Commands on page 317](#)

CHAPTER 6

Routine Monitoring

- [Monitoring 802.1X Authentication on page 313](#)
- [Verifying 802.1X Authentication on page 314](#)

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 \(J-Web Procedure\) on page 127](#)
- [Configuring 802.1X Interface Settings \(CLI Procedure\) on page 126](#)
- [Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 50](#)

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 126](#)
- [Configuring 802.1X Authentication \(J-Web Procedure\) on page 127](#)
- [Configuring MAC RADIUS Authentication \(CLI Procedure\) on page 146](#)
- [Configuring RADIUS Server Fail Fallback \(CLI Procedure\) on page 144](#)

CHAPTER 7

Operational Commands

- `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 ethernet-switching interfaces`
- `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`
- `show services unified-access-control authentication-table`
- `show services unified-access-control policies`
- `show services unified-access-control status`

clear captive-portal

Syntax	<code>clear captive-portal (firewall [<i>interface-names</i>] interface (802.1X) (all [<i>interface-names</i>]) mac-address [<i>mac-addresses</i>])</code>
Release Information	Command introduced in Junos OS Release 10.1 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 a captive portal interface or captive portal firewall statistics on one or more interfaces.
Options	<p>firewall [<i>interface-names</i>] —Resets captive portal statistics on all interfaces or on the specified interface.</p> <p>interface (all <i>interface-names</i>) —Resets the authentication state of users connected to all interfaces or the specified interfaces.</p> <p>mac-address <i>mac-addresses</i> —Resets the authentication state for the specified MAC addresses.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show captive-portal authentication-failed-users on page 324 • show captive-portal interface on page 328 • show captive-portal firewall on page 326 • Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102 • Configuring Captive Portal Authentication (CLI Procedure) on page 151
List of Sample Output	clear captive-portal interface on page 319 clear captive-portal interface on page 319 clear captive-portal mac-address on page 319 clear captive-portal firewall on page 319
Output Fields	Table 24 on page 318 lists the output fields for the clear captive-portal interface command. (The clear captive-portal firewall and clear captive-portal mac-address commands have no output). Output fields are listed in the approximate order in which they appear.

Table 24: clear captive-portal interface Output Fields

Field Name	Field Description
Interface	Interface on which captive portal has been configured.

Table 24: clear captive-portal interface Output Fields (*continued*)

Field Name	Field Description
State	<p>The state of the port:</p> <ul style="list-style-type: none"> • Authenticated—The client has been authenticated through the RADIUS server or has been permitted access through server fail fallback. • Authenticating—The client is authenticating through the RADIUS server. • Connecting—Switch is attempting to contact the RADIUS server. • Initialize—The interface link is down. • Held—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.
MAC address	The MAC address of the connected client on the interface.
User	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  aclallow
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 331](#)
- [Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch on page 50](#)
- [Filtering 802.1X Suplicants by Using RADIUS Server Attributes on page 131](#)

List of Sample Output

- [clear dot1x firewall on page 321](#)
- [clear dot1x interface \(Specific Interfaces\) on page 321](#)
- [clear dot1x mac-address \(Specific MAC Address\) on page 321](#)
- [clear dot1x statistics interface \(Specific Interface\) on page 321](#)

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

Syntax	<code>clear lldp neighbors</code> <code><interface <i>interface</i>></code>
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Clear the learned remote neighbor information on all or selected interfaces.
Options	none —Clear the remote neighbor information on all interfaces. interface <i>interface</i> —(Optional) Clear the remote neighbor information from one or more selected interfaces.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show lldp on page 344• Configuring LLDP (CLI Procedure) on page 136• Understanding LLDP and LLDP-MED on EX Series Switches on page 18
List of Sample Output	clear lldp neighbors on page 322 clear lldp neighbors interface ge-0/1/1.0 on page 322

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

Syntax	clear lldp statistics <interface <i>interface</i> >
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Clear LLDP statistics on one or more interfaces.
Options	<p>none—Clears LLDP statistics on all interfaces.</p> <p>interface <i>interface-names</i>—(Optional) Clear LLDP statistics on one or more interfaces.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Configuring LLDP (CLI Procedure) on page 136 • Understanding LLDP and LLDP-MED on EX Series Switches on page 18
List of Sample Output	<p>clear lldp statistics on page 323</p> <p>clear lldp statistics interface ge-0/1/1.0 on page 323</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

Syntax	show captive-portal authentication-failed-users
Release Information	Command introduced in Junos OS Release 10.1 for EX Series switches. Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.
Description	Display the users that have failed captive portal authentication.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show captive-portal interface on page 328 • show captive-portal firewall on page 326 • clear captive-portal on page 318 • Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102 • Configuring Captive Portal Authentication (CLI Procedure) on page 151
List of Sample Output	show captive-portal authentication-failed-users on page 324
Output Fields	Table 25 on page 324 lists the output fields for the show captive-portal authentication-failed-users command. Output fields are listed in the approximate order in which they appear.

Table 25: show captive-portal authentication-failed-users Output Fields

Field Name	Field Description	Level of Output
Interface	The MAC address configured to bypass captive portal authentication.	all
MAC address	The MAC address configured statically on the interface.	all
User	Name of the user that has failed captive portal authentication.	all
Failure Count	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

Syntax	<code>show captive-portal firewall</code> <code><brief detail></code> <code><interface-name></code> <code><interface-name detail></code>
Release Information	Command introduced in Junos OS Release 10.1 for EX Series switches. Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.
Description	Display information about the firewall filters for each user that is authenticated on each captive portal interface.
Options	none —Display all the firewall filters on all captive portal interfaces. brief detail —(Optional) Display the specified level of output. interface-name —(Optional) Display all the terms of the firewall filters for the specified interface. interface-name detail —(Optional) Display all of the terms of the firewall filters for the specified interface.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show captive-portal authentication-failed-users on page 324• show captive-portal interface on page 328• clear captive-portal on page 318• Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102• Configuring Captive Portal Authentication (CLI Procedure) on page 151
List of Sample Output	show captive-portal firewall brief on page 326 show captive-portal firewall (Specific Interface) on page 327 show captive-portal firewall on page 327
Output Fields	Output fields for the show captive-portal firewall 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

Syntax	show captive-portal interface <interface-name> detail
Release Information	Command introduced in Junos OS Release 10.1 for EX Series switches. Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.
Description	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.
Options	<p>none—Display all captive portal interfaces.</p> <p>interface-name—(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>interface-name detail—(Optional) Display the configured values of captive portal attributes on the specified captive portal interface.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show captive-portal authentication-failed-users on page 324 • show captive-portal firewall on page 326 • captive-portal on page 206 • clear captive-portal on page 318 • Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 102 • Configuring Captive Portal Authentication (CLI Procedure) on page 151
List of Sample Output	<p>show captive-portal interface (Only Captive Portal Enabled) on page 330</p> <p>show captive-portal interface (802.1X Authentication and Captive Portal Enabled) on page 330</p> <p>show captive-portal interface detail (Only Captive Portal Enabled) on page 330</p> <p>show captive-portal interface detail (802.1X Authentication and Captive Portal Enabled) on page 330</p>
Output Fields	Table 26 on page 328 lists the output fields for the show captive-portal interface command. Output fields are listed in the approximate order in which they appear.

Table 26: show captive-portal interface Output Fields

Field Name	Field Description	Level of Output
Interface	Interface on which captive portal has been configured.	All levels

Table 26: show captive-portal interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
State	<p>The state of the interface:</p> <ul style="list-style-type: none"> • Authenticated—The client has been authenticated through the RADIUS server or has been permitted access through server fail fallback. • Authenticating—The client is authenticating through the RADIUS server. • Connecting—Switch is attempting to contact the RADIUS server. • Initialize—The interface link is down. • Held—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. 	All levels
MAC address	The MAC address of the connected client on the interface..	brief
User	Users connected to the captive portal interface.	brief
Fallen back	<p>Indicates when 802.1X authentication and captive portal are both enabled on an interface:</p> <ul style="list-style-type: none"> • If 802.1X authentication and captive portal are both enabled, CP fallen back status is Yes. • If 802.1X authentication and captive portal are not both enabled, CP fallen back status is No. 	
Supplicant mode	Mode used to authenticate clients—multiple, single, or single-supplicant.	detail
Number of retries	Number of times the user can attempt to submit authentication information.	detail
Quiet period	Time, in seconds, after a user exceeds the maximum number of retries before they can attempt to authenticate.	detail
Configured CP session timeout	Time, in seconds, that a client can be idle before the session expires.	detail
Server timeout	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
Number of connected supplicants	<p>Number of users connecting through the captive portal interface. Information for each user includes:</p> <ul style="list-style-type: none"> • Supplicant—User name and MAC address. • Operational state—See State (above). • Dynamic CP session timeout—Timeout value dynamically downloaded from the RADIUS server for this user, if any. • CP Session expiration due in—Time remaining in session. 	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

Syntax	show dot1x <brief detail> <interface <i>interface-name</i>>
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.
Description	Display the current operational state of all ports with the list of connected users. 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.
Options	none —Display information for all authenticator ports. brief detail —(Optional) Display the specified level of output. interface <i>interface-name</i> —(Optional) Display information for the specified port with a list of connected supplicants.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dot1x on page 320 • Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch on page 50 • Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch on page 79 • Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 107 • Filtering 802.1X Supplicants by Using RADIUS Server Attributes on page 131 • Verifying 802.1X Authentication on page 314
List of Sample Output	show dot1x interface brief on page 334 show dot1x interface detail on page 335
Output Fields	Table 27 on page 331 lists the output fields for the show dot1x command. Output fields are listed in the approximate order in which they appear.

Table 27: show dot1x Output Fields

Field Name	Field Description	Level of Output
Interface	Name of a port.	All levels

Table 27: show dot1x Output Fields (*continued*)

Field Name	Field Description	Level of Output
MAC address	The MAC address of the connected supplicant on the port.	All levels
Role	The 802.1X authentication role of the interface. When 802.1X is enabled on an interface, the role is Authenticator . As Authenticator , the interface blocks LAN access until a supplicant is authenticated through 802.1X or MAC RADIUS authentication.	brief, detail
State	<p>The state of the port:</p> <ul style="list-style-type: none"> • Authenticated—The supplicant has been authenticated through the RADIUS server or has been permitted access through server fail fallback. • Authenticating—The supplicant is authenticating through the RADIUS server. • Held—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. 	brief
User	The username of the connected supplicant.	brief
Administrative state	<p>The administrative state of the port:</p> <ul style="list-style-type: none"> • auto—Traffic is allowed through the port based on the authentication result (by default). • force-authorize—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 dynamic. • force-unauthorize—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 dynamic. 	detail
Supplicant	<p>The mode for the supplicant:</p> <ul style="list-style-type: none"> • single—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. • single-secure—Only one supplicant is allowed to connect to the port. No other supplicant is allowed to connect until the first supplicant logs out. • multiple—Multiple supplicants are allowed to connect to the port. Each supplicant is authenticated individually. 	detail
Quiet period	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.	detail
Transmit period	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.	detail

Table 27: show dot1x Output Fields (*continued*)

Field Name	Field Description	Level of Output
MAC radius	MAC RADIUS authentication: <ul style="list-style-type: none"> • enabled—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. • disabled—The default. The switch does not attempt to authenticate the MAC address of the connecting host. 	detail
MAC radius authentication protocol	MAC RADIUS authentication protocol: <ul style="list-style-type: none"> • EAP-MD5—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. • PAP—The Password Authentication Protocol (PAP) authentication protocol is used for MAC RADIUS authentication. 	detail
MAC radius restrict	The authentication method is restricted to MAC RADIUS only. 802.1X authentication is not enabled.	detail
Reauthentication	The reauthentication state: <ul style="list-style-type: none"> • disable—Periodic reauthentication of the client is disabled. • interval—Sets the periodic reauthentication time interval. The default value is 3600 seconds. The range is 1 through 65,535 seconds. 	detail
Supplicant timeout	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.	detail
Server timeout	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.	detail
Maximum EAPOL requests	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.	detail
Number of clients bypassed because of authentication	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"> • Client—MAC address of the client. • vlan—The name of the VLAN to which the client is connected. 	detail
Guest VLAN member	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 <not configured> .	detail
Number of connected supplicants	The number of supplicants connected to a port.	detail
Supplicant	The username and MAC address of the connected supplicant.	detail

Table 27: 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"> • CWA Authentication—A supplicant is authenticated by the central Web authentication (CWA) server. • Guest VLAN—A supplicant is connected to the LAN through the guest VLAN. • MAC RADIUS—A nonresponsive host is authenticated based on its MAC address. The MAC address is configured as permitted on the RADIUS server, the RADIUS server lets the switch know that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected. • RADIUS—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. • Server-fail deny—If the RADIUS servers time out, all supplicants are denied access to the LAN, preventing traffic from flowing from the supplicant through the interface. This is the default. • Server-fail permit—When the RADIUS server is unavailable, a supplicant is still permitted access to the LAN as if the supplicant had been successfully authenticated by the RADIUS server. • Server-fail use-cache—If the RADIUS servers time out during reauthentication, previously authenticated supplicants are reauthenticated, 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.) 	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		
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

Syntax	show dot1x authentication-failed-users
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display the supplicants (users) that have failed 802.1X authentication.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dot1x on page 320 • Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 75 • Configuring 802.1X Interface Settings (CLI Procedure) on page 126
List of Sample Output	show dot1x authentication-failed-users on page 336
Output Fields	Table 28 on page 336 lists the output fields for the show dot1x authentication-failed-users command. Output fields are listed in the approximate order in which they appear.

Table 28: show dot1x authentication-failed-users Output Fields

Field Name	Field Description	Level of Output
Interface	The MAC address configured to bypass 802.1X authentication.	all
MAC address	The MAC address configured statically on the interface.	all
User	The user that is configured on the RADIUS server and that has failed 802.1X authentication.	all
Failure Count	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

Syntax	<code>show dot1x firewall <interface <i>interface-name</i>></code>
Release Information	Command introduced 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	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.
Options	none —Display information for all interfaces. interface <i>interface-names</i> —(Optional) Display information for the specified interface.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dot1x on page 320 • Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on page 97
List of Sample Output	show dot1x firewall on page 337 show dot1x firewall on page 337
Output Fields	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

Syntax	<code>show dot1x static-mac-address <(interface <i>[interface-name]</i>)></code>
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.
Description	Display all the static MAC addresses that are configured to bypass 802.1X authentication on the switch.
Options	none —Display static MAC addresses for all interfaces. interface <i>interface-name</i> —(Optional) Display static MAC addresses for a specific interface.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dot1x on page 320 • Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch on page 75 • Adding a Static MAC Address Entry to the Ethernet Switching Table (CLI Procedure) • Configuring 802.1X Interface Settings (CLI Procedure) on page 126 • Understanding Authentication on EX Series Switches on page 10
List of Sample Output	show dot1x static-mac-address on page 338 show dot1x static-mac-address interface (Specific Interface) on page 339
Output Fields	Table 29 on page 338 lists the output fields for the show dot1x static-mac-address command. Output fields are listed in the approximate order in which they appear.

Table 29: show dot1x static-mac-address Output Fields

Field Name	Field Description	Level of Output
MAC address	The MAC address of the device that is configured to bypass 802.1X authentication.	all
VLAN-Assignment	The name of the VLAN to which the device is assigned.	all
Interface	The name of the interface on which authentication is bypassed for a given MAC address.	all

Sample Output

show dot1x static-mac-address

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

MAC address	VLAN-Assignment	Interface
00:00:00:11:22:33		
00:00:00:00:12:12		ge-0/0/3.0
00:00:00:02:34:56	facilities	ge-0/0/1.0

show dot1x static-mac-address interface (Specific Interface)

```
user@switch> show dot1x static-mac-address interface ge-0/0/0.1
```

MAC address	VLAN-Assignment	Interface
00:00:00:12:24:12	support	ge-0/0/1.0
00:00:00:72:30:58	support	ge-0/0/1.0

show ethernet-switching interfaces

Syntax	<code>show ethernet-switching interfaces</code> <code><brief detail summary></code> <code><interface <i>interface-name</i>></code>
Release Information	<p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>In Junos OS Release 9.6 for EX Series switches, the following updates were made:</p> <ul style="list-style-type: none">• Blocking field output was updated.• The default view was updated to include information about 802.1Q tags.• The detail view was updated to include information on VLAN mapping. <p>In Junos OS Release 11.1 for EX Series switches, the detail view was updated to include reflective relay information.</p>
Description	Display information about Ethernet switching interfaces.
Options	<p>none—Display brief information for Ethernet switching interfaces.</p> <p>brief detail summary—(Optional) Display the specified level of output.</p> <p>interface <i>interface-name</i>—(Optional) Display Ethernet switching information for a specific interface.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>show ethernet-switching mac-learning-log</i>• <i>show ethernet-switching table</i>• <i>Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)</i>
List of Sample Output	<p>show ethernet-switching interfaces on page 342</p> <p>show ethernet-switching interfaces ge-0/0/15 brief on page 342</p> <p>show ethernet-switching interfaces ge-0/0/2 detail (Blocked by RTG rtggroup) on page 342</p> <p>show ethernet-switching interfaces ge-0/0/15 detail (Blocked by STP) on page 343</p> <p>show ethernet-switching interfaces ge-0/0/17 detail (Disabled by bpdu-control) on page 343</p> <p>show ethernet-switching interfaces detail (C-VLAN to S-VLAN Mapping) on page 343</p> <p>show ethernet-switching interfaces detail (Reflective Relay Is Configured) on page 343</p>
Output Fields	Table 30 on page 341 lists the output fields for the show ethernet-switching interfaces command. Output fields are listed in the approximate order in which they appear.

Table 30: show ethernet-switching interfaces Output Fields

Field Name	Field Description	Level of Output
Interface	Name of a switching interface.	none, brief , detail , summary
Index	VLAN index internal to Junos OS.	detail
State	Interface state. Values are up and down .	none, brief , detail
Port mode	The access mode is the port mode default and works with a single VLAN. Port mode can also be trunk , which accepts tagged packets from multiple VLANs on other switches. The third port mode value is tagged-access , which accepts tagged packets from access devices.	detail
Reflective Relay Status	Reflective relay allows packets to use the same interface for both upstream and downstream traffic. When reflective relay has been configured, the status displayed is always enabled . When reflective relay is not configured, this entry does not appear in the command output.	detail
Ether type for the interface	Ether type is a two-octet field in an Ethernet frame used to indicate which protocol is encapsulated in the payload of an incoming Ethernet packet. Both 802.1Q packets and Q-in-Q packets use this field. The output displayed for this particular field indicates the interface's Ether type, which is used to match the Ether type of incoming 802.1Q packets and Q-in-Q packets. The indicated Ether type field is also added to the interface's outgoing 802.1Q and Q-in-Q packets.	detail
VLAN membership	Names of VLANs that belong to this interface.	none, brief , detail ,
Tag	Number of the 802.1Q tag.	none, brief , detail ,
Tagging	Specifies whether the interface forwards 802.1Q tagged or untagged traffic.	none, brief , detail ,
Blocking	<p>The forwarding state of the interface:</p> <ul style="list-style-type: none"> • unblocked—Traffic is forwarded on the interface. • blocked—Traffic is not being forwarded on the interface. • Disabled by bpdu control—The interface is disabled due to receiving BPDUs on a protected interface. If the disable-timeout statement has been included in the BPDU configuration, the interface automatically returns to service after the timer expires. • blocked by RTG—The specified redundant trunk group is disabled. • blocked by STP—The interface is disabled due to a spanning-tree protocol error. • MAC limit exceeded—The interface is temporarily disabled due to a MAC limit error. The disabled interface is automatically restored to service when the disable timeout expires. • MAC move limit exceeded—The interface is temporarily disabled due to a MAC move limit error. The disabled interface is automatically restored to service when the disable timeout expires. • Storm control in effect—The interface is temporarily disabled due to a storm control error. The disabled interface is automatically restored to service when the disable timeout expires. 	none, brief , detail ,

Table 30: show ethernet-switching interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Number of MACs learned on IFL	Number of MAC addresses learned by this interface.	detail
mapping	<p>When mapping is configured, the status is one of the following C-VLAN to S-VLAN mapping types:</p> <ul style="list-style-type: none"> dot1q-tunneled—The interface maps all traffic to the S-VLAN (all-in-one bundling). native—The interface maps untagged and priority tagged packets to the S-VLAN. push—The interface maps packets to a firewall filter to an S-VLAN. policy-mapped—The interface maps packets to a specifically defined S-VLAN. integer—The interface maps packets to the specified S-VLAN. <p>When mapping is not configured, this entry does not appear in the command output.</p>	detail

Sample Output

show ethernet-switching interfaces

```
user@switch> show ethernet-switching interfaces
```

Interface	State	VLAN members	Tag	Tagging	Blocking
ae0.0	up	default		untagged	unblocked
ge-0/0/2.0	up	vlan300	300	untagged	blocked by RTG (rtggroup)
ge-0/0/3.0	up	default			blocked by STP
ge-0/0/4.0	down	default			MAC limit exceeded
ge-0/0/5.0	down	default			MAC move limit exceeded
ge-0/0/6.0	down	default			Storm control in effect
ge-0/0/7.0	down	default			unblocked
ge-0/0/13.0	up	default		untagged	unblocked
ge-0/0/14.0	up	vlan100	100	tagged	unblocked
		vlan200	200	tagged	unblocked
ge-0/0/15.0	up	vlan100	100	tagged	blocked by STP
		vlan200	200	tagged	blocked by STP
ge-0/0/16.0	down	default		untagged	unblocked
ge-0/0/17.0	down	vlan100	100	tagged	Disabled by bpdu-control
		vlan200	200	tagged	Disabled by bpdu-control

show ethernet-switching interfaces ge-0/0/15 brief

```
user@switch> show ethernet-switching interfaces ge-0/0/15 brief
```

Interface	State	VLAN members	Tag	Tagging	Blocking
ge-0/0/15.0	up	vlan100	100	tagged	blocked by STP
		vlan200	200	tagged	blocked by STP

show ethernet-switching interfaces ge-0/0/2 detail (Blocked by RTG rtggroup)

```
user@switch> show ethernet-switching interfaces ge-0/0/2 detail
```

```

Interface: ge-0/0/2.0, Index: 65, State: up, Port mode: Access
Ether type for the interface: 0X8100
VLAN membership:
    vlan300, 802.1Q Tag: 300, untagged, msti-id: 0, blocked by RTG(rtggroup)
Number of MACs learned on IFL: 0

```

show ethernet-switching interfaces ge-0/0/15 detail (Blocked by STP)

```

user@switch> show ethernet-switching interfaces ge-0/0/15 detail

Interface: ge-0/0/15.0, Index: 70, State: up, Port mode: Trunk
Ether type for the interface: 0X8100
VLAN membership:
    vlan100, 802.1Q Tag: 100, tagged, msti-id: 0, blocked by STP
    vlan200, 802.1Q Tag: 200, tagged, msti-id: 0, blocked by STP

Number of MACs learned on IFL: 0

```

show ethernet-switching interfaces ge-0/0/17 detail (Disabled by bpdu-control)

```

user@switch> show ethernet-switching interfaces ge-0/0/17 detail

Interface: ge-0/0/17.0, Index: 71, State: down, Port mode: Trunk
Ether type for the interface: 0X8100
VLAN membership:
    vlan100, 802.1Q Tag: 100, tagged, msti-id: 1, Disabled by bpdu-control
    vlan200, 802.1Q Tag: 200, tagged, msti-id: 2, Disabled by bpdu-control
Number of MACs learned on IFL: 0

```

show ethernet-switching interfaces detail (C-VLAN to S-VLAN Mapping)

```

user@switch> show ethernet-switching interfaces ge-0/0/6.0 detail
Interface: ge-0/0/6.0, Index: 73, State: up, Port mode: Access
Ether type for the interface: 0X8100
VLAN membership:
    map, 802.1Q Tag: 134, Mapped Tag: native, push, dot1q-tunneled, unblocked
    map, 802.1Q Tag: 134, Mapped Tag: 20, push, dot1q-tunneled, unblocked

```

show ethernet-switching interfaces detail (Reflective Relay Is Configured)

```

user@switch1> show ethernet-switching interfaces ge-7/0/2 detail
Interface: ge-7/0/2, Index: 66, State: down, Port mode: Tagged-access
Ether type for the interface: 0X8100
Reflective Relay Status: Enabled
Ether type for the interface: 0x8100
VLAN membership:
    VLAN_Purple VLAN_Orange VLAN_Blue, 802.1Q Tag: 450, tagged, unblocked
Number of MACs learned on IFL: 0

```

show lldp


Syntax	<code>show lldp</code> <code><detail></code>
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series.
Description	Display information about Link Layer Discovery Protocol (LLDP) and Link Level Discovery Protocol—Media Endpoint Discovery (LLDP-MED) configuration and capabilities on the switch. LLDP and LLDP-MED are used to learn about and to distribute device information on network links.
<div>  NOTE: LLDP-MED is not available on the QFX Series. </div>	
Options	none —Display LLDP information for all interfaces. detail —(Optional) Display detailed LLDP information for all interfaces.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Configuring LLDP (CLI Procedure) on page 136 • Configuring LLDP-MED (CLI Procedure) on page 140 • Understanding LLDP and LLDP-MED on EX Series Switches on page 18 • Configuring LLDP • Understanding LLDP
List of Sample Output	show lldp (EX3200 switches) on page 347 show lldp (EX4300 switches) on page 347 show lldp detail (EX4300 switches) on page 348
Output Fields	Table 31 on page 344 lists the output fields for the show lldp command. Output fields are listed in the approximate order in which they appear.

Table 31: show lldp Output Fields

Field Name	Field Description	Level of Output
LLDP	LLDP operating state. The state can be enabled or disabled . NOTE: If a VLAN that has been configured for untagged packets on an interface also has Layer 2 protocol tunneling (L2PT) enabled for LLDP, the LLDP operating state for that interface is displayed as disabled .	All levels

Table 31: show lldp Output Fields (*continued*)

Field Name	Field Description	Level of Output
Advertisement interval	Frequency, in seconds, at which LLDP advertisements are sent. This value is set by the advertisement-interval configuration statement.	All levels
Transmit delay	Seconds of delay before advertisements are sent to neighbors following a change to a TLV (type, length, or value) element in the LLDP protocol or to the state of the local system, such as a change in hostname or management address. You can set this value to reduce the delay in notifying neighbors of a change in the local system. This value is set by the transmit-delay configuration statement.	All levels
Hold timer	On EX4300 switches, the hold timer shows the length of time LLDP information is held before it is discarded. The hold timer value is equal to the advertisement interval multiplied by the hold multiplier. On all other switches, the hold timer shows the value of the hold multiplier. The hold multiplier value is set by the hold-multiplier configuration statement.	All levels
Notification interval	How often LLDP trap notifications are generated as a result of LLDP database changes. If the interval value is 0, LLDP trap notifications on database changes are disabled. This value is set by the lldp-configuration-notification-interval configuration statement.	All levels
Config Trap Interval	How often LLDP trap notifications are generated as a result of changes in topology—for example, when an endpoint connects or disconnects. If the interval value is 0, LLDP trap notifications on topology changes are disabled. This value is set by the ptopo-configuration-trap-interval configuration statement.	All levels
Connection Hold timer	Amount of time the system maintains dynamic topology entries. This value is set by the ptopo-configuration-maximum-hold-time configuration statement.	All levels
LLDP-MED	LLDP-MED operating state. The state can be Enabled or Disabled .	All levels
MED fast start count	Number of advertisements sent from a switch to a device, such as a VoIP telephone, when the device is first detected by the switch. These increased advertisements are temporary. After a device and a switch exchange information and can communicate, advertisements are reduced to one per second. This value is set by using the fast-start configuration statement. NOTE: fast-start is not available on the QFX Series.	All levels
Interface	Name of the interface for which LLDP configuration information is being reported.	All levels
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs.	All levels

Table 31: show lldp Output Fields (*continued*)

Field Name	Field Description	Level of Output
LLDP	LLDP operating state. The state can be Enabled or Disabled .	All levels
Power Negotiation	LLDP power negotiation operating state. The state can be Enabled or Disabled .	All levels
Neighbor count	Total number of new LLDP neighbors detected since the last switch reboot.	detail
Interface	Name of the interface that is advertising VLAN information.	All levels
Vlan-id	VLAN tag associated with the interface sending LLDP frames. If the interface is not a member of a VLAN, the VLAN ID is advertised as 0.	detail
Vlan-name	VLAN name associated with the VLAN ID.	detail
LLDP basic TLVs supported	<p>Basic TLVs supported on the switch:</p> <ul style="list-style-type: none"> • Chassis identifier—TLV that advertises the MAC address associated with the local system. • Port identifier—TLV that advertises the port identification for the specified port in the local system. • Port description—Interface name for the port. • System name—TLV that advertises the user-configured name of the local system. • System description—TLV that advertises the system description containing information about the software and current image running on the system. This information is taken from the software and is not configurable. • System capabilities—TLV that advertises the primary functions performed by the system—for example, bridge or router. • Management address—TLV that advertises the IP management address of the local system. 	detail
Supported LLDP 802 TLVs	<p>802.3 TLVs supported on the switch:</p> <ul style="list-style-type: none"> • MAC/PHY configuration status—TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information is based on the physical interface structure and is not configurable. • Power via MDI—TLV that advertises MDI power support, PSE power pair, and power class information. • Link aggregation—TLV that advertises if the interface is aggregated and its aggregated interface ID. • Maximum frame size—TLV that advertises the maximum transmission unit (MTU) of the interface sending LLDP frames. • Port VLAN tag—TLV that advertises the VLAN tag configured on the interface. • Port VLAN name—TLV that advertises the VLAN name configured on the interface. 	detail

Table 31: 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"> • LLDP MED capabilities—TLV that advertises the primary function of the port. The capabilities values range from 0 through 15: <ul style="list-style-type: none"> • 0—Capabilities • 1—Network Policy • 2—Location Identification • 3—Extended Power via MDI-PSE • 4—Inventory • 5–15—Reserved • Network policy—TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types—such as voice or streaming video—802.1Q VLAN tagging, and 802.1p priority bits and DiffServ code points. • Endpoint location—TLV that advertises the physical location of the endpoint. • Extended power Via MDI—TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port. 	detail

Sample Output

show lldp (EX3200 switches)

```

user@switch> show lldp
LLDP                               : Enabled
Advertisement interval             : 30 seconds
Transmit delay                     : 2 seconds
Hold timer                        : 4 seconds
Notification interval             : 0 Second(s)
Config Trap Interval              : 0 seconds
Connection Hold timer             : 300 seconds

LLDP MED                           : Disabled
MED fast start count              : 3 Packets

```

Interface	Parent Interface	LLDP	LLDP-MED	Power Negotiation
all	-	Enabled	Enabled	Enabled

show lldp (EX4300 switches)

```

user@switch> show lldp
LLDP                               : Enabled
Advertisement interval             : 30 seconds
Transmit delay                     : 2 seconds
Hold timer                        : 120 seconds
Notification interval             : 0 Second(s)
Config Trap Interval              : 0 seconds
Connection Hold timer             : 300 seconds

LLDP MED                           : Disabled
MED fast start count              : 3 Packets

```

Interface	Parent Interface	LLDP	LLDP-MED	Power Negotiation
all	-	Enabled	Enabled	Enabled

show lldp detail (EX4300 switches)

```

user@switch> show lldp detail
LLDP : Enabled
Advertisement interval : 30 seconds
Transmit delay : 2 seconds
Hold timer : 120 seconds
Notification interval : 0 Second(s)
Config Trap Interval : 0 seconds
Connection Hold timer : 300 seconds

LLDP MED : Disabled
MED fast start count : 3 Packets

```

Interface	Parent Interface	LLDP	LLDP-MED	Power Negotiation
Neighbor count				
all	-	Enabled	Enabled	Enabled
8				

Interface	Parent Interface	Vlan-id	Vlan-name
xe-3/0/0.0	ae31.0	100	v100
xe-3/0/0.0	ae31.0	101	v101
xe-3/0/0.0	ae31.0	4000	v4000
xe-3/0/1.0	ae31.0	100	v100
xe-3/0/1.0	ae31.0	101	v101
xe-3/0/1.0	ae31.0	4000	v4000
xe-3/0/2.0	ae31.0	100	v100
xe-3/0/2.0	ae31.0	101	v101
xe-3/0/2.0	ae31.0	4000	v4000

LLDP basic TLVs supported:

Chassis identifier, Port identifier, Port description, System name, System description, System capabilities, Management address.

Supported LLDP 802 TLVs:

MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum frame size, Port VLAN tag, Port VLAN name.

Supported LLDP MED TLVs:

LLDP MED capabilities, Network policy, Endpoint location, Extended power Via MDI.

show lldp local-information

Syntax	show lldp local-information
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series.
Description	Display the information that the switch provides in Link Layer Discovery Protocol (LLDP) advertisements to its neighbors.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Configuring LLDP (CLI Procedure) on page 136 • Understanding LLDP and LLDP-MED on EX Series Switches on page 18 • management-address on page 249 • <i>Configuring LLDP</i> • <i>Understanding LLDP</i>
List of Sample Output	show lldp local-information (EX Series Switch) on page 350
Output Fields	Table 32 on page 349 lists the output fields for the show lldp local-information command. Output fields are listed in the approximate order in which they appear.

Table 32: show lldp local-information Output Fields

Field Name	Field Description
LLDP Local Information details	Information about the local system (the switch): <ul style="list-style-type: none"> • Chassis ID—MAC address associated with the switch. • System name—User-configured name of the switch. • System descr—System description containing information about the switch model and the current software image running on the switch. This information is taken from the software and is not configurable.
System Capabilities	Capabilities (such as bridge or router) that are supported or enabled on the system.
Management Information	Details of the management information: Port Name , Port Address (such as 10.204.34.35), Address Type (such as ipv4 or ipv6), Port ID (SNMP interface index), Port ID Subtype , and Port Subtype . <p>The Port Subtype displays:</p> <ul style="list-style-type: none"> • ifindex(2)—IP address of the switch's management Ethernet interface (me0) or virtual management Ethernet (VME) interface address (for a virtual chassis) is used to manage the switch. • unknown(1)—IP management address has been configured with set protocols lldp management-address.

Table 32: show lldp local-information Output Fields (*continued*)

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

Sample Output

show lldp local-information (EX Series Switch)

```
user@switch> show lldp local-information
```

LLDP Local Information details

```
Chassis ID   : 00:1d:b5:aa:b9:f0
System name  : switch
System descr : Juniper Networks, Inc. ex8208 , version 10.4I0 [builder] Build
               date: 2010-11-17 12:38:30 UTC
```

System Capabilities

```
Supported   : Bridge Router
Enabled     : Bridge Router
```

Management Information

```
Port Name    : -
Port Address : 10.93.54.6
Address Type  : IPv4
Port ID       : 34
Port ID Subtype : local(7)
Port Subtype  : ifIndex(2)
```

Interface name	Parent Interface	SNMP Index	Interface description	Status	Tunneling
me0.0	-	34	-	Down	Disabled
xe-3/0/0.0	ae31.0	769	xe-3/0/0.0	Up	Disabled
xe-3/0/1.0	ae31.0	770	xe-3/0/1.0	Up	Disabled
xe-3/0/2.0	ae31.0	771	xe-3/0/2.0	Up	Disabled
xe-3/0/3.0	ae31.0	772	xe-3/0/3.0	Up	Disabled
xe-3/0/4.0	ae31.0	577	xe-3/0/4.0	Up	Disabled
xe-3/0/5.0	ae31.0	578	xe-3/0/5.0	Up	Disabled
xe-3/0/6.0	ae31.0	579	xe-3/0/6.0	Up	Disabled
xe-3/0/7.0	ae31.0	581	xe-3/0/7.0	Up	Disabled

show lldp neighbors

Syntax `show lldp neighbors`
`<interface interface>`

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 136](#)
- [Understanding LLDP and LLDP-MED on EX Series Switches on page 18](#)

List of Sample Output

[show lldp neighbors on page 353](#)
[show lldp neighbors interface ge-0/0/2 on page 354](#)
[show lldp neighbors interface ge-0/0/0.0 \(for a VoIP Avaya Telephone with LLDP-MED Support\) on page 355](#)
[show lldp neighbors interface ge-0/0/5.0 \(with NetBIOS Snooping Enabled on the Switch\) on page 356](#)

Output Fields [Table 33 on page 351](#) lists the output fields for the `show lldp neighbors` command. Output fields are listed in the approximate order in which they appear.

Table 33: 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 33: 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 interface option is used).
Local Information	Information about the local system (appears when the interface option is used).
Index	Local interface index (appears when the interface option is used).
Time to live	Number of seconds for which this information is valid (appears when the interface option is used).
Time mark	Date and timestamp of information (appears when the interface option is used).
Local Interface	Name of the local physical interface (appears when the interface option is used).
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the interface option is used).
Local Port ID	Local interface SNMP index (appears when the interface option is used).
Ageout Count	Number of times the complete set of information advertised by the neighbor has been deleted from LLDP neighbor information maintained by the local system because the information timeliness interval expired (appears when the interface option is used).
Neighbor Information	Information about a neighbor system on the interface (appears when the interface option is used).
Chassis type	Type of chassis identifier supplied, such as Mac address (appears when the interface option is used).
Chassis ID	Chassis identifier of the chassis type listed (appears when the interface option is used).
Port type	Type of port identifier supplied, such as Locally assigned (appears when the interface option is used).
Port ID	Port identifier of the port type listed (appears when the interface option is used).
Port description	The port description field uses the configured port description, the port name or the SNMP ifIndex (appears when the interface option is used).
System name	Name supplied by the system on the interface (appears when the interface option is used).

Table 33: show lldp neighbors Output Fields (*continued*)

Field Name	Field Description
System Description	Description supplied by the system on the interface (appears when the interface option is used).
System capabilities	Capabilities (such as Bridge , Bridge Router , and Bridge Telephone) that are supported or enabled by the system on the interface (appears when the interface option is used).
Management Info	<p>Details of management information: Type (such as IPv4 or IPv6), Address (such as 10.204.34.35), Port ID, Subtype, Interface Subtype, and organization identifier (OID) (appears when the interface option is used).</p> <p>The Interface Subtype displays:</p> <ul style="list-style-type: none"> ifIndex(2)—IP address of the neighbor's management Ethernet interface (me0) or virtual management Ethernet (VME) interface address (for a Virtual Chassis) is used to manage the switch. unknown(1)—Neighbor's IP management address has been configured with set protocols lldp management-address.
Media Info	Additional details about the endpoint device appear when a device that supports LLDP-MED is attached to the interface. The specific details depend upon the capabilities of the device. Details might include: Media endpoint class (such as Class 3 for communication devices such as IP phones), MED Hardware revision , MED Firmware revision , MED Software revision , MED Serial number , MED Manufacturer name , MED Model name .
Organization Info	One or more entries listing remote information by organizationally unique identifier (OUI), Subtype , Index , and Info (appears when the interface option is used).
Age	How long the neighbor has been identified (appears when the interface option is used and NetBIOS snooping is enabled on the switch).
Local Interface	Name of the local physical interface (appears when the interface option is used and NetBIOS snooping is enabled on the switch).
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the interface option is used and NetBIOS snooping is enabled on the switch).
Chassis ID	Chassis identifier of the chassis type listed (appears when the interface option is used and NetBIOS snooping is enabled on the switch).
System name	NetBIOS name of the host (appears when the interface option is used and NetBIOS snooping is enabled on the switch).

Sample Output

show lldp neighbors

```
user@switch> show lldp neighbors
```

Local Interface	Parent Interface	Chassis Id	Port info	System Name
xe-3/0/4.0	ae31.0	b0:c6:9a:63:80:40	xe-0/0/0.0	newyork31
xe-3/0/5.0	ae31.0	b0:c6:9a:63:80:40	xe-0/0/1.0	newyork31
xe-3/0/6.0	ae31.0	b0:c6:9a:63:80:40	xe-0/0/2.0	newyork31
xe-3/0/7.0	ae31.0	b0:c6:9a:63:80:40	xe-0/0/3.0	newyork31
xe-3/0/0.0	ae31.0	b0:c6:9a:63:80:40	xe-0/1/0.0	newyork31
xe-3/0/1.0	ae31.0	b0:c6:9a:63:80:40	xe-0/1/1.0	newyork31
xe-3/0/2.0	ae31.0	b0:c6:9a:63:80:40	xe-0/1/2.0	newyork31
xe-3/0/3.0	ae31.0	b0:c6:9a:63:80:40	xe-0/1/3.0	newyork31

show lldp neighbors interface 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 Avaya Telephone 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  : 169.254.58.17
System name       : JNPRU\
```

show lldp remote-global-statistics

Syntax	show lldp remote-global-statistics
Release Information	Command introduced in Junos OS Release 10.0 for EX Series switches.
Description	Display remote Link Layer Discovery Protocol (LLDP) global statistics.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Configuring LLDP (CLI Procedure) on page 136 • Understanding LLDP and LLDP-MED on EX Series Switches on page 18
List of Sample Output	show lldp remote-global-statistics on page 358
Output Fields	Table 34 on page 357 describes the output fields for the show lldp remote-global-statistics command. Output fields are listed in the approximate order in which they appear.

Table 34: 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

Syntax	show lldp statistics <interface <i>interface</i>>
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display LLDP statistics for all interfaces or for the specified interface.
Options	none —Display LLDP statistics for all interfaces. interface <i>interface</i> —(Optional) Display LLDP statistics for the specified interface.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Configuring LLDP (CLI Procedure) on page 136 • Understanding LLDP and LLDP-MED on EX Series Switches on page 18
List of Sample Output	show lldp statistics on page 360 show lldp statistics interface xe-3/0/0.0 on page 360
Output Fields	Table 35 on page 359 lists the output fields for the show lldp statistics command. Output fields are listed in the approximate order in which they appear.

Table 35: show lldp statistics Output Fields

Field Name	Field Description
Interface	Name of the interface.
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs. NOTE: Because LLDP packets are transmitted and received on member interfaces only, statistics are available only for the member interfaces, not for the aggregated interface.
Received	Total number of LLDP frames received on an interface.
Unknown TLVs	Number of unrecognized LLDP TLVs received on an interface.
With Errors	Number of invalid LLDP TLVs received on an interface.
Discarded	Number of LLDP TLVs received and then discarded on an interface.
Transmitted	Total number of LLDP frames that were transmitted on an interface.
Untransmitted	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

Syntax	show network-access aaa statistics accounting
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for QFX Series switches.
Description	Display authentication, authorization, and accounting (AAA) accounting statistics.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • accounting-server on page 187 • accounting-stop-on-access-deny on page 189 • <i>Configuring RADIUS Accounting</i>
List of Sample Output	show network-access aaa statistics accounting on page 361
Output Fields	Table 36 on page 361 lists the output fields for the show network-access aaa statistics accounting command. Output fields are listed in the approximate order in which they appear.

Table 36: show network-access aaa statistics accounting Output Fields

Field Name	Field Description
Requests received	The number of accounting-request packets sent from a switch to a RADIUS accounting server.
Accounting Response failures	The number of accounting-response failure packets sent from the RADIUS accounting server to the switch.
Accounting Response Success	The number of accounting-response success packets sent from the RADIUS accounting server to the switch.
Requests timedout	The number of requests-timedout packets sent from the RADIUS accounting server to the switch.

Sample Output

show network-access aaa statistics accounting

```

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

```

show network-access aaa statistics authentication

Syntax	show network-access aaa statistics authentication
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for QFX Series switches.
Description	Display authentication, authorization, and accounting (AAA) authentication statistics.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> authentication-server on page 200 Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41
List of Sample Output	show network-access aaa statistics authentication on page 362 show network-access aaa statistics authentication (in QFX Series Switches) on page 362
Output Fields	Table 37 on page 362 lists the output fields for the show network-access aaa statistics authentication command. Output fields are listed in the approximate order in which they appear.

Table 37: 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

Syntax	show network-access aaa statistics dynamic-requests;
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for QFX Series switches.
Description	Display authentication, authorization, and accounting (AAA) authentication statistics for disconnects.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • authentication-server on page 200 • Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 41
List of Sample Output	show network-access aaa statistics authentication on page 364
Output Fields	Table 38 on page 364 lists the output fields for the show network-access aaa statistics dynamic-requests command. Output fields are listed in the approximate order in which they appear.

Table 38: 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

```

show services unified-access-control authentication-table

Syntax	show services unified-access-control authentication-table
Release Information	Command introduced in Junos OS Release 9.4. Options updated in Junos OS Release 12.1.
Description	<p>Display a summary of the authentication table entries configured from the IC Series UAC Appliance. Authentication tables store mappings between traffic sessions and Unified Access Control (UAC) roles. The IC Series appliance uses the roles specified in the mappings to help determine which UAC policies to apply to a session.</p> <p>Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a UAC deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series appliance.</p> <p>You can also use this command to display the content of the authentication table in a user role firewall implementation. The table, pushed from a supporting UAC device, provides the user roles associated with incoming traffic.</p>
Options	<ul style="list-style-type: none"> • detail—Display a detailed view of all authentication table entries. • extended—Display a view of all authentication table entries with the user roles listed. • identifier <i>id</i>—Display all authentication table entries with the specified identifier number. • ip <i>source-ip-address</i>—Display any authentication table entry for the specified IP address. • role <i>role-name</i>—Display all authentication table entries for the specified role name. • user <i>username</i>—Display all authentication table entries for the specified user.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>Firewall User Authentication Overview</i>
List of Sample Output	show services unified-access-control authentication-table on page 365 show services unified-access-control authentication-table detail on page 366 show services unified-access-control authentication-table extended on page 366 show services unified-access-control authentication-table identifier id on page 366 show services unified-access-control authentication-table ip on page 366 show services unified-access-control authentication-table role on page 366 show services unified-access-control authentication-table user username on page 366

Sample Output

show services unified-access-control authentication-table

```

user@host>show services unified-access-control authentication-table
Id      Source IP      Username      Age      Role identifier
1       172.24.72.79   atsang       0        0000000001.000005.0
Total: 1

```

show services unified-access-control authentication-table detail

```
user@host>show services unified-access-control authentication-table detail
Identifier: 1
Source IP: 172.24.72.79
Username: atsang
Age: 0
Role identifier      Role name
0000000001.000005.0 Users
1113249951.100616.0 PersonalFirewall
1183670148.427197.0 UAC
Total: 1
```

show services unified-access-control authentication-table extended

```
user@host>show services unified-access-control authentication-table extended
Id   Source IP      Username      Age  Role name
3    10.214.161.195 prasanta     60   Users, PersonalFirewall
6    10.214.161.183 june        60   role-1
Total: 2
```

show services unified-access-control authentication-table identifier id

```
user@host>show services unified-access-control authentication-table identifier 1
Identifier: 1
Source IP: 172.24.72.79
Username: atsang
Age: 0
Role identifier      Role name
0000000001.000005.0 Users
1113249951.100616.0 PersonalFirewall
1183670148.427197.0 UAC
Total: 1
```

show services unified-access-control authentication-table ip

```
user@host>show services unified-access-control authentication-table ip 10.214.161.183
Id   Source IP      Username      Age  Role identifier
8    10.214.161.183 june          0    1420298444.225667.0
Total: 1
```

show services unified-access-control authentication-table role

```
user@host>show services unified-access-control authentication-table role role-1
Id   Source IP      Username      Age  Role identifier
6    10.214.161.183 june          60   1420298444.225667.0
Total: 1
```

show services unified-access-control authentication-table user username

```
user@host>show services unified-access-control authentication-table user prasanta
Id   Source IP      Username      Age  Role identifier
7    10.214.161.195 prasanta     0    0000000001.000005.0
Total: 1
```

show services unified-access-control policies

Syntax	show services unified-access-control policies
Release Information	Command introduced in Junos OS Release 9.4.
Description	<p>Display a summary of resource access policies configured from the IC Series UAC Appliance.</p> <p>Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series appliance.</p>
Options	<ul style="list-style-type: none"> detail—Display a detailed view of all policies. identifier <i>id</i>—Display information about a specific policy by identification number.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> <i>Firewall User Authentication Overview</i>
List of Sample Output	show services unified-access-control policies on page 367 show services unified-access-control policies detail on page 367 show services unified-access-control policies identifier 1 on page 368

Sample Output

show services unified-access-control policies

```

user@host> services unified-access-control policies
Id      Resource                Action Apply      Role identifier
1       10.100.15.0/24:*        allow selected  1113249951.100616.0
2       10.100.17.0/24:*        deny  all

```

Sample Output

show services unified-access-control policies detail

```

user@host> services unified-access-control policies detail
Identifier: 1
Resource: 10.100.15.0/24:*
Resource: 10.100.16.23-10.100.16.60:*
Action: allow
Apply: selected
Role identifier      Role name
1113249951.100616.0 Personal Firewall
1112927873.881659.0 Antivirus
1183670148.427197.0 UAC
Identifier: 2
Resource: 10.100.17.0/24:*
Resource: 10.100.16.23-10.100.16.60:*
Resource: 10.100.18.0/24:*

```

Action: deny
Apply: all

Sample Output

show services unified-access-control policies identifier 1

```
user@host> show services unified-access-control policies identifier 1
Identifier: 1
Resource: 10.100.15.0/24:*
Resource: 10.100.16.23-10.100.16.60:*
Action: allow
Apply: selected
Role identifier      Role name
1113249951.100616.0 Personal Firewall
1112927873.881659.0 Antivirus
1183670148.427197.0 UAC
```

show services unified-access-control status

Syntax	show services unified-access-control status
Release Information	Command introduced in Junos OS Release 9.4.
Description	<p>Display the status of the connection between the SRX Series device and the IC Series UAC Appliance as well as statistics to help debug connections to the IC Series appliance.</p> <p>Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series appliance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>Firewall User Authentication Overview</i>
List of Sample Output	show services unified-access-control status on page 369

Sample Output

show services unified-access-control status

```

user@host> show services unified-access-control status
Host      Address      Port  Interface  State
dev106vm26 10.64.11.106 11123 ge-0/0/0.0 connected
dev107vm26 10.64.11.106 11123 ge-0/0/0.0 closed

```


PART 4

Troubleshooting

- [Troubleshooting on page 373](#)

CHAPTER 8

Troubleshooting

- [Troubleshooting Authentication of End Devices on EX Series Switches on page 373](#)

Troubleshooting Authentication of End Devices on EX Series Switches

Problem **Description:** End devices configured using static MAC addresses lose connection to the switch after the clear dot1x interface command is run to clear all learned MAC addresses. Before clearing MAC addresses:

```
user@switch# run show ethernet-switching table
Ethernet-switching table: 3 entries, 1 learned, 0 persistent entries
  VLAN      MAC address      Type      Age Interfaces
  ----      -
vlan100     *                Flood     - All-members
default     *                Flood     - All-members
default     00:a0:d4:00:03:00 Learn     0 ge-3/0/16.0

user@switch> show dot1x authentication-bypassed-users
MAC address      Interface      VLAN
00:a0:d4:00:03:00 ge-3/0/16.0    configured/default
```

To clear MAC addresses:

```
user@switch> clear dot1x interface
```

After clearing MAC addresses:

```
user@switch> show ethernet-switching table
Ethernet-switching table: 2 entries, 0 learned, 0 persistent entries
  VLAN      MAC address      Type      Age Interfaces
  ----      -
vlan100     *                Flood     - All-members
default     *                Flood     - All-members

user@switch> show dot1x authentication-bypassed-users
```

Note that there are no end devices on the authentication bypass list.

Cause Static MAC addresses are treated the same as other learned MAC addresses on an interface. When the clear dot1x interface command is run, it clears all learned MAC addresses from the interface, including the static MAC bypass list (also known as the exclusion list).

Solution If you run the `clear dot1x interfaces` command for an interface that has static MAC addresses configured for authentication bypass, re-add the static MAC addresses to the static MAC bypass list.

Related Documentation

- [clear dot1x on page 320](#)
- [Understanding Authentication on EX Series Switches on page 10](#)