Junos® OS for EX Series Ethernet Switches

Access Control on EX4300 Switches

Release
14.1X53

Modified: 2016-11-19

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

Junos® OS for EX Series Ethernet Switches Access Control on EX4300 Switches
Release 14.1X53

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

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

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

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

Supported Platforms

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

- EX Series

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

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

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

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

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

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

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

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/feedback/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Access Control Overview

802.1X for Switches Overview

How 802.1X Authentication Works

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

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

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

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

- Whether or not the end device is 802.1X-enabled.
- Whether or not MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected.
- Whether the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message. See "Configuring Server Fail Fallback (CLI Procedure)" on page 114.

802.1X Features Overview

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

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

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

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

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

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

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

Related Documentation

- Understanding Authentication on Switches on page 6
- Understanding 802.1X and VoIP on page 17
- Understanding 802.1X and LLDP and LLDP-MED on page 14
- Understanding 802.1X and RADIUS Accounting on Switches on page 13
- Understanding Guest VLANs for 802.1X on Switches on page 12
- Understanding 802.1X and VSAs on Switches on page 19
- Understanding Server Fail Fallback and Authentication on Switches on page 20

Understanding Authentication on Switches

You can control access to your network through a Juniper Networks Ethernet Switch using several different authentication methods—802.1X, MAC RADIUS, or captive portal. Authentication prevents unauthorized 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 DHCP server. For captive portal authentication, the switch allows the end devices to get an IP address and allows forwarding of DHCP, DNS, and ARP packets.

You can allow end devices to access the network without authentication by including the MAC address of the end device in the static MAC bypass list or, for captive portal, by including the MAC address of the end device in the authentication whitelist.

You can configure 802.1X, MAC RADIUS, and captive portal on the same interface and in any combination, except that you cannot configure MAC RADIUS and captive portal on an interface without also configuring 802.1X. If you configure multiple authentication methods on a single interface, the switch falls back to another method if the first method is unsuccessful. For a description of the process flow when multiple authentication methods are configured on an interface, see "Authentication Process Flow for Switches" on page 21.

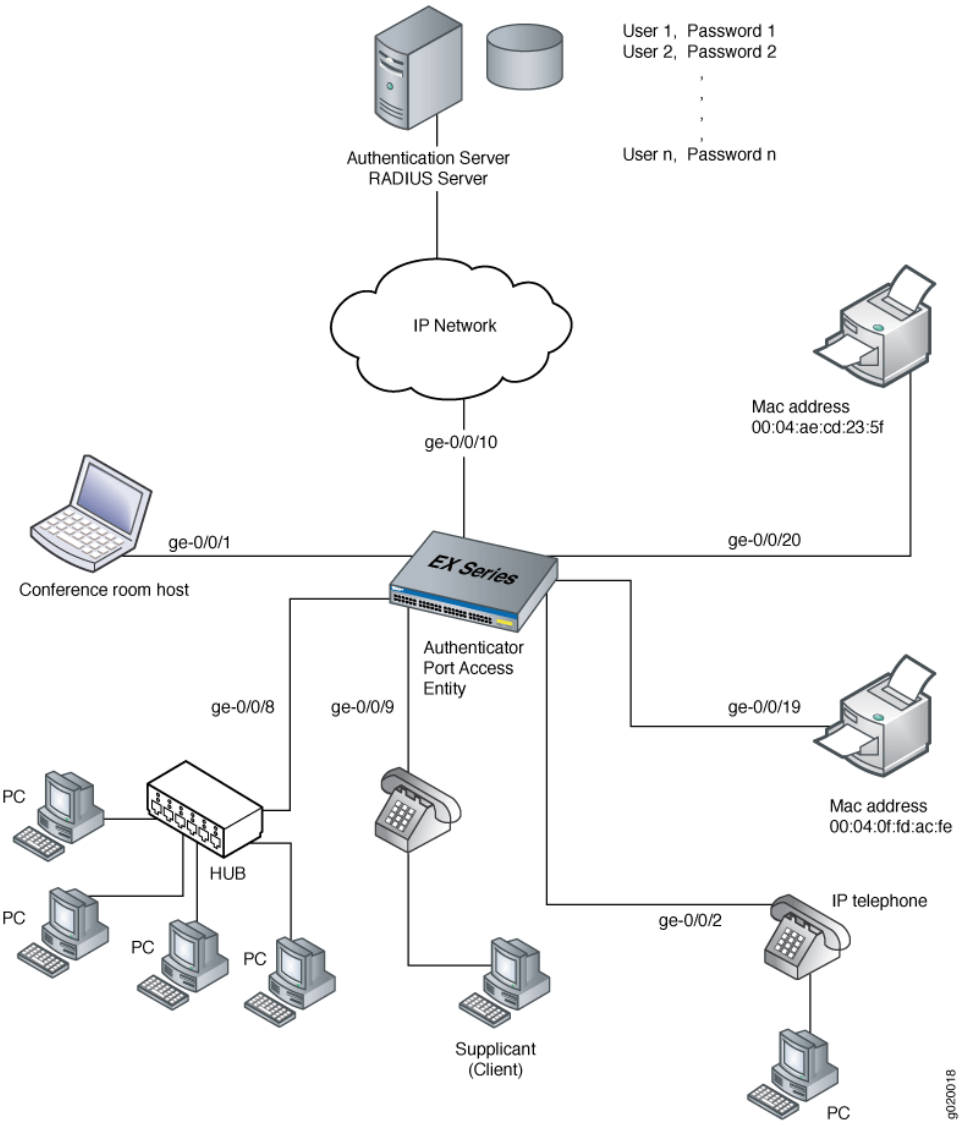
This topic covers:

Sample Basic Authentication Topology

Figure 1 on page 7 illustrates a basic deployment topology for authentication on an EX Series switch:

NOTE: For illustration purposes, we have used an EX Series switch, but a QFX5100 switch can be used in the same way.

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 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 to allow devices to access a LAN. The 802.1X authentication feature on switches is based on the IEEE 802.1D 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 is allowed. Other traffic, such as DHCP and HTTP, 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 102.

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 EAP-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 end devices that are 802.1X-enabled but that have sent the wrong credentials. A server-reject VLAN can provide a remedial connection, typically just to the Internet, for these devices. See"Example: Configuring Fallback Options on Switches for EAP-TTLS Authentication and Odyssey Access Clients" on page 95 for additional information.

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

  A nonresponsive end device is not 802.1X-enabled, but it can be authenticated through MAC RADIUS authentication.

- *Authenticator port access entity*—The IEEE term for the authenticator. The 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 allowed 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 switches support RADIUS authentication servers.

NOTE: You cannot configure 802.1X authentication on redundant trunk groups (RTGs). For more information on 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 but that you want to allow to access the LAN.

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

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 using 802.1X, and if that method fails, it attempts to authenticate the end device 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 while the switch determines that the end device is not 802.1X-enabled by configuring the **mac-radius restrict** option. When this option is configured, 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 permitted on the RADIUS server, the switch opens LAN access to the end device on the interface to which it is connected.

This option is useful when no other 802.1X authentication methods, such as guest VLAN, are needed on the interface. When you configure **mac-radius restrict** on an interface to eliminate the delay caused when the switch attempts to authenticate the end device through 802.1X, the switch drops all 802.1X packets.

Captive Portal Authentication

Captive portal authentication (hereafter referred to as captive portal) allows you to authenticate users on 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. Captive portal controls network access by requiring users to provide information that is authenticated against a RADIUS server database 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) provides a template that allows 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 web page, 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 Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) is enabled, Hypertext Transfer Protocol (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 the 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 switches has the following limitations:

- Captive portal does not support dynamic assignment of VLANs downloaded from the RADIUS server.
- If the user is 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 while the switch determines 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 multiple authentication methods on a single interface to enable fallback to another method if one method fails.

If an interface is configured in multiple supplicant mode, all end devices connecting through the interface must use either captive portal or a combination of 802.1X authentication and MAC RADIUS authentication, captive portal cannot be mixed with 802.1X authentication or MAC RADIUS authentication. Therefore, if there is already an end device on the interface that was authenticated through 802.1X or MAC RADIUS authentication, then additional end devices authenticating do not fall back to captive portal. If only 802.1X authentication or MAC RADIUS authentication is configured, some end devices can be authenticated using 802.1X authentication and others can still be authenticated using MAC RADIUS authentication.

Fallback of authentication methods occurs in the following order:

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 using this method after attempting any other configured authentication methods. If an end device is authenticated on the interface using captive portal, this becomes the active authentication method on the interface. When captive portal is the active authentication method, the switch falls back to 802.1X authentication if there are no sessions in the authenticated state and if the interface receives an EAP packet.

Related Documentation

- 802.1X for Switches Overview on page 3
- Authentication Process Flow for Switches on page 21
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37
- Configuring 802.1X Interface Settings (CLI Procedure) on page 102
- Configuring MAC RADIUS Authentication (CLI Procedure) on page 117
- *Configuring Captive Portal Authentication (CLI Procedure)*
- Configuring Static MAC Bypass of Authentication (CLI Procedure) on page 118
- Controlling Authentication Session Timeouts (CLI Procedure) on page 124

Understanding Guest VLANs for 802.1X on Switches

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

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

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

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

A guest VLAN is not used when MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected. Some end devices, such as a printer, cannot be enabled for 802.1X. The hosts for such devices should be connected to switch interfaces that are configured for MAC RADIUS authentication. See "Configuring MAC RADIUS Authentication (CLI Procedure)" on page 117.

Related Documentation

- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 31
- Understanding Dynamic VLANs for 802.1X on Switches on page 19
- Understanding Authentication on Switches on page 6

Understanding 802.1X and RADIUS Accounting on Switches

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

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

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

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

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

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

Related Documentation

- 802.1X for Switches Overview on page 3
- Example: Connecting a RADIUS Server for 802.1X to a Switch on page 27
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 103

Understanding 802.1X and LLDP and LLDP-MED

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

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

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

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

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

NOTE: PoE is not supported on QFX5100 switches.

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

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

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

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

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

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

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

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

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

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

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

Related Documentation

- *Understanding Layer 2 Protocol Tunneling on EX Series Switches*
- *Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch*
- Configuring LLDP (CLI Procedure) on page 107
- Configuring LLDP-MED (CLI Procedure) on page 111
- *Understanding PoE on EX Series Switches*

Understanding 802.1X and VoIP

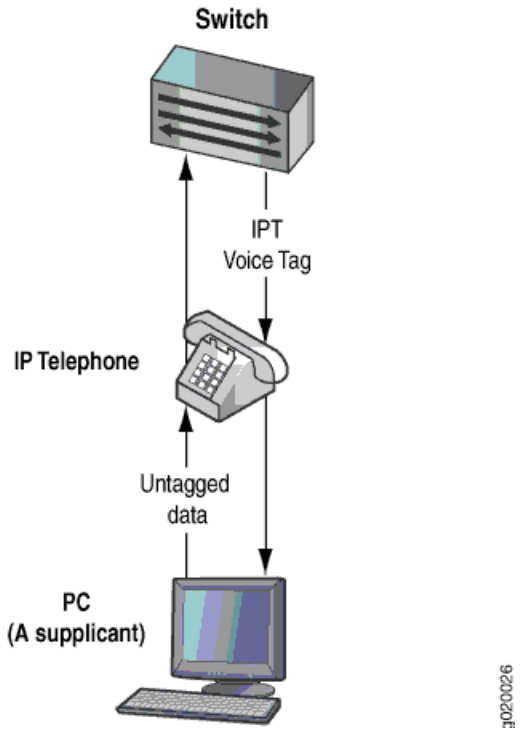
When you use Voice over IP (VoIP), you can connect IP telephones to the switch and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. The 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.

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

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

You can configure 802.1X authentication to work with VoIP in multiple supplicant or single supplicant mode. In *multiple-supplicant* mode, the 802.1X process allows multiple supplicants to connect to the interface. Each supplicant will be authenticated individually. For an example of a VoIP multiple supplicant topology, see Figure 2 on page 17.

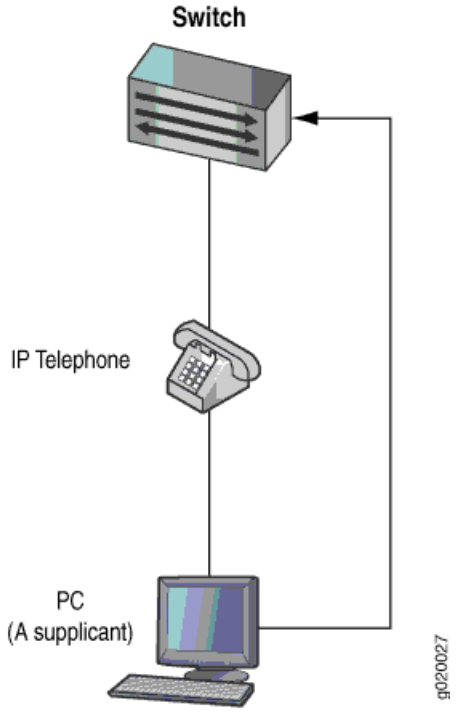
Figure 2: VoIP Multiple Supplicant Topology



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 18 .

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 802.1X and LLDP and LLDP-MED on page 14
- *Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch*
- *Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication*
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 51

Understanding 802.1X and VSAs on Switches

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

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

Besides configuring port-filtering attributes through VSAs, you can apply a port firewall filter that has already been configured on the switch directly to the RADIUS server. Like port-filtering attributes, the filter is applied during the 802.1X authentication process, and its actions are applied at the switch port. Adding a port firewall filter to a RADIUS server eliminates the need to add the filter to multiple ports and switches. For more information, see "Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on a Switch" on page 78.

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

Related Documentation

- Understanding Authentication on Switches on page 6
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37
- Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 105
- *Configuring Firewall Filters (CLI Procedure)*
- VSA Match Conditions and Actions on page 112

Understanding Dynamic VLANs for 802.1X on Switches

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

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

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

Related Documentation

- Understanding Guest VLANs for 802.1X on Switches on page 12
- Example: Configuring MAC RADIUS Authentication on a Switch on page 72
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 31

Understanding Server Fail Fallback and Authentication on Switches

Server fail fallback allows 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 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. An authenticator port access entity (the switch) block all traffic to and from the end device until the end device's credentials are presented and matched on the authentication server. If the end device is configured on the authentication server, the device is granted access to the LAN and the switch opens the interface to the end device.

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 allows you to specify one of four actions to be taken toward 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.

Related Documentation

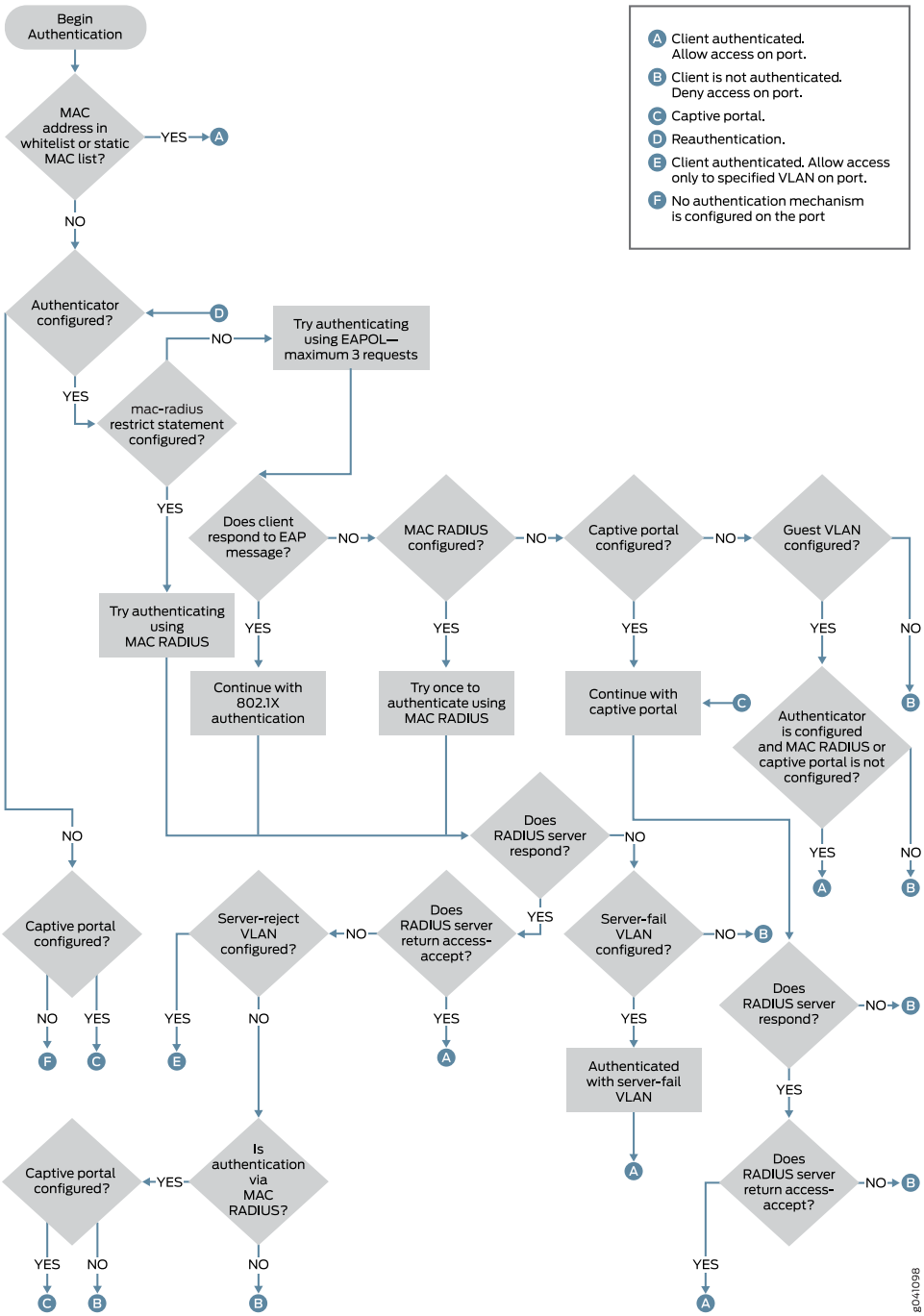
- 802.1X for Switches Overview on page 3
- Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to a Switch on page 66
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37
- Configuring Server Fail Fallback (CLI Procedure) on page 114
- Configuring 802.1X Interface Settings (CLI Procedure) on page 102

Authentication Process Flow for Switches

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

Figure 4 on page 22 illustrates the authentication process:

Figure 4: Authentication Process Flow for Switches



Related Documentation

- Understanding Authentication on Switches on page 6
- Understanding Server Fail Fallback and Authentication on Switches on page 20
- Understanding Guest VLANs for 802.1X on Switches on page 12

- Understanding Dynamic VLANs for 802.1X on Switches on page 19
- *Example: Setting Up Captive Portal Authentication on an EX Series Switch*

Understanding Authentication Session Timeout

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

For captive portal authentication, 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 Switches on page 6
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37
- Controlling Authentication Session Timeouts (CLI Procedure) on page 124
- *Configuring MAC Table Aging (CLI Procedure)*

PART 2

Configuration

CHAPTER 2

Configuration Examples

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

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

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

Requirements

This example uses the following hardware and software components:

NOTE: This example also applies to QFX5100 switches.

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

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

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

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

- Configured users on the RADIUS authentication server.

Overview and Topology

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

Figure 5 on page 29 shows one EX4200 switch that is connected to the devices listed in Table 3 on page 29.

NOTE: This figure also applies to QFX5100 switches.

Figure 5: Topology for Configuration

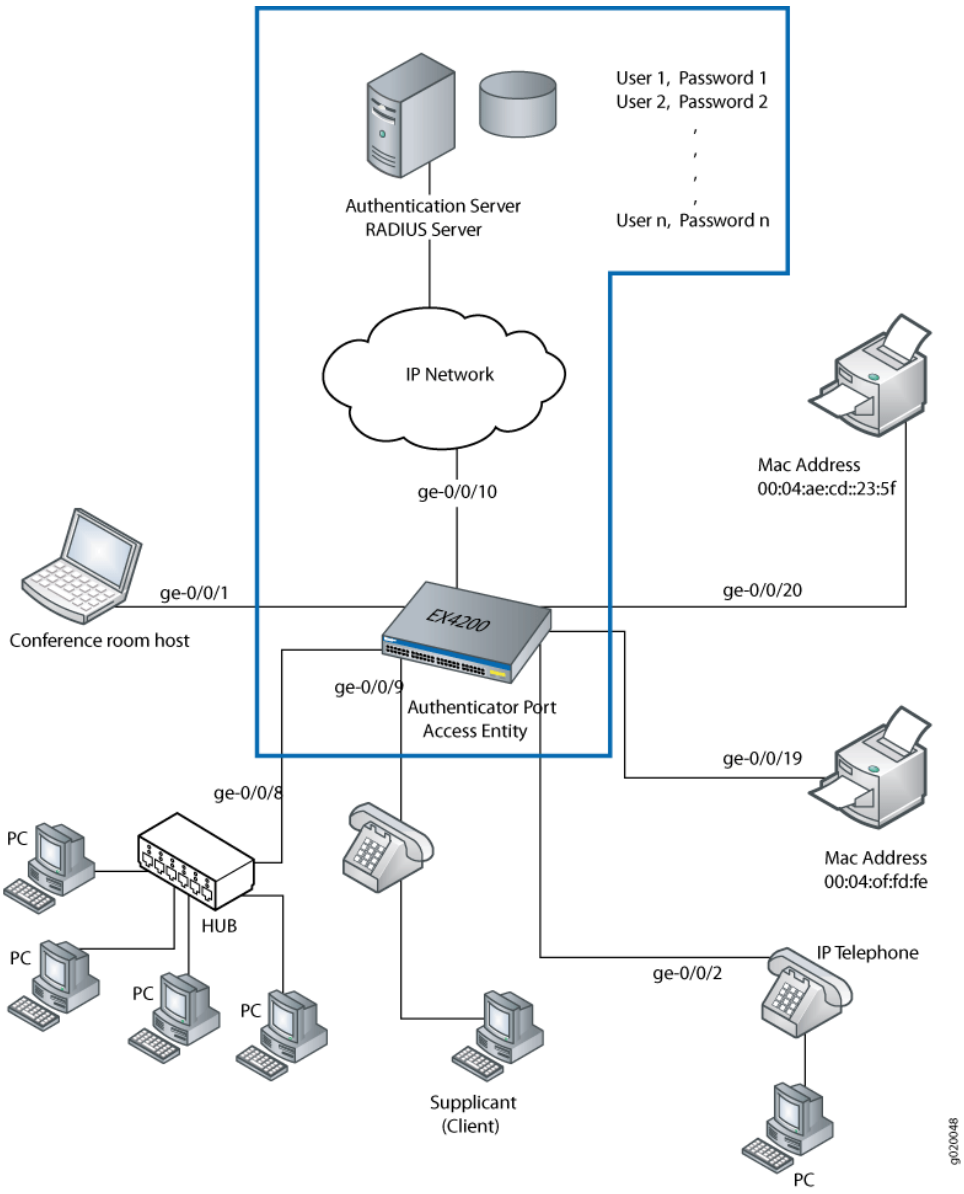


Table 3: Components of the Topology

Property	Settings
Switch hardware	EX4200 access switch, 24 Gigabit Ethernet ports: 8 PoE ports (ge-0/0/0 through ge-0/0/7) and 16 non-PoE ports (ge-0/0/8 through ge-0/0/23)
VLAN name	default

Table 3: Components of the Topology *(continued)*

Property	Settings
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 31

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 Ping the RADIUS server to verify the connection between the switch and the server:

```
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
```

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

- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 31
- *Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch*
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 103
- Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 105

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

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

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

Requirements

This example uses the following hardware and software components:

NOTE: This example also applies to QFX5100 switches.

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

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

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

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

Overview and Topology

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

Figure 6 on page 33 shows the conference room connected to the switch at interface **ge-0/0/1**.

NOTE: This figure also applies to QFX5100 switches.

Figure 6: Topology for Guest VLAN Example

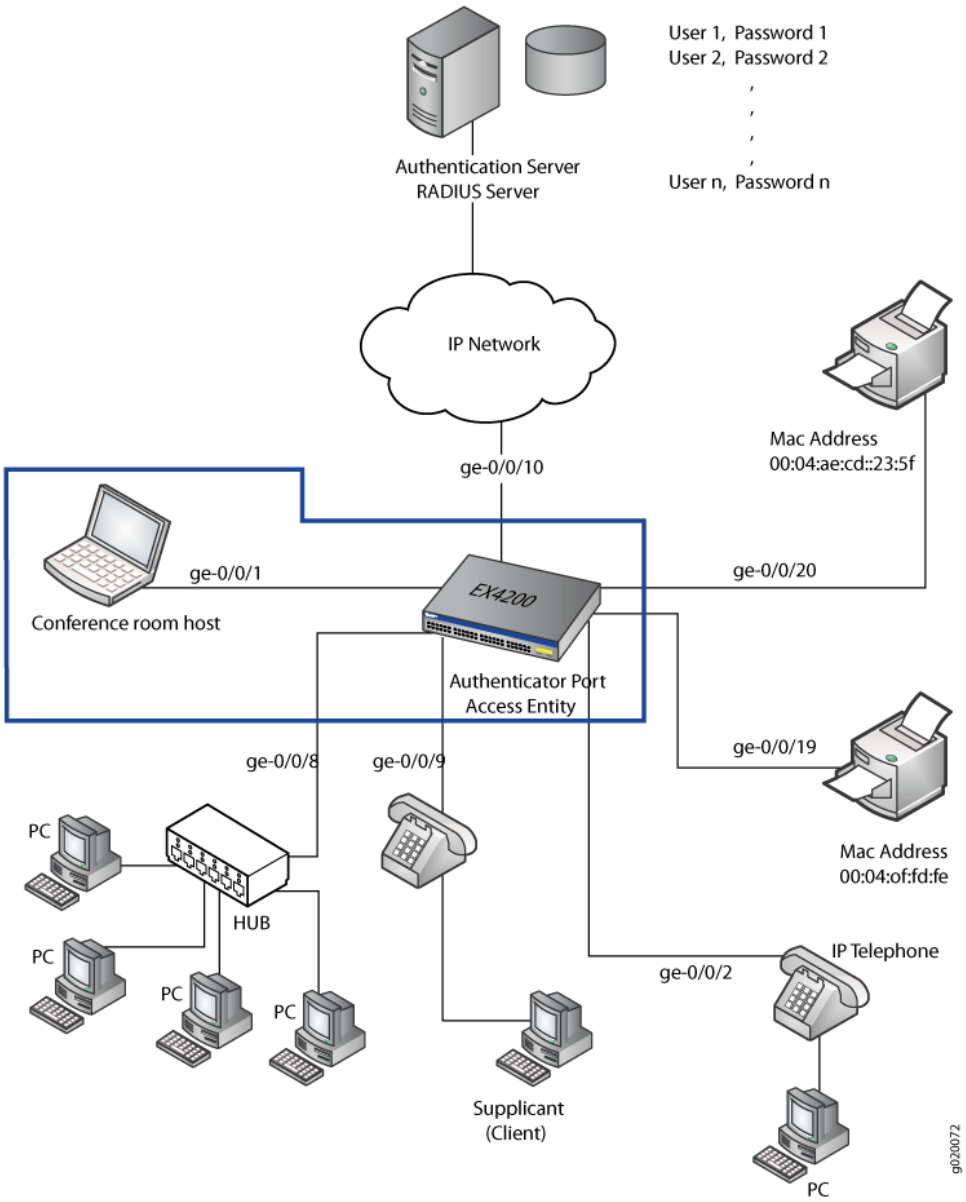


Table 4: Components of the Guest VLAN Topology

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**)

Table 4: Components of the Guest VLAN Topology *(continued)*

Property	Settings
VLAN names and tag IDs	**sales**, tag **100** **support**, tag **200** **guest-vlan**, tag **300**
One RADIUS server	Backend database connected to the switch through interface **ge-0/0/10**

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

Configuration of a Guest VLAN That Includes 802.1X Authentication

CLI Quick Configuration

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

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

Step-by-Step Procedure

To configure a guest VLAN that includes 802.1X authentication on a switch:

1. Configure the VLAN ID for the guest VLAN:

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

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

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

Results

Check the results of the configuration:

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

Verification

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

Verifying That the Guest VLAN is Configured

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

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

Action Issue the operational mode commands:

```
user@switch> show vlans

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

```
user@switch> show dot1x interface ge-0/0/1.0 detail
ge-0/0/1.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: guest-vlan
  Number of connected supplicants: 1
    Supplicant: user1, 00:00:00:00:13:23
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

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

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

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to a Switch on page 27
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37
- *Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch*
- Configuring 802.1X Interface Settings (CLI Procedure) on page 102

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

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

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

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

Requirements

This example uses the following hardware and software components:

NOTE: This example also applies to QFX5100 switches.

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

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

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

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

- Configured users on the authentication server.

Overview and Topology

As shown in Figure 7 on page 39, the topology contains an EX4200 access switch connected to the authentication server on port ge-0/0/10. Interfaces ge-0/0/8, ge-0/0/9, and ge-0/0/11 will be configured for three different administrative modes.

NOTE: This figure also applies to QFX5100 switches.

Figure 7: Topology for Configuring Supplicant Modes

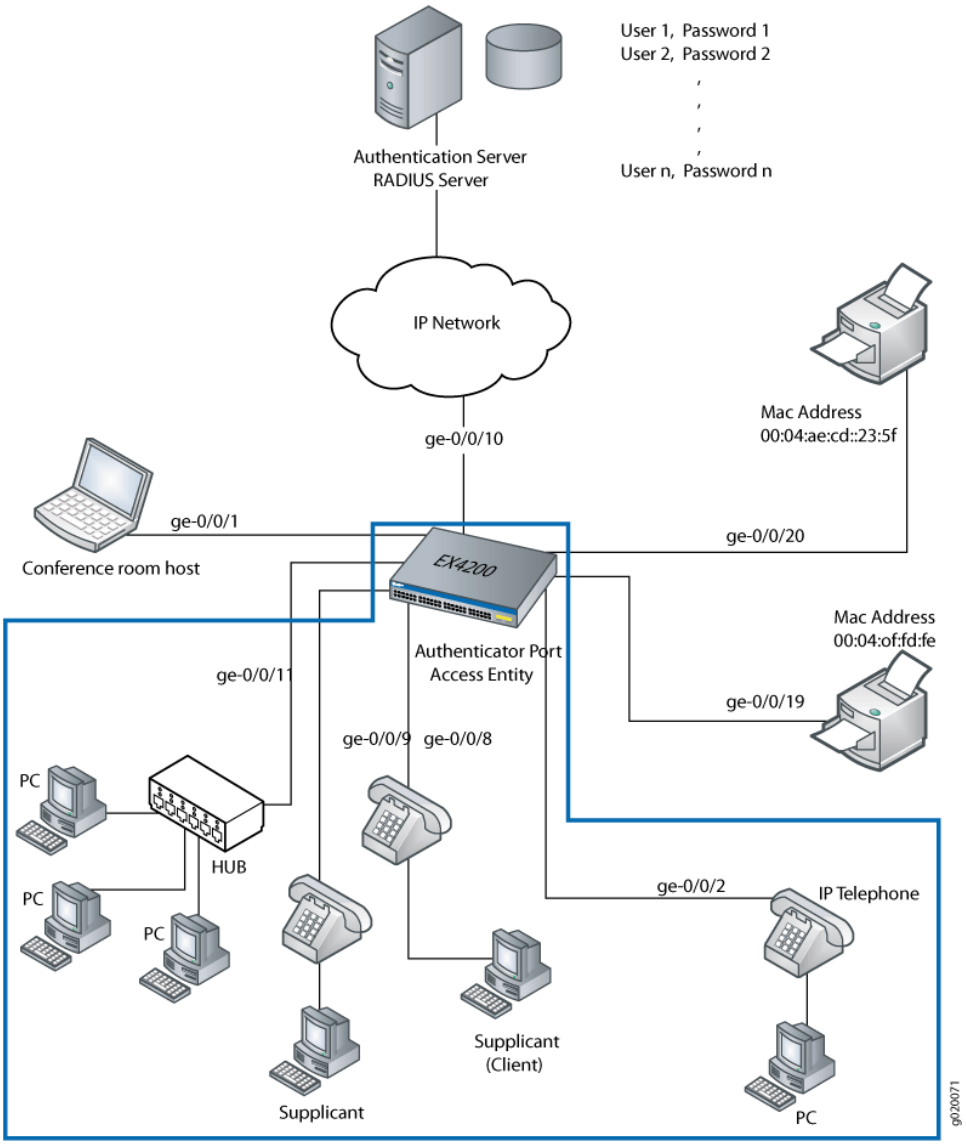


Table 5: Components of the Supplicant Mode Configuration Topology

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.

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 41

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 124
- Example: Connecting a RADIUS Server for 802.1X to a Switch on page 27
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 31
- *Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch*
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 103
- Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 105
- Understanding Authentication on Switches on page 6

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

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

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

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

- Requirements on page 43
- Overview and Topology on page 44
- Configuration on page 46
- Verification on page 48

Requirements

This example uses the following hardware and software components:

NOTE: This example also applies to QFX5100 switches.

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

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

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See the installation information for your switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch* or *Example: Setting Up Basic Bridging and a VLAN on the QFX Series*.
- Configured the RADIUS server for 802.1X authentication and set up the access profile. See "Example: Connecting a RADIUS Server for 802.1X to a Switch" on page 27.
- (Optional) Configured the interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see *Configuring PoE on EX Series Switches (CLI Procedure)*.

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

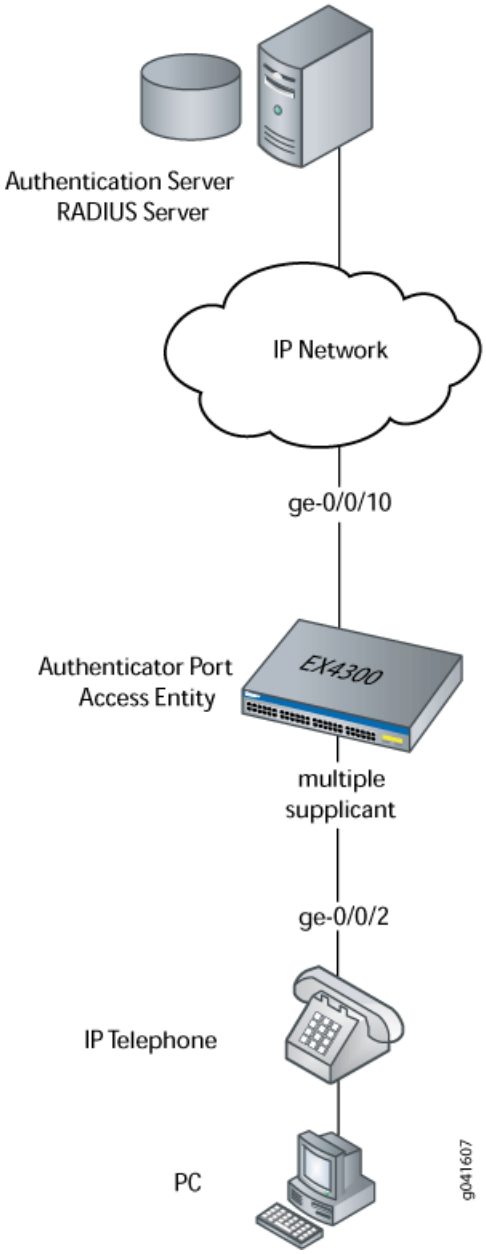
Overview and Topology

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

In this example, the access interface ge-0/0/2 on the EX4300 switch is connected to an Avaya IP telephone. Avaya phones have a built-in bridge that allows you to connect a desktop PC to the phone, so the desktop and phone in a single office require only one interface on the switch. The EX Series switch is connected to a RADIUS server on the ge-0/0/10 interface (see Figure 8 on page 45).

NOTE: This figure also applies to QFX5100 switches.

Figure 8: 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 6 on page 45 describes the components used in this VoIP configuration example.

Table 6: Components of the VoIP Configuration Topology

Property	Settings
Switch hardware	EX4300 switch

Table 6: Components of the VoIP Configuration Topology *(continued)*

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

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

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

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

Configuration

CLI Quick Configuration

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

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

Step-by-Step Procedure

To configure VoIP with LLDP-MED and 802.1X:

1. Configure the VLANs for voice and data:

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

2. Associate the VLAN **data-vlan** with the interface:

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

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

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

4. Configure VoIP on the interface and specify the **assured-forwarding** forwarding class to provide the most dependable class of service:

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

5. Configure LLDP-MED protocol support:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/2
```

6. To authenticate an IP phone and a PC connected to the IP phone on the interface, configure 802.1X authentication support and specify **multiple** supplicant mode:

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

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

Results Display the results of the configuration:

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

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

Verification

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

- Verifying LLDP-MED Configuration on page 48
- Verifying 802.1X Authentication for IP Phone and Desktop PC on page 49
- Verifying the VLAN Association with the Interface on page 50

Verifying LLDP-MED Configuration

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

Action

```
user@switch> show lldp detail
LLDP                     : Enabled
Advertisement interval   : 30 seconds
Transmit delay           : 2 seconds
Hold timer               : 120 seconds
Notification interval    : 0 Second(s)
Config Trap Interval     : 0 seconds
Connection Hold timer    : 300 seconds

LLDP MED                 : Enabled
MED fast start count     : 3 Packets

Port ID TLV subtype      : locally-assigned

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

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

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

 System Description, System Capabilities, Management Address

Organizationally Specific TLVs supported:
MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum Frame Size,

 Port VLAN tag, Port VLAN name.
```

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

Verifying 802.1X Authentication for IP Phone and Desktop PC

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

Action

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

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

Verifying the VLAN Association with the Interface

Purpose Display the interface's VLAN membership.

Action

```
user@switch> show ethernet-switching interface ge-0/0/2.0
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/0/2.0                    65535                                 untagged
             voice-vlan 99
                              65535    Discarding
             data-vlan  77
                              65535    Discarding
```

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

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to a Switch on page 27
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37
- *Defining CoS Forwarding Classes (CLI Procedure)*

- *Defining CoS Forwarding Classes (J-Web Procedure)*
- Configuring LLDP-MED (CLI Procedure) on page 111

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

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*.

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

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 port-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
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 55

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*
- *Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication*
- Understanding 802.1X and VoIP on page 17
- Understanding 802.1X and LLDP and LLDP-MED on page 14

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

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

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

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

This example describes how to configure VoIP on a switch without 802.1X authentication by using static MAC bypass of authentication:

Requirements

This example uses the following hardware and software components:

NOTE: This figure also applies to QFX5100 switches.

- One EX4300 switch.
- Junos OS Release 13.2 or later for EX Series switches
- An Avaya IP telephone

Before you configure VoIP, be sure you have:

- Installed your switch. See the installation information for your switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch* or *Example: Setting Up Basic Bridging and a VLAN on the QFX Series*.
- Configured the RADIUS server for 802.1X authentication and set up the access profile. See "Example: Connecting a RADIUS Server for 802.1X to a Switch" on page 27.
- (Optional) Configured the interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see *Configuring PoE on EX Series Switches (CLI Procedure)*.

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

Overview

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

In this example, the access interface ge-0/0/2 on the EX4300 switch is connected to a non-802.1X IP phone.

To configure VoIP on an EX Series switch to support an IP phone that does not support 802.1X authentication, add the MAC address of the phone as a static entry in the authenticator database and set the supplicant mode to multiple.

Configuration

CLI Quick Configuration

To quickly configure VoIP without using 802.1X authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan switch-options interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set switch-options voip interface ge-0/0/2.0 vlan voice-vlan
set switch-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2
set protocols dot1x authenticator authentication-profile-name auth-profile
set protocols dot1x authenticator static 00:04:f2:11:aa:a7
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Step-by-Step Procedure

To configure VoIP without 802.1X authentication:

1. Configure the VLANs for voice and data:

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

2. Associate the VLAN **data-vlan** with the interface:

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

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

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

4. Configure VoIP on the interface and specify the **assured-forwarding** forwarding class to provide the most dependable class of service:

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

5. Configure LLDP-MED protocol support:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/2
```

6. Set the authentication profile (see "Configuring 802.1X Interface Settings (CLI Procedure)" on page 102 and "Configuring 802.1X RADIUS Accounting (CLI Procedure)" on page 103):

```
[edit protocols]
set dot1x authenticator authentication-profile-name auth-profile
```

7. Add the MAC address of the phone to the static MAC bypass list:

```
[edit protocols]
set dot1x authenticator static 00:04:f2:11:aa:a7
```

8. Set the supplicant mode to **multiple**:

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

Results Display the results of the configuration:

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

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

Verification

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

- Verifying LLDP-MED Configuration on page 59
- Verifying Authentication for the Desktop PC on page 60
- Verifying the VLAN Association with the Interface on page 61

Verifying LLDP-MED Configuration

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

Action

```
user@switch> show lldp detail
LLDP                     : Enabled
Advertisement interval   : 30 seconds
Transmit delay           : 2 seconds
Hold timer               : 120 seconds
Notification interval    : 0 Second(s)
Config Trap Interval     : 0 seconds
Connection Hold timer    : 300 seconds

LLDP MED                 : Enabled
MED fast start count     : 3 Packets

Port ID TLV subtype      : locally-assigned

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

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

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

 System Description, System Capabilities, Management Address

Organizationally Specific TLVs supported:
MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum Frame Size,

 Port VLAN tag, Port VLAN name.
```

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

Verifying Authentication for the Desktop PC

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

Action

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

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

Verifying the VLAN Association with the Interface

Purpose Display the interface's VLAN membership.

Action

```
user@switch> show ethernet-switching interface ge-0/0/2.0
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/0/2.0                    65535                                 untagged
             voice-vlan 99
                              65535    Discarding
             data-vlan  77
                              65535    Discarding
```

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

Related Documentation

- Example: Setting Up VoIP with 802.1X and LLDP-MED on a Switch on page 43
- Understanding 802.1X and VoIP on page 17
- Understanding 802.1X and LLDP and LLDP-MED on page 14

Example: Configuring Static MAC Bypass of Authentication on a Switch

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

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

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

Requirements

This example uses the following hardware and software components:

NOTE: This example also applies to QFX5100 switches.

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

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

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

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

- Specified the RADIUS server connections and configured an access profile on the switch. See "Example: Connecting a RADIUS Server for 802.1X to a Switch" on page 27.

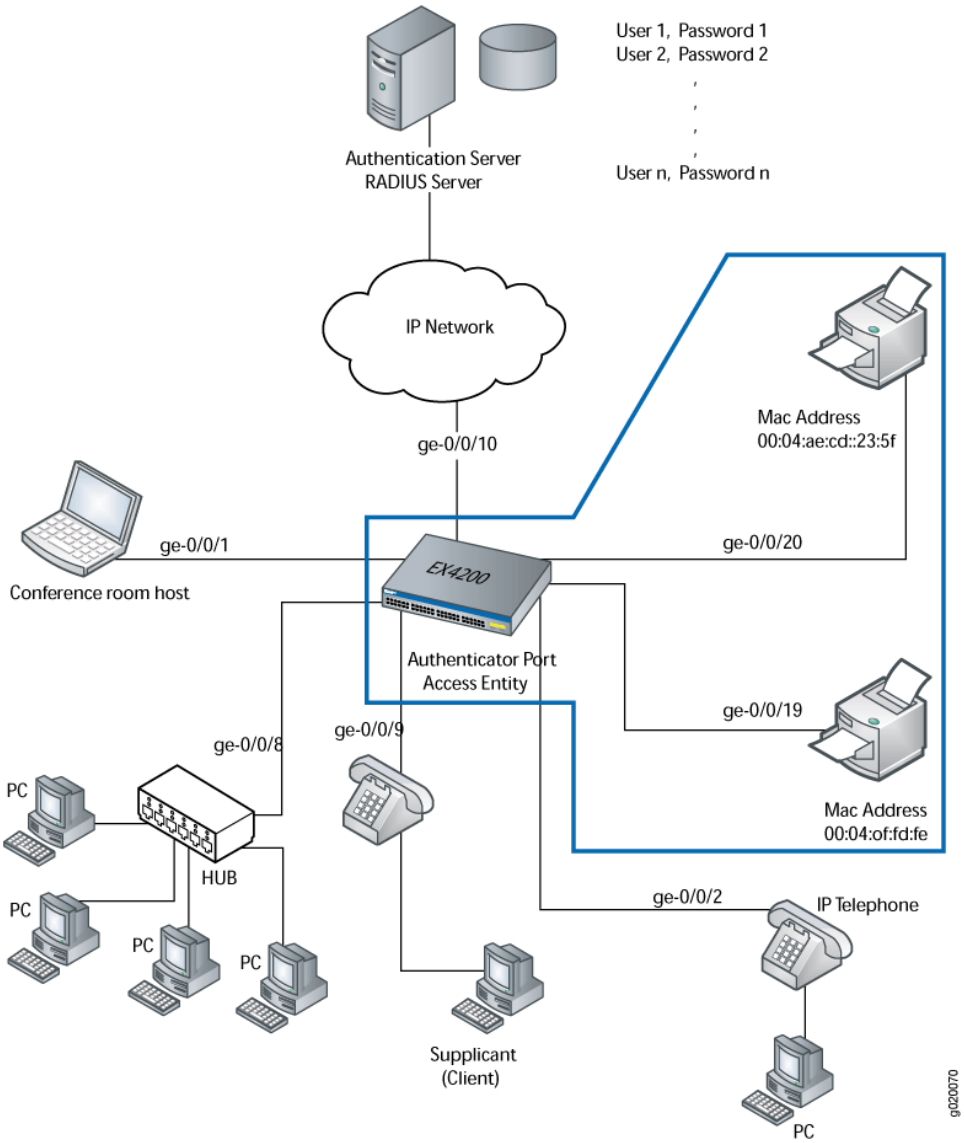
Overview and Topology

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 9 on page 63 shows the two printers connected to the EX4200.

NOTE: This figure also applies to QFX5100 switches.

Figure 9: Topology for Static MAC Authentication Configuration



The interfaces shown in Table 7 on page 64 will be configured for static MAC authentication.

Table 7: Components of the Static MAC Authentication Configuration Topology

Property	Settings
Switch hardware	EX4200, 24 Gigabit Ethernet ports: 8 PoE ports (**ge-0/0/0** through **ge-0/0/23**)
VLAN name	**default**
Connections to integrated printer/fax/copier machines (no PoE required)	**ge-0/0/19**, MAC address 00:04:0f:fd:ac:fe **ge-0/0/20**, MAC address 00:04:ae:cd:23:5f

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

Configuration

CLI Quick Configuration

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

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

Step-by-Step Procedure

Configure static MAC authentication:

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

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

2. Configure the 802.1X authentication method:

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

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

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

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

Results

Display the results of the configuration:

```
user@switch> show
interfaces {
```

```
    ge-0/0/19 {
      unit 0 {
        family ethernet-switching {
          vlan members default;
        }
      }
    }
    ge-0/0/20 {
      unit 0 {
        family ethernet-switching {
          vlan members default;
        }
      }
    }
  }
  protocols {
    dot1x {
      authenticator {
        authentication-profile-name profile1
        static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f];
        interface {
          all {
            supplicant multiple;
          }
        }
      }
    }
  }
```

Verification

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

- Verifying Static MAC Bypass of Authentication on page 65

Verifying Static MAC Bypass of Authentication

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

Action Issue the operational mode command:

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

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

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

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

Related Documentation

- *Configuring 802.1X Authentication (J-Web Procedure)*
- Configuring Static MAC Bypass of Authentication (CLI Procedure) on page 118
- Configuring 802.1X Interface Settings (CLI Procedure) on page 102
- Understanding Authentication on Switches on page 6

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

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

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

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

- Requirements on page 66
- Overview and Topology on page 67
- Configuration on page 69
- Verification on page 70

Requirements

This example uses the following hardware and software components:

NOTE: **This example also applies to QFX5100 switches.**

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

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

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

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

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to a Switch" on page 27.
- Disable firewall filters on the interface. Firewall filters interfere with server fail fallback operation.
- Configured users on the authentication server.

Overview and Topology

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

Figure 10 on page 68 shows the topology used for this example. The RADIUS server is connected to the EX4200 switch on access port **ge-0/0/10**. The switch acts as the authenticator port access entity (PAE) and forwards credentials from the supplicant to the user database on the RADIUS server. The switch blocks all traffic and acts as a control gate until the supplicant is authenticated by the authentication server. A supplicant is connected to the switch through interface **ge-0/0/1**.

NOTE: This figure also applies to QFX5100 switches.

Figure 10: Topology for Configuration

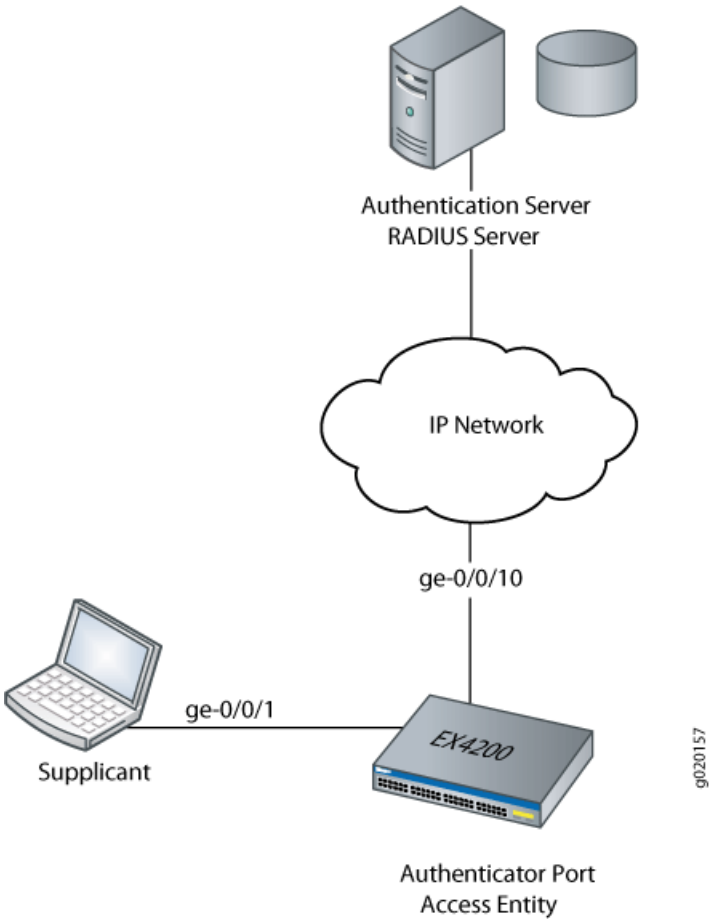


Table 8 on page 68 describes the components in this topology.

Table 8: Components of the Topology

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

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

interface **ge-0/0/1**. When a RADIUS timeout occurs, supplicants on the interface will be moved from the **default** VLAN to the VLAN named **vlan-sf**.

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

Configuration

CLI Quick Configuration

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

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

Step-by-Step Procedure

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

1. Define the VLAN to which supplicants are diverted:

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

Results

Display the results of the configuration:

```
user@switch> show configuration
  interfaces {
    ge-0/0/1 {
      unit 0 {
        family ethernet-switching {
          vlan {
            members default;
          }
        }
      }
    }
  protocols {
    dot1x {
      authenticator {
        authentication-profile-name profile52;
        interface {
          ge-0/0/1.0 {
            server-fail vlan-name vlan-sf;
          }
        }
      }
    }
  }
}
```

Verification

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

- Verifying That the Supplicants Are Moved to an Alternative VLAN During a RADIUS Timeout on page 70

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

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

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

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

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

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

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

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

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

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

```
user@switch> show dot1x interface brief

802.1X Information:
Interface     Role           State           MAC address          User
ge-0/0/1.0    Authenticator  Connecting
ge-0/0/10.0   Authenticator  Initialize
ge-0/0/14.0   Authenticator  Connecting
ge-0/0/15.0   Authenticator  Initialize
ge-0/0/20.0   Authenticator  Initialize
```

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

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

Related Documentation

- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37
- Configuring Server Fail Fallback (CLI Procedure) on page 114
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 103
- Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 105
- Understanding Server Fail Fallback and Authentication on Switches on page 20

Example: Configuring MAC RADIUS Authentication on a Switch

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

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

Requirements

This example uses the following hardware and software components:

NOTE: **This example also applies to QFX5100 switches.**

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

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

- Configured basic access between the EX Series switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to a Switch" on page 27.
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch* or *Example: Setting Up Basic Bridging and a VLAN on the QFX Series*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

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

- Performed basic 802.1X configuration. See "Configuring 802.1X Interface Settings (CLI Procedure)" on page 102.

Overview and Topology

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

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

Figure 11 on page 74 shows the two printers connected to the switch.

NOTE: This figure also applies to QFX5100 switches.

Figure 11: Topology for MAC RADIUS Authentication Configuration

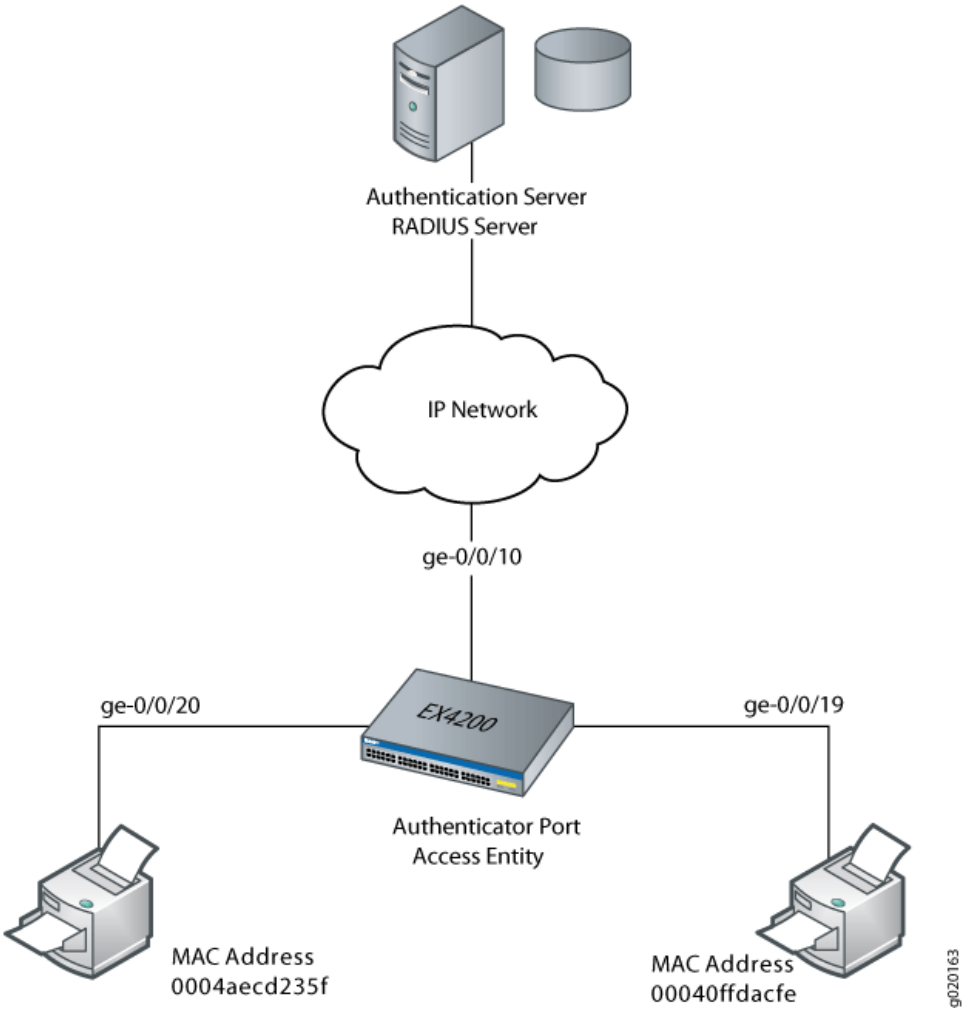


Table 9 on page 74 shows the components in the example for MAC RADIUS authentication.

Table 9: Components of the MAC RADIUS Authentication Configuration Topology

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

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

Configuration

CLI Quick Configuration

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

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

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

Step-by-Step Procedure

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

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

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

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

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

Results

Display the results of the configuration on the switch:

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

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

Verification

Verify that the supplicants are authenticated:

- Verifying That the Supplicants Are Authenticated on page 76

Verifying That the Supplicants Are Authenticated

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

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

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

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

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

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

Related Documentation

- Configuring MAC RADIUS Authentication (CLI Procedure) on page 117
- Configuring 802.1X Interface Settings (CLI Procedure) on page 102
- *Configuring 802.1X Authentication (J-Web Procedure)*
- Understanding Authentication on Switches on page 6

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

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

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

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

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

- Requirements on page 79
- Overview and Topology on page 79
- Configuring the Port Firewall Filter and Counters on page 82
- Applying the Port Firewall Filter to the Supplicant User Profiles on the RADIUS Server on page 84
- Verification on page 84

Requirements

This example uses the following hardware and software components:

NOTE: This example also applies to QFX5100 switches.

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

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

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to a Switch" on page 27.
- 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 102 and "Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch" on page 37.
- Configured users on the RADIUS authentication server (in this example, the user profiles for Supplicant 1 and Supplicant 2 in the topology are modified on the RADIUS server).

Overview and Topology

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

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

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

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

Figure 12 on page 81 shows the topology used for this example. The RADIUS server is connected to an EX4200 switch on access port **ge-0/0/10**. Two end devices (supplicants) are accessing the LAN on interface **ge-0/0/2**. Supplicant 1 has the MAC address **00:50:8b:6f:60:3a**. Supplicant 2 has the MAC address **00:50:8b:6f:60:3b**.

NOTE: This figure also applies to QFX5100 switches.

Figure 12: Topology for Firewall Filter and RADIUS Server Attributes Configuration

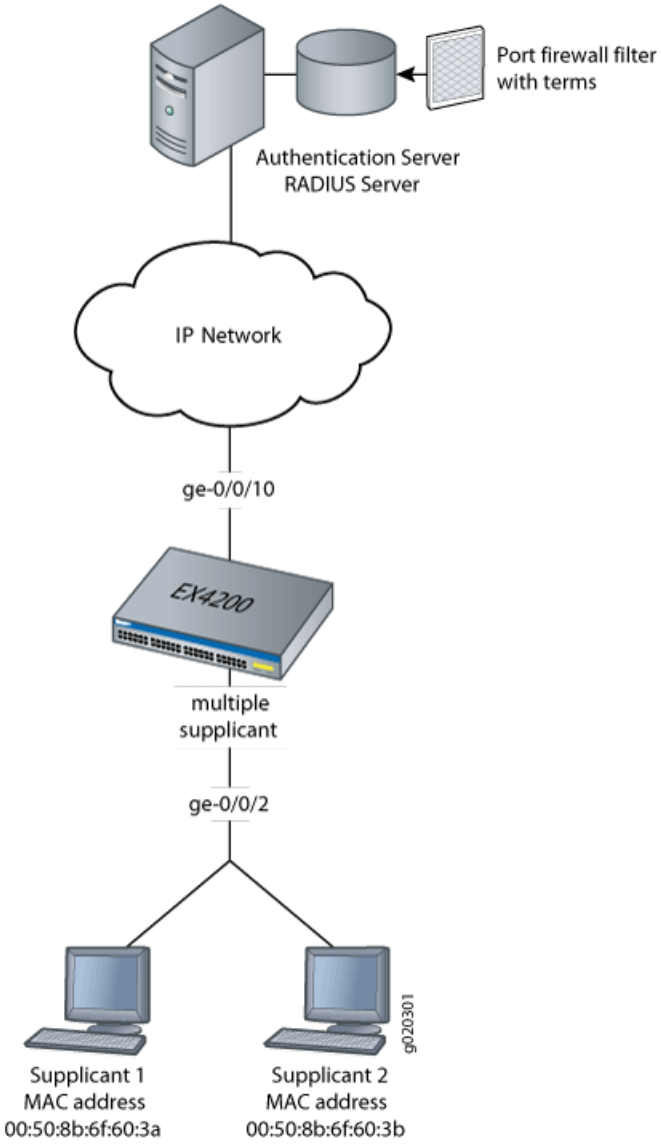


Table 10 on page 81 describes the components in this topology.

Table 10: Components of the Firewall Filter and RADIUS Server Attributes Topology

Property	Settings
Switch hardware	EX4200 access switch, 24 Gigabit Ethernet ports, 8 PoE ports.
One RADIUS server	Backend database with the address **10.0.0.100** connected to the switch at port **ge-0/0/10**.
802.1X supplicants connected to the switch on interface **ge-0/0/2**	• **Supplicant 1** has MAC address **00:50:8b:6f:60:3a**. • **Supplicant 2** has MAC address **00:50:8b:6f:60:3b**.

Table 10: Components of the Firewall Filter and RADIUS Server Attributes Topology *(continued)*

Property	Settings
Port firewall filter to be applied on the RADIUS server	**filter1**
Counters	**counter1** counts packets from Supplicant 1, and **counter2** counts packets from Supplicant 2.
Policer	**policer p1**
User profiles on the RADIUS server	• Supplicant 1 has the user profile **supplicant1**. • Supplicant 2 has the user profile **supplicant2**.

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

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

Configuring the Port Firewall Filter and Counters

CLI Quick Configuration

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

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

Step-by-Step Procedure

To configure a port firewall filter and counters on the switch:

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

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

2. Set policer definition:

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

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

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

Results Display the results of the configuration:

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

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

Step-by-Step Procedure

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

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

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

2. Close the dictionary file.

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

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

   The output shows:

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

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

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

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

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

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

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

Verification

Verifying That the Filter Has Been Applied to the Supplicants

Purpose

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

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

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

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

Related Documentation

- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37
- *Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches*
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 103
- Understanding Authentication on Switches on page 6
- Understanding 802.1X and VSAs on Switches on page 19

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

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

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

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

Requirements

This example uses the following hardware and software components:

NOTE: This example also applies to QFX5100 switches.

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

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

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to a Switch" on page 27.
- Configured 802.1X authentication on the switch, with the authentication mode for the interface ge-0/0/2 set to **multiple**. See "Configuring 802.1X Interface Settings (CLI Procedure)" on page 102 and "Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch" on page 37.
- Configured users on the RADIUS authentication server.

Overview and Topology

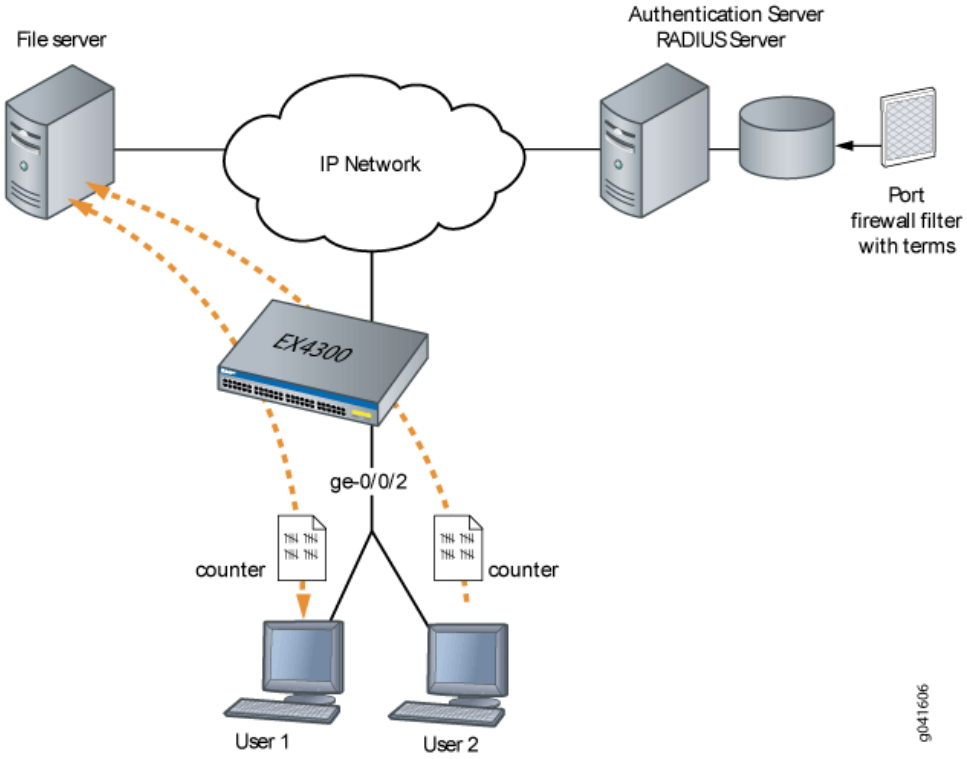
When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines the interface firewall filter with the user policies sent to the switch from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms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

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in Figure 13 on page 87, when User 1 is authenticated

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

NOTE: This figure also applies to QFX5100 switches.

Figure 13: Conceptual Model: Dynamic Filter Updated for Each New User

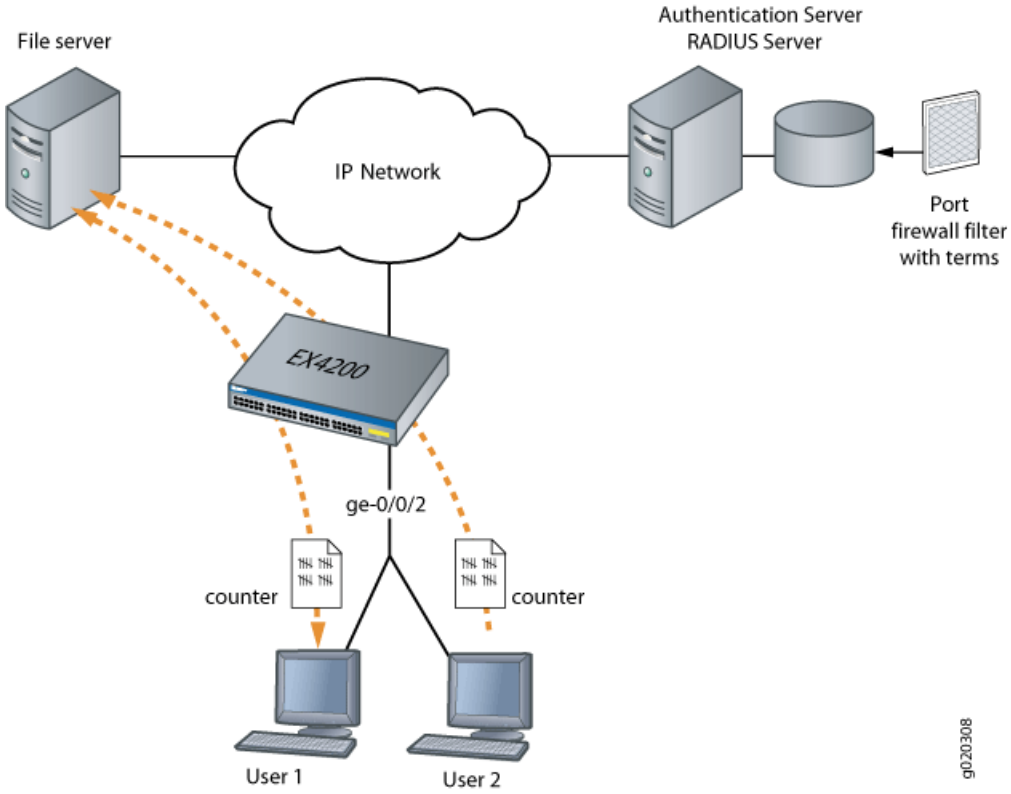


This is a conceptual model of the internal process—you cannot access or view the dynamic filter.

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 14 on page 88 shows the network topology for this example.

Figure 14: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server



Configuration

Configuring Firewall Filters on Interfaces with Multiple Supplicants

CLI Quick Configuration

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

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

Step-by-Step Procedure

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

1. Set the policer definition:

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

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

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

Results Check the results of the configuration:

```
user@switch> show configuration

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

Verification

Verifying Firewall Filters on Interfaces with Multiple Supplicants

Purpose Verify that firewall filters are functioning on the interface with multiple supplicants.

Action

1. Check the results with one user authenticated on the interface. In this case, User 1 is authenticated on ge-0/0/2:

```
user@switch> show dot1x firewall
Filter: dot1x_ge-0/0/2
Counters
counter1_dot1x_ge-0/0/2_user1 100
```

2. When a second user, User 2, is authenticated on the same interface, ge-0/0/2, you can verify that the filter includes the results for both of the users authenticated on the interface:

```
user@switch> show dot1x firewall
Filter: dot1x-filter-ge-0/0/0
Counters
counter1_dot1x_ge-0/0/2_user1 100
counter1_dot1x_ge-0/0/2_user2 400
```

Meaning The results displayed by the **show dot1x firewall** command output reflect the dynamic filter created with the authentication of each new user. User 1 accessed the file server located at the specified destination address 100 times, while User 2 accessed the same file server 400 times.

Related Documentation

- Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on a Switch on page 78
- *Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches*
- Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 105

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

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

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

This example describes how to set up captive portal on an EX4300 switch:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 13.2X50 or later for EX Series switches
- An EX4300 Series switch

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 a Switch" on page 27.
- Designed your captive portal login page. See "Designing a Captive Portal Authentication Login Page on Switches" on page 122.

Overview and Topology

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

The topology for this example consists of one EX4300 switch connected to a RADIUS authentication server. One interface on the switch is configured for captive portal. In this example, the interface is configured in multiple supplicant mode.

Configuration

To configure captive portal on your switch:

CLI Quick Configuration

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

```
[edit]
set system services web-management https local-certificate my-signed-cert
set services captive-portal secure-authentication https
set services captive-portal interface ge-0/0/10.0 supplicant multiple
```

```
set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment vlan1
set custom-options post-authentication-url http://www.my-home-page.com
```

Step-by-Step Procedure

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

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

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

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

   b. Configure captive portal to use HTTPS:

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

2. Enable an interface for captive portal:

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

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

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

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

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

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

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

Results Display the results of the configuration:

```
[edit]
user@switch# show
system {
  services {
    web-management {
      https {
        local-certificate my-signed-cert;
      }
    }
  }
}
security {
  certificates {
    local {
      my-signed-cert {
        "-----BEGIN RSA PRIVATE KEY-----\nMIICXwIBAAKBgQDk8sUggnXdDUmr7T
          vLv63yJq/LRpDASfIDZlX3z9ZDe1Kfk5C9\nr/tkyvzv
          ...
          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;
    custom-options {
      post-authentication-url http://www.my-home-page.com;
    }
  }
}
switch-options {
  authentication-whitelist {
    00:10:12:e0:28:22/48 {
      vlan-assignment vlan1;
    }
  }
}
```

Verification

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

- Verifying That Captive Portal Is Enabled on the Interface on page 94
- Verify That Captive Portal Is Working Correctly on page 94

Verifying That Captive Portal Is Enabled on the Interface

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

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

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

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

Verify That Captive Portal Is Working Correctly

Purpose Verify that captive portal is working on the switch.

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

Troubleshooting

To troubleshoot captive portal, perform this task:

- Troubleshooting Captive Portal on page 94

Troubleshooting Captive Portal

Problem The switch does not return the captive portal login page when a user connected to a captive portal interface on the switch requests a webpage.

Solution You can examine the ARP, DHCP, HTTPS, and DNS counters—if one or more of these counters are not incrementing, this provides an indication of where the problem lies. For example, if the client cannot get an IP address, you might check the switch interface to determine whether the DHCP counter is incrementing—if the counter increments, the DHCP packet was received by the switch.

```
user@switch> show captive-portal firewall ge-0/0/10.0
ge-0/0/10.0
  Filter name: dot1x_ge-0/0/10
Counters:
Name                                Bytes              Packets
dot1x_ge-0/0/10_CP_arp               7616                  119
dot1x_ge-0/0/10_CP_dhcp                 0                    0
```

```
dot1x_ge-0/0/10_CP_http          0                0
dot1x_ge-0/0/10_CP_https         0                0
dot1x_ge-0/0/10_CP_t_dns         0                0
dot1x_ge-0/0/10_CP_u_dns         0                0
```

Related Documentation

- Configuring Captive Portal Authentication (CLI Procedure) on page 120
- Designing a Captive Portal Authentication Login Page on Switches on page 122

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

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

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

- Requirements on page 95
- Overview and Topology on page 96
- Configuration on page 97
- Verification on page 99

Requirements

This example uses the following hardware and software components:

NOTE: This example also applies to QFX5100 switches.

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

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

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to a Switch" on page 27.
- Configured EAP-TTLS on the server. See your RADIUS server documentation.

- Configured users on the RADIUS server. See your RADIUS server documentation.

Overview and Topology

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

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

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

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

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

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

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

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

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

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

Figure 15 on page 97 shows an EX Series switch connecting an OAC end device to a RADIUS server, and indicates the protocols being used to connect the network entities.

NOTE: This figure also applies to QFX5100 switches.

Figure 15: EX Series Switch Connecting OAC to RADIUS Server Using EAP-TTLS Authentication

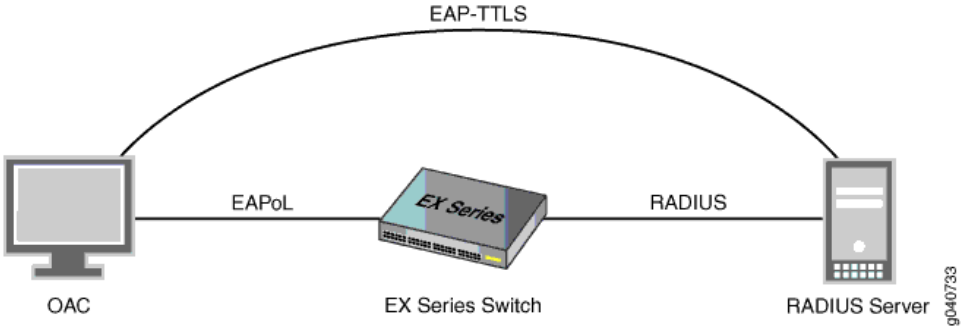


Table 11 on page 97 describes the components in this OAC deployment:.

Table 11: Components of the OAC Deployment

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

Configuration

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

CLI Quick Configuration

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

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

set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan block-interval 130

Step-by-Step Procedure

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

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

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

```
[edit]
user@switch# set vlans remedial vlan-id 700
```

2. Configure the number of times for the client to be prompted for username and password before an incorrect login is directed to the server-reject VLAN:

```
[edit protocols dot1x authenticator interface ge-0/0/8]
user@switch# set retries 4
```

3. Configure the 802.1X authenticator interface to use the server-reject VLAN as a fallback for incorrect logins:

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

4. Enable the EAPoL block timer on the 802.1X interface that is configured to belong to the server-reject VLAN.

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

5. Configure the amount of time for the EAPoL block to remain in effect:

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

Results

Check the results of the configuration:

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

Verification

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

- Verifying the Configuration of the 802.1X Interface on page 99

Verifying the Configuration of the 802.1X Interface

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

Action

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

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

Related Documentation

- Understanding Authentication on Switches on page 6

CHAPTER 3

Configuration Tasks

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 can that can bypass authentication and be automatically connected to the LAN. See "Configuring Static MAC Bypass of Authentication (CLI Procedure)" on page 118.
- You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.
- You cannot configure 802.1X user authentication on redundant trunk groups (RTGs). For more information on RTGs, see *Understanding Redundant Trunk Links* .

Before you begin, specify the RADIUS server or servers to be used as the authentication server. See "Specifying RADIUS Server Connections on Switches (CLI Procedure)" on page 119.

To configure 802.1X on an interface:

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

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface interface-name supplicant multiple
   ```
2. Enable reauthentication and specify the reauthentication interval:

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface interface-name reauthentication interval seconds
   ```
3. Configure the interface timeout value for the response from the supplicant:

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface interface-name supplicant-timeout seconds
   ```
4. Configure the timeout for the interface before it resends an authentication request to the RADIUS server:

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface interface-name server-timeout seconds
   ```
5. Configure how long, in seconds, the interface waits before retransmitting the initial EAPOL PDUs to the supplicant:

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

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

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

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

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

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

Related Documentation

- *Configuring 802.1X Authentication (J-Web Procedure)*
- *Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch*
- Monitoring 802.1X Authentication on page 197
- Verifying 802.1X Authentication on page 198
- Configuring LLDP (CLI Procedure) on page 107
- Understanding Authentication on Switches on page 6

Configuring 802.1X RADIUS Accounting (CLI Procedure)

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

To configure basic RADIUS accounting by using the CLI:

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

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

2. Define the RADIUS accounting servers:

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

3. Enable accounting for an access profile:

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

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

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

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

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

6. Display accounting statistics collected on the switch:

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

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

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

detail-20071214


[root@freeradius 122.69.1.250]# vi details-20071214

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

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

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to a Switch on page 27
- Understanding 802.1X and RADIUS Accounting on Switches on page 13

Filtering 802.1X Supplicants By Using RADIUS Server Attributes

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

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

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

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

This topic includes the following tasks:

1. Configuring Match Statements on the RADIUS Server on page 105
2. Applying a Port Firewall Filter from the RADIUS Server on page 107

Configuring Match Statements on the RADIUS Server

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

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

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

See "VSA Match Conditions and Actions" on page 112 for definitions of match statement options.

To configure match conditions on the RADIUS server:

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

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

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

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

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

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

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

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

   - To deny access based on a destination IP address:

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

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

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

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

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

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

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

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

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

Applying a Port Firewall Filter from the RADIUS Server

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

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

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

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

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

   ```
   [root@freeradius]#
   cd /usr/local/pool/raddb
   vi users
   ```
3. For each relevant user, add the filter (here, the filter ID is **filter1**):

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

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

Related Documentation

- Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on a Switch on page 78
- *Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches*
- Configuring 802.1X Interface Settings (CLI Procedure) on page 102
- Understanding 802.1X and VSAs on Switches on page 19

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

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

- To configure LLDP on all interfaces:

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

- To configure LLDP on a specific interface:

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

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

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

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

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

Adjusting LLDP Advertisement Settings

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

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

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

For example, using the default value:

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

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

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

  For example, using the default value:

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

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

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

  For example:

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

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

Adjusting SNMP Notification Settings of LLDP Changes

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

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

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

  For example:

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

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

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

  For example:

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

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

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

For example:

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

Specifying a Management Address for the LLDP Management TLV

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

To configure the management address:

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

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

Configuring LLDP Power Negotiation

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

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

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

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

- To disable LLDP power negotiation on switch interfaces:

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

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

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

Related Documentation

- *Configuring LLDP (J-Web Procedure)*
- Configuring LLDP-MED (CLI Procedure) on page 111
- Understanding 802.1X and LLDP and LLDP-MED on page 14

Configuring LLDP-MED (CLI Procedure)

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

LLDP-MED is turned on by default.

This topic describes:

- Enabling LLDP-MED on Interfaces on page 111
- Configuring Location Information Advertised by the Switch on page 111
- Configuring for Fast Start on page 112

Enabling LLDP-MED on Interfaces

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

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

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

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

Configuring Location Information Advertised by the Switch

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

- To specify a location by geography:

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

```
user@switch# set interface ge-0/0/2.0 location civic-based ca-type 21 ca-value “Holiday Market”
```

- To specify a location using an **elin** string:

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

Configuring for Fast Start

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

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

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

Related Documentation

- *Configuring LLDP (J-Web Procedure)*
- *Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch*
- Example: Setting Up VoIP with 802.1X and LLDP-MED on a Switch on page 43
- Configuring LLDP (CLI Procedure) on page 107
- Understanding 802.1X and LLDP and LLDP-MED on page 14

VSA Match Conditions and Actions

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

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

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

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

Table 12 on page 113 describes the match conditions you can specify when configuring a VSA using the **match** command on the RADIUS server. The string that defines a match condition is called a *match statement*.

Table 12: Match Conditions

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

When you define one or more terms that specify the filtering criteria, you also define the action to take if the packet matches all criteria. Table 13 on page 114 shows the actions that you can specify in a term.

Table 13: Actions for VSAs

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

Related Documentation

- Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 105
- Understanding 802.1X and VSAs on Switches on page 19
- *Understanding VSAs*

Configuring Server Fail Fallback (CLI Procedure)

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

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

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

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

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

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

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

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

To configure 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
  ```

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

To configure a server reject fallback VLAN:

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

Release History Table

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

Related Documentation

- Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to a Switch on page 66
- *Configuring 802.1X Authentication (J-Web Procedure)*
- Configuring 802.1X Interface Settings (CLI Procedure) on page 102
- Monitoring 802.1X Authentication on page 197
- Understanding Server Fail Fallback and Authentication on Switches on page 20
  ```

Configuring MAC RADIUS Authentication (CLI Procedure)

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

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

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

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

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

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

- Configured basic access between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to a Switch" on page 27.

To configure MAC RADIUS authentication using the CLI:

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

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

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

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

Related Documentation

- Example: Configuring MAC RADIUS Authentication on a Switch on page 72
- Verifying 802.1X Authentication on page 198

- Understanding Authentication on Switches on page 6

Configuring Static MAC Bypass of Authentication (CLI Procedure)

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

To configure the static MAC bypass list:

- Specify a MAC address to bypass authentication:

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

- Configure a supplicant to bypass authentication if connected through a particular interface:

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

- You can configure a supplicant to be moved to a specific VLAN after it is authenticated:

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

Related Documentation

- Example: Configuring Static MAC Bypass of Authentication on a Switch on page 62
- Configuring 802.1X Interface Settings (CLI Procedure) on page 102
- *Configuring 802.1X Authentication (J-Web Procedure)*

Specifying RADIUS Server Connections on Switches (CLI Procedure)

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

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

To configure a RADIUS server on the switch:

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

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

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

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

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

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

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

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

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

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

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

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

Related Documentation

- Configuring 802.1X Interface Settings (CLI Procedure) on page 102
- *Configuring 802.1X Authentication (J-Web Procedure)*
- Configuring MAC RADIUS Authentication (CLI Procedure) on page 117
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 103

Configuring Captive Portal Authentication (CLI Procedure)

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

Configure captive portal authentication (hereafter referred to as captive portal) on a 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 switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to a Switch" on page 27.
- Designed your captive portal login page. See "Designing a Captive Portal Authentication Login Page on Switches" on page 122.

This topic includes the following tasks:

- Configuring Secure Access for Captive Portal on page 120
- Enabling an Interface for Captive Portal on page 121
- Configuring Bypass of Captive Portal Authentication on page 121

Configuring Secure Access for Captive Portal

To configure secure access for captive portal:

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

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

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

2. Configure captive portal to use HTTPS:

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

Enabling an Interface for Captive Portal

To enable an interface for use with captive portal authentication:

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

Configuring Bypass of Captive Portal Authentication

You can allow specific clients to bypass captive portal authentication:

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

NOTE: Optionally, you can use **set switch-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** *session-mac-addr* command after adding its MAC address to the whitelist. Otherwise the new entry for the MAC address will not be added to the Ethernet switching table and the authentication bypass will not be allowed.

Related Documentation

- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 90
- Understanding Authentication on Switches on page 6

Designing a Captive Portal Authentication Login Page on Switches

You can set up captive portal authentication on your switch to redirect all Web browser requests to a login page that requires the user to input a username and password before they are allowed access. Upon successful authentication, the user is 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 16 on page 122 shows an example of a captive portal login page:

Figure 16: Example of a Captive Portal Login Page

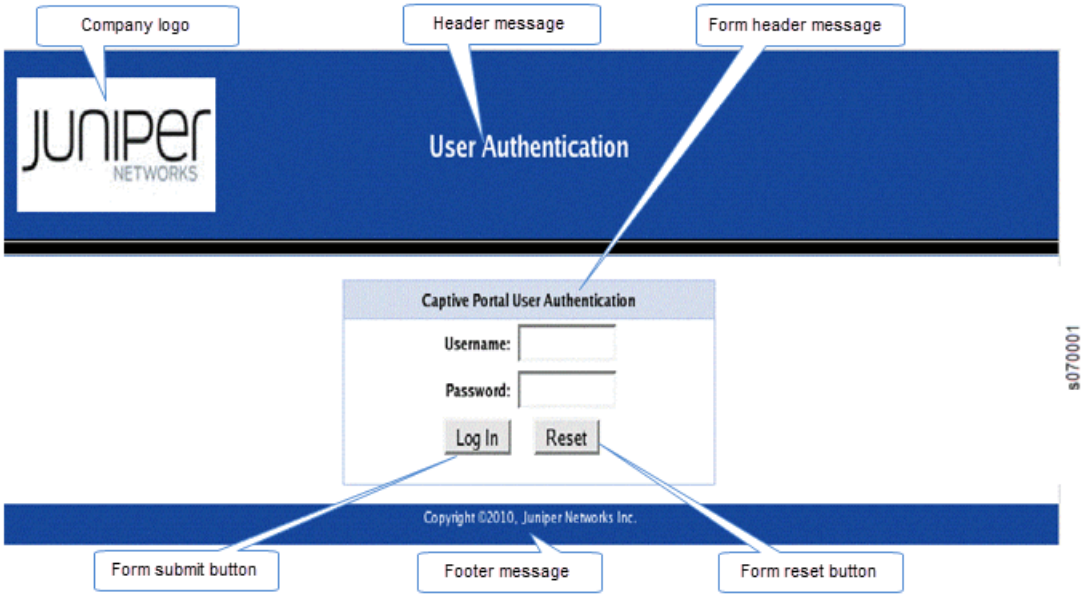


Table 14 on page 122 summarizes the configurable elements of a captive portal login page.

Table 14: Configurable Elements of a Captive Portal Login Page

Element	CLI Statement	Description
Footer background color	**footer-bgcolor** *hex-color*	The HTML hexadecimal code for the background color of the captive portal login page footer.

Table 14: Configurable Elements of a Captive Portal Login Page *(continued)*

Element	CLI Statement	Description
Footer message	**footer-message** ***text-string***	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** ***color***	Color of the text in the footer. The default color is white.
Form header background color	**form-header-bgcolor** ***hex-color***	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** ***text-string***	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** *color*	Color of the text in the form header. The default color is black.
Form reset button label	**form-reset-label** ***label-name***	Using the **Reset** button, the user can clear the username and password fields on the form.
Form submit button label	**form-submit-label** ***label-name***	Using the **Login** button, the user can submit the login information.
Header background color	**header-bgcolor** ***hex-color***	The HTML hexadecimal code for the background color of the captive portal login page header.
Header logo	**header-logo** ***filename***	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** ***text-string***	Text displayed in the page header. The default text is **User Authentication**.
Header text color	**header-text- color***color*	Color of the text in the header. The default color is white.
Post-authentication URL	**post-authentication-url** ***url***	URL to which the users are directed on successful authentication. By default, users are directed to the page they had originally requested.

To design the captive portal login page:

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

   ```
   user@switch> file copy ftp://username:prompt@ftp.hostname.net/var/tmp/my-logo.jpeg
   ```

2. Configure the custom options to specify the background colors and text displayed in the captive portal page:

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

Now you can commit the configuration.

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

Related Documentation

- *Example: Setting Up Captive Portal Authentication on an EX Series Switch*
- Understanding Authentication on Switches on page 6
- *captive-portal*

Controlling Authentication Session Timeouts (CLI Procedure)

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

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

Before you begin:

- Specify the RADIUS server or servers to be used as the authentication server. See “Specifying RADIUS Server Connections on Switches (CLI Procedure)” on page 119.
- Configure 802.1X authentication on the switch. See “Configuring 802.1X Interface Settings (CLI Procedure)” on page 102.

To configure the authentication session time on all interfaces:

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

To configure the authentication session time on a single interface:

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

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

To remove the binding:

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

Related Documentation

- *Configuring MAC Table Aging (CLI Procedure)*
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37
- Understanding Authentication on Switches on page 6
- Understanding Authentication Session Timeout on page 23

CHAPTER 4

Configuration Statements

[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 *EX Series Switch Software Features Overview*.

This topic lists:

- Supported Statements in the [edit access] Hierarchy Level on page 129
- Unsupported Statements in the [edit access] Hierarchy Level on page 134

Supported Statements in the [edit access] Hierarchy Level

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

```
access {
  address-assignment {
    abated-utilization;
    abated-utilization-v6;
    high-utilization;
    high-utilization-v6;
    neighbor-discovery-router-advertisement;
    pool name {
      family {
        inet {
          dhcp-attributes {
            boot-file filename;
            boot-server server-address;
            domain-name domain-name;
            grace-period seconds;
            maximum-lease-time (length | infinite);
            name-server ip-address;
            netbios-node-type (b-node | h-node | m-node | p-node);
            option option-identifier-code;
            option-match {
              option-82 {
                circuit-id match-value;
                remote-id match-value;
              }
            }
            router ip-address;
            server-identifier;
            tftp-server;
            wins-server ip-address;
```

```
            }
            host;
            network;
            range;
            xauth-attributes;
          }
          inet6 {
            dhcp-attributes;
            prefix;
            range;
          }
        }
        link name {
          family {
            inet;
            inet6;
          }
        }
      }
    }
    address-pool pool-name {
      address address-or-prefix;
      address-range <low lower-limit> <high upper-limit>;
    }
    address-protection;
    domain {
      delimiter characters;
      map name {
        aaa-logical-system name {
          aaa-routing-instance;
        }
        aaa-routing-instance aaa-routing-instance;
        access-profile;
        address-pool;
        dynamic-profile;
        padn destination-ip-address;
        strip-domain;
        target-logical-system;
        target-routing-instance;
      }
      parse-direction (left-to-right | right-to-left);
    }
    domain-name-server address;
    domain-name-server-inet address;
    domain-name-server-inet6 address;
    group-profile;
    gx-plus {
      global {
        include-ipv6;
        max-outstanding-requests;
      }
      partition {
        destination-host;
        destination-realm;
        diameter-instance;
      }
```

```
}
ldap-options {
    assemble {
        common-name name;
    }
    base-distinguished-name name;
    revert-interval seconds;
    search {
        admin-search {
            distinguished-name name;
            password password;
        }
        search-filter filter;
    }
}
ldap-server address {
    port number;
    retry number;
    routing-instance routing-instance;
    source-address address;
    timeout seconds;
}
ppp-options;
profile profile-name {
    accounting (Access Profile) {
        accounting-stop-on-access-deny;
        accounting-stop-on-failure;
        coa-immediate-update;
        duplication;
        immediate-update;
        order (radius | none);
        statistics (time | volume-time);
        wait-for-acct-on-ack;
    }
    accounting-order (radius | [accounting-order-data-list]);
    address-assignment {
        pool;
    }
    authentication-order [(ldap | none | password | radius | secureid)];
    authorization-order (jsrc | [authorization-order-data-list]);
    client client-name {
        chap-secret chap-secret;
        client-group;
        firewall-user {
            password password;
        }
        ike;
        no-rfc2486;
        pap-password password;
    }
    client-name-filter {
        count number;
        domain-name name;
        separator character;
    }
    domain-name-server;
```

```
domain-name-server-inet;
domain-name-server-inet6;
ldap-options {
  assemble {
    common-name name;
  }
  base-distinguished-name name;
  revert-interval seconds;
  search {
    admin-search {
      distinguished-name name;
      password password;
    }
    search-filter filter;
  }
}
ldap-server address {
  port number;
  retry number;
  routing-instance routing-instance;
  source-address address;
  timeout seconds;
}
provisioning-order {
  gx-plus;
  jsrc;
}
radius {
  accounting-server [server-addresses];
  attributes {
    exclude [exclude-options];
    ignore [ignore-options];
  }
  authentication-server [server-addresses];
  options {
    accounting-session-id-format (decimal | description);
    client-accounting-algorithm (direct | round-robin);
    client-authentication-algorithm (direct | round-robin);
    coa-dynamic-variable-validation;
    ethernet-port-type-virtual;
    interface-description-format {
      exclude-adapter;
      exclude-sub-interface;
    }
    juniper-dsl-attributes;
    nas-identifier nas-identifier;
    nas-port-extended-format {
      adapter-width adapter-width;
      ae-width ae-width;
      port-width port-width;
      slot-width slot-width;
      stacked-vlan-width stacked-vlan-width;
      vlan-width vlan-width;
    }
    nas-port-id-delimiter nas-port-id-delimiter;
    nas-port-id-format {
```

```
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            nas-identifier;
          }
          nas-port-type {
            ethernet;
          }
          revert-interval seconds;
          vlans-nas-port-stacked-format;
        }
      }
      radius-server address {
        max-outstanding-requests max-outstanding-requests;
        port port-number;
        retry retry;
        routing-instance instance-name;
        secret secret;
        source-address address;
        timeout seconds;
      }
      service {
        accounting-order {
          activation-protocol;
          radius;
        }
      }
      session-options {
        client-group [group-names];
        client-idle-timeout minutes;
        client-session-timeout minutes;
      }
    }
    radius-options {
      interim-rate number;
      interim-update-tolerance interim-update-tolerance;
      request-rate number;
      revert-interval interval;
    }
    radius-server server-address {
      accounting-port port-number;
      max-outstanding-requests number;
      port port-number;
      retry attempts;
      routing-instance instance-name;
      secret password;
      source-address address;
      timeout seconds;
    }
    securid-server server-name{
      configuration-file file-path;
    }
    terminate-code {
    }
  }
```

Unsupported Statements in the [edit access] Hierarchy Level

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

Statement	Hierarchy Level
NOTE: Variables, such as *filename*, are not shown in the statements or hierarchies listed below.	
aaa	[edit access terminate-code]
administrative-reset	[edit access terminate-code aaa shutdown]
authentication-denied	[edit access terminate-code aaa deny]
client-request	[edit access terminate-code aaa dhcp]
compliance	[edit access ppp-options]
deny	[edit access terminate-code aaa]
dhcp	[edit access terminate-code]
group-profile	[edit access]
ike	[edit access profile client]
initiate-dead-peer-detection	[edit access profile client ike]
lost-carrier	[edit access terminate-code dhcp]
nak	[edit access terminate-code dhcp]
nas-logout	[edit access terminate-code dhcp]
no-offers	[edit access terminate-code dhcp]
no-resources	[edit access terminate-code aaa deny]
ppp-options	[edit access]
preference	[edit access profile client ike reverse-route]
remote-reset	[edit access terminate-code aaa shutdown]
rfc	[edit access ppp-options compliance]

Table 15: Unsupported [edit access] Configuration Statements on EX Series Switches *(continued)*

Statement	Hierarchy Level
reverse-route	[edit access profile client ike]
server-request-timeout	[edit access terminate-code aaa deny]
shutdown	[edit access terminate-code aaa]
terminate-code	[edit access]

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to a Switch on page 27
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 103
- *Security Features for EX Series Switches Overview*

[edit protocols dot1x] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the **[edit protocols dot1x]** hierarchy level on EX Series switches.

- *Supported* statements are those that you can use to configure some aspect of a software feature on the switch.
- *Unsupported* statements are those that appear in the 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 dot1x] Hierarchy Level on page 135
- Unsupported Statements in the [edit protocols dot1x] Hierarchy Level on page 136

Supported Statements in the [edit protocols dot1x] Hierarchy Level

The following hierarchy shows the **[edit protocols dot1x]** configuration statements supported on EX Series switches:

```
protocols {
    dot1x {
        authenticator {
            authentication-profile-name access-profile-name;
            interface (all | [ interface-names ]) {
                disable;
                guest-vlan (vlan-id | vlan-name);
                mac-radius {
                    flap-on-disconnect;
```

```
            restrict;
          }
          maximum-requests number;
          no-reauthentication;
          quiet-period seconds;
          reauthentication {
            interval seconds;
          }
          retries number;
          server-fail (deny | permit | use-cache | vlan-id | vlan-name);
          server-reject-vlan (vlan-id | vlan-name) {
            eapol-block;
             block-interval block-interval;
          }
          server-timeout seconds;
          supplicant (single | single-secure | multiple);
          supplicant-timeout seconds;
          transmit-period seconds;
        }
        no-mac-table-binding {
          interface interface-names
          static mac-address
        }
        static  mac-address {
          interface interface-names;
          vlan-assignment (vlan-id |vlan-name);
        }
      }
    }
  }
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match
      regex>;
    flag flag ;
  }
```

Unsupported Statements in the [edit protocols dot1x] Hierarchy Level

All statements in the **[edit protocols dot1x]** hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

Related Documentation

- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on a Switch on page 31
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37
- Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to a Switch on page 66
- Example: Configuring Fallback Options on Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 95
- Example: Configuring Static MAC Bypass of Authentication on a Switch on page 62

- 802.1X for Switches Overview on page 3
- *[edit protocols] Configuration Statement Hierarchy on EX Series Switches*

accounting

Syntax

```
accounting {
  events [login change-log interactive-commands];
  destination {
    radius {
      server {
        server-address {
          accounting-port port-number;
          secret password;
          source-address address;
          retry number;
          timeout seconds;
        }
      }
    }
    tacplus {
      server {
        server-address {
          port port-number;
          secret password;
          single-connection;
          timeout seconds;
        }
      }
    }
  }
  enhanced-avs-max <number>;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
enhanced-avs-max statement introduced in Junos OS Release 14.1.

Description Configure audit of TACACS+ or RADIUS authentication events, configuration changes, and interactive commands. Auditing these factors helps you track network usage for auditing and billing purposes.

The remaining statements are explained separately.

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

Related Documentation

- *Configuring RADIUS System Accounting*
- *Configuring TACACS+ System Accounting*
- *enhanced-avs-max*

accounting (Access Profile)

Syntax

```
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-vrf {
    access-profile-name profile-name;
    vrf-name vrf-name;
  }
  immediate-update;
  order [accounting-method];
  send-acct-status-on-config-change
  statistics (time | volume-time);
  update-interval minutes;
  wait-for-acct-on-ack;
}
```

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.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile.

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 Authentication and Accounting Parameters for Subscriber Access*
- *Configuring Per-Subscriber Session Accounting*
- *Understanding RADIUS Accounting Duplicate Reporting*

accounting-order

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

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

Release Information Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description Enable RADIUS accounting for an L2TP profile.

Options **radius**—Use the RADIUS accounting method.

[*accounting-order-data-list*]—Set of data listing the accounting order to be used, enclosed by brackets. This can be any combination of accounting methods, up to and including and entire list of the entire accounting order.

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

Related Documentation

- *Configuring Access Profiles for L2TP or PPP Parameters*

accounting-port

Syntax accounting-port *port-number*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches with support for Enhanced Layer 2 software (ELS).
Statement introduced on Junos OS without ELS in the following releases:

- Junos OS Release 12.3 for EX Series switches: Release 12.3R10.
- Junos OS Release 14.1X53 for EX Series switches: Release 14.1X53-D25.

Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

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 ***port-number***—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

- *Configuring RADIUS System Accounting*
- *Configuring Router or Switch Interaction with RADIUS Servers*
- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Configuring RADIUS Authentication for L2TP*

address-assignment (Address-Assignment Pools)

Syntax

```
address-assignment {
  abated-utilization percentage;
  abated-utilization-v6 percentage;
  high-utilization percentage;
  high-utilization-v6 percentage;
  neighbor-discovery-router-advertisement ndra-pool-name;
  pool pool-name {
    family family {
      dhcp-attributes {
        protocol-specific attributes;
      }
      host hostname {
        hardware-address mac-address;
        ip-address ip-address;
      }
      network ip-prefix/<prefix-length>;
      prefix ipv6-prefix;
      range range-name {
        high upper-limit;
        low lower-limit;
        prefix-length prefix-length;
      }
    }
    link pool-name;
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description Configure address-assignment pools that can be used by different client applications.

NOTE: Support for subordinate statements is platform-specific. See individual statement topics for support information.

Options ***pool-name***—Name assigned to an address-assignment pool.

The remaining statements are explained separately.

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

Related Documentation

- *Address-Assignment Pools Overview*
- *Configuring Address-Assignment Pools*

- *Configuring an Address-Assignment Pool for L2TP LNS with Inline Services*
- *Configuring a DHCP Server on Switches (CLI Procedure)*

address-protection

Syntax address-protection;

Hierarchy Level [edit access],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* access]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description Prevent IPv4 addresses and IPv6 prefixes from being assigned to more than one subscriber session when you use AAA to supply IPv4 addresses.

For IPv4:

If enabled, the router checks the following attributes received from external servers:

- *Framed-IP-Address*
- *Framed-Pool*

The router then takes one of the following actions:

- If an address matches an address in an address pool, the address is taken from the pool, provided it is available.
- If the address is already in use, it is rejected as unavailable.

For IPv6:

If enabled, the router checks the following attributes received from external servers:

- *Framed-IPv6-Prefix*
- *Framed-IPv6-Pool*

The router then takes one of the following actions:

- If a prefix matches a prefix in an address pool, the prefix is taken from the pool, provided it is available.
- If the prefix is already in use, it is rejected as unavailable.
- If the prefix length requested from the external server does not exactly match the pool's prefix length, the authentication request is denied. If configured, the Acct-Stop message includes the cause for termination.

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

Related Documentation

- *Configuring Duplicate Prefix Protection for Router Advertisement*
- *Configuring Duplicate IPv4 Address Protection for AAA*

authorization-order

Syntax authorization-order (jsrc | [*authorization-order-data-list*]);

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

Release Information Statement introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure AAA to use JSRC in an SRC environment to request authorization from the SAE when verifying that a DHCP subscriber can access the router or switch. When you include this statement, AAA ignores any configured authentication order settings. This statement is ignored for non-DHCP subscribers.

Options jsrc—Use JSRC application to communicate with the SAE for subscriber authorization. JSRC is the only application that is currently available.

[*authorization-order-data-list*]—Set of data listing the authorization order to be used, enclosed by brackets. This can be any combination of authorization methods, up to and including a list of the entire authorization order.

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

Related Documentation

- *Configuring JSRC*
- *Authorizing Subscribers with JSRC*

authentication-order

Syntax authentication-order [(none | ldap | password | radius | secureid)];

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

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

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

none—No authentication for specified subscribers.

ldap— Lightweight Directory Access Protocol.

password—Locally configured password in access profile.

radius—RADIUS authentication.

securid—RSA SecurID authentication.

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

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to a Switch on page 27
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 103

authentication-whitelist

Syntax

```
authentication-whitelist {
  mac-address {
  interface interface-name;
  vlan-assignment ( vlan-id |vlan-name);
}
```

Hierarchy Level

[edit ethernet-switching-options],
[edit switch-options]

Release Information

Statement introduced in Junos OS Release 10.1 for EX Series switches.
Hierarchy level [edit switch-options] introduced in Junos OS Release 13.2X50-D10 for EX Series switches with support for ELS.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure MAC addresses for which RADIUS authentication is to be bypassed.

Required Privilege Level

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

Related Documentation

- *Example: Setting Up Captive Portal Authentication on an EX Series Switch*
- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 90
- *Configuring Captive Portal Authentication (CLI Procedure)*
- Configuring Captive Portal Authentication (CLI Procedure) on page 120

authenticator

Syntax

```
authenticator {
  authentication-profile-name access-profile-name;
  interface (all | [ interface-names ]) {
    disable;
    guest-vlan ( vlan-id | vlan-name);
    lldp-med-bypass;
    mac-radius <restrict>;
    maximum-requests number;
    no-reauthentication;
    quiet-period seconds;
    reauthentication interval;
    retries number;
    server-fail (deny | permit | use-cache | vlan-id | vlan-name);
    server-reject-vlan (vlan-id | vlan-name) {
      eapol-block;
       block-interval block-interval;
    }
    server-timeout seconds;
    supplicant (single | single-secure | multiple);
    supplicant-timeout seconds;
    transmit-period seconds;
  }
  no-mac-table-binding;
  radius-options {
    use-vlan-id;
    use-vlan-name;
  }
  static mac-address {
    vlan-assignment vlan-identifier;
  }
}
```

Hierarchy Level [edit protocols dot1x]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description Configure an authenticator for 802.1X authentication.

The statements are explained separately.

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

Default 802.1X authentication is disabled.

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

Related Documentation

- Configuring 802.1X Interface Settings (CLI Procedure) on page 102
- Specifying RADIUS Server Connections on Switches (CLI Procedure) on page 119
- Example: Configuring Static MAC Bypass of Authentication on a Switch on page 62

client-accounting-algorithm

Syntax client-accounting-algorithm (direct | round-robin);

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

Release Information Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS for EX Series switches Release 13.2X50-D10.

Description Configure the access method the router uses to access RADIUS accounting servers.

Default direct

Options **direct**—Use the direct method.

round-robin—Use the round-robin method.

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*
- *Configuring RADIUS Server Options for Subscriber Access*

client-authentication-algorithm

Syntax client-authentication-algorithm (direct | round-robin);

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

Release Information Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure the access method the router uses to access RADIUS authentication servers.

Default direct

Options **direct**—Use the direct method.

round-robin—Use the round-robin method.

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*
- *Configuring RADIUS Server Options for Subscriber Access*

coa-dynamic-variable-validation

Syntax coa-dynamic-variable-validation;

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

Release Information Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Specify that when a CoA operation includes a change to a client profile dynamic variable that cannot be applied (such as an update to a non-existent filter), the router does not apply any changes to client profile dynamic variables in the request, and responds with a NACK message.

Default If you do not configure this statement, the router does not apply any incorrect variable updates but does make any other changes to the client profile dynamic variables, and then responds with an ACK message.

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*
- *Configuring RADIUS Server Parameters for Subscriber Access*

destination (Accounting)

Syntax

```
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;
      }
    }
  }
}
```

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 The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Configuring RADIUS System Accounting*
- *Configuring TACACS+ System Accounting*

destination-host (Gx-Plus)

Syntax destination-host *hostname*;

Hierarchy Level [edit access gx-plus partition *partition-name*]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure the host on which the PCRF application resides.

Options ***hostname***—Host on which the PCRF is installed.

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

Related Documentation
- *Configuring Gx-Plus*
- *Configuring the Gx-Plus Partition*

destination-realm (Gx-Plus)

Syntax destination-realm *realm*;

Hierarchy Level [edit access gx-plus partition *partition-name*]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure the realm in which the PCRF host resides.

Options ***realm***—Realm in which the PCRF host resides.

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

Related Documentation
- *Configuring Gx-Plus*
- *Configuring the Gx-Plus Partition*

diameter-instance (Gx-Plus)

Syntax diameter-instance *instance-name*;

Hierarchy Level [edit access gx-plus partition *partition-name*]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Specify the Diameter instance associated with the Gx-Plus partition.

Options ***instance-name***—Name of the Diameter instance. Currently, only **master** is supported.

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

Related Documentation

- *Configuring Gx-Plus*
- *Configuring the Gx-Plus Partition*

domain (Domain Map)

Syntax

```
domain {
  delimiter [delimiter-character];
  map domain-map-name {
    aaa-logical-system logical-system-name {
      aaa-routing-instance routing-instance-name;
    }
    aaa-routing-instance routing-instance-name;
    access-profile profile-name;
    address-pool pool-name;
    dynamic-profile profile-name;
    padn destination-address {
      mask destination-mask;
      metric route-metric;
    }
    strip-domain;
    target-logical-system logical-system-name {
      target-routing-instance routing-instance-name;
    }
    target-routing-instance routing-instance-name;
    tunnel-profile profile-name;
  }
  parse-direction (left-to-right | right-to-left);
  parse-order (domain-first | realm-first);
  realm-delimiter [delimiter-character];
  realm-parse-direction (left-to-right | right-to-left);
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure a domain map, which is used to map access options and session parameters for subscriber sessions.

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 a Domain Map*

domain-name-server (Routing Instances and Access Profiles)

Syntax domain-name-server *dns-address*;

Hierarchy Level [edit access],
[edit access profile]

Release Information Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the **[edit access]** hierarchy level or for an access profile at the **[edit access profile *profile-name*]** hierarchy level. You can configure more than one address by including the statement multiple times.

NOTE: A DNS name server address configured with this statement is lower in preference than one configured with the domain-name-server-inet statement.

Options ***dns-address***—IPv4 address of the DNS name server.

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

Related Documentation

- *Configuring DNS Name Server Addresses for Subscriber Management*
- *DNS Name Server Address Overview*

domain-name-server-inet (Routing Instances and Access Profiles)

Syntax domain-name-server-inet *dns-address*;

Hierarchy Level [edit access],
[edit access profile]

Release Information Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the **[edit access]** hierarchy level or for an access profile at the **[edit access profile *profile-name*]** hierarchy level. You can configure more than one address by including the statement multiple times.

NOTE: A DNS name server address configured with this statement is higher in preference than one configured with the domain-name-server statement.

Options ***dns-address***—IPv4 address of the DNS name server.

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

Related Documentation

- *Configuring DNS Name Server Addresses for Subscriber Management*
- *DNS Name Server Address Overview*

domain-name-server-inet6 (Routing Instances and Access Profiles)

Syntax domain-name-server-inet6 *dns-address*;

Hierarchy Level [edit access],
[edit access profile]

Release Information Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure an IPv6 address for a DNS name server. You can configure an address globally for a routing instance at the **[edit access]** hierarchy level or for an access profile at the **[edit access profile *profile-name*]** hierarchy level. You can configure more than one address by including the statement multiple times.

Options ***dns-address***—IPv6 address of the DNS name server.

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

Related Documentation
- *Configuring DNS Name Server Addresses for Subscriber Management*
- *DNS Name Server Address Overview*

ethernet-port-type-virtual

Syntax ethernet-port-type-virtual;

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.

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**.

NOTE: This statement takes precedence over the nas-port-type statement if you include both statements in the same access profile.

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

Related Documentation
- *Configuring RADIUS Server Options for Subscriber Access*
- *Configuring RADIUS Server Parameters for Subscriber Access*

global (Gx-Plus)

Syntax

```
global {
  include-ipv6;
  max-outstanding-requests number;
}
```

Hierarchy Level [edit access gx-plus]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure global attributes for the Gx-Plus application.

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 Gx-Plus*

gx-plus (Gx-Plus)

Syntax

```
gx-plus {
  global {
    include-ipv6;
    max-outstanding-requests number;
  }
  partition partition-name {
    diameter-instance instance-name;
    destination-host hostname;
    destination-realm realm;
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure the Gx-Plus application to interact with a PCRF to authorize and provision 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 Gx-Plus*

ignore

Syntax

```
ignore {
  dynamic-iflset-name;
  framed-ip-netmask;
  input-filter;
  logical-system-routing-instance;
  output-filter;
}
```

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.

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

dynamic-iflset-name—Ignore Interface-Set/Dynamic-Iflset-Name (VSA 26-130).

framed-ip-netmask—Ignore Framed-IP-Netmask (RADIUS attribute 9).

input-filter—Ignore Ingress-Policy-Name (VSA 26-10).

logical-system-routing-instance—Ignore Virtual-Router (VSA 26-1).

output-filter—Ignore Egress-Policy-Name (VSA 26-11).

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*

include-ipv6 (Gx-Plus)

Syntax include-ipv6;

Hierarchy Level [edit access gx-plus global]

Release Information Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Include IPv6 subscribers in Gx-Plus provisioning requests.

Default By default, IPv6 subscribers are not included.

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

Related Documentation

- *Configuring Gx-Plus Global Attributes*
- *Configuring Gx-Plus*

interface (Static MAC Bypass)

Syntax interface [*interface-names*];

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).
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

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 ***interface-names***—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

- show dot1x static-mac-address on page 221
- Example: Configuring Static MAC Bypass of Authentication on a Switch on page 62
- *Example: Setting Up Captive Portal Authentication on an EX Series Switch*
- *Example: Setting Up Captive Portal Authentication on an EX Series Switch*
- *Configuring Captive Portal Authentication (CLI Procedure)*

interface (VoIP)

Syntax

```
interface (all | [interface-name] | access-ports) {
  vlan vlan-name );
  forwarding-class <assured-forwarding | best-effort | expedited-forwarding |
    network-control>;
}
```

Hierarchy Level

- For platforms with ELS:

  [edit switch-options voip]

- For platforms without ELS:

  [edit ethernet-switching-options voip],

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level **[edit switch-options]** introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Enable voice over IP (VoIP) for all interfaces or specific interfaces.

Options

all | ***interface-name*** | **access-ports**—Enable VoIP on all interfaces, on a specific interface, or on all access ports.

Required Privilege Level

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

Related Documentation

- *Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch*
- *Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication*
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 51

interface-description-format

Syntax

```
interface-description-format {
  exclude-adapter;
  exclude-sub-interface;
}
```

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.
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

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

juniper-dsl-attributes

Syntax juniper-dsl-attributes;

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

Release Information Statement introduced in Junos OS Release 11.4.

Description Configure AAA to add Juniper Networks DSL VSAs to the RADIUS authentication and accounting request messages for subscribers. If the router has not received and processed the corresponding ANCP attributes from the access node, then AAA provides only the following in these RADIUS messages:

- Downstream-Calculated-QoS-Rate (IANA 4874, 26-141)—Default configured advisory transmit speed.
- Upstream-Calculated-QoS-Rate (IANA 4874, 26-142)—Default configured advisory receive speed.

Default The Juniper Networks DSL VSAs are not added to the RADIUS authentication and accounting request messages. However, the DSL Forum VSA—if available—is added to RADIUS messages by default.

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

Related Documentation

- *Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages*
- *Configuring the ANCP Agent*

lldp

Syntax

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

Hierarchy Level [edit protocols]

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

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

The remaining statements are explained separately.

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

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

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

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

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

Default LLDP is enabled.

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

Related Documentation

- show lldp on page 226
- Configuring LLDP (CLI Procedure) on page 107
- *Configuring LLDP*
- *Understanding LLDP*
- Understanding 802.1X and LLDP and LLDP-MED on page 14

lldp-med (Ethernet Switching)

Syntax

```
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;
                    }
                }
            }
        }
    }
}
```

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-D30 for the QFX Series.

Description 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).

The statements are explained separately.

Default Disabled.

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 226
- *Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch*
- Configuring LLDP-MED (CLI Procedure) on page 111

max-outstanding-requests (Gx-Plus)

Syntax max-outstanding-requests *number*;

Hierarchy Level [edit access gx-plus global]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Limit the number of outstanding requests to the PCRF that Gx-Plus can retry when the requests are improperly answered. Too many requests risks overloading the PCRF and increases the chance of losing messages.

Options ***number***—Number of outstanding requests from Gx-Plus to the PCRF that can exist at any time.

Default: 40

Range: 2 through 40

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

Related Documentation
- *Configuring Gx-Plus Global Attributes*
- *Configuring Gx-Plus*

nas-identifier

Syntax nas-identifier *identifier-value*;

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.

Description Configure the value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests.

Options ***identifier-value***—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
- *Configuring RADIUS Server Options for Subscriber Access*
- *Configuring RADIUS Server Parameters for Subscriber Access*

nas-port-extended-format (Access Profile)

Syntax

```
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;
  }
}
```

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.
Option **ae-width** introduced in Junos OS Release 12.1.
Option **stacked** introduced in Junos OS Release 12.3.
Option **atm** introduced in Junos OS Release 12.3R3 and supported in later 12.3R*x* releases.
Option **atm** supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description In an access profile, 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. You can use the same access profile to configure the NAS-Port extended format for Ethernet subscribers and ATM subscribers.

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.

slot-width *width*—Number of bits in the slot field.

stacked—Include stacked VLAN IDs, in addition to VLAN IDs, in the NAS-Port extended format.

stacked-vlan-width *width*—Number of bits in the SVLAN ID field.

vlan-width *width*—Number of bits in the VLAN ID field.

atm—Configure the NAS-Port extended format for ATM subscribers; options include:

- **adapter-width *width***—Number of bits in the adapter field.
- **port-width *width***—Number of bits in the port field.

- **slot-width *width***—Number of bits in the slot field.
- **vci-width *width***—Number of bits in the ATM virtual circuit identifier (VCI) field.
- **vpi-width *width***—Number of bits in the ATM virtual path identifier (VPI) field.

NOTE: Each field can be 0 through 32 bits wide; however, the total of the widths of all fields must not exceed 32 bits, or the configuration fails.

The router may truncate the values of individual fields depending on the bit width you specify.

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

Related Documentation
- *Configuring RADIUS Server Options for Subscriber Access*
- *Configuring RADIUS Server Parameters for Subscriber Access*

nas-port-id-delimiter (Subscriber Management)

Syntax nas-port-id-delimiter *delimiter-character*;

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

Release Information Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Specify the character that the router uses as a separator between the concatenated values in the NAS-Port-ID string. The router uses the delimiter when you configure more than one value in the **nas-port-id-format** statement.

Default The hash (**#**) character.

Options ***delimiter-character***—Character used for the delimiter.

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

Related Documentation
- *Configuring RADIUS Server Options for Subscriber Access*
- *Configuring RADIUS Server Parameters for Subscriber Access*
- *Configuring a NAS-Port-ID with Additional Options*

nas-port-id-format (Subscriber Management)

Syntax

```
nas-port-id-format {
  agent-circuit-id;
  agent-remote-id;
  interface-description;
  nas-identifier;
}
```

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

Release Information Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Specify the information that the router includes in the NAS-Port-ID (RADIUS attribute 87) that it is passed to the RADIUS server during authentication and accounting. You can include any combination of the optional values.

Default The router includes the interface description.

Options

agent-circuit-id—Include the agent circuit ID from either DHCP option 82 or the DSL forum VSAs.

agent-remote-id—Include the agent remote ID from either DHCP option 82 or the DSL forum VSAs.

interface-description—Include the interface description.

nas-identifier—Include the NAS identifier value (RADIUS attribute 32).

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

Related Documentation

- *Configuring RADIUS Server Options for Subscriber Access*
- *Configuring RADIUS Server Parameters for Subscriber Access*
- *Configuring a NAS-Port-ID with Additional Options*

nas-port-type (Subscriber Management)

Syntax

```
nas-port-type {
  ethernet {
    port-type;
  }
}
```

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

Release Information Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Specify the port type used to authenticate subscribers. The router includes the port type in RADIUS attribute 61 (NAS-Port-Type attribute).

NOTE: This statement is ignored if the ethernet-port-type-virtual statement is included in the same access profile.

Default The router uses a port type of **ethernet**.

Options ***port-type***—One of the following port types:

- *value*—A value from 0-65535
- **adsl-cap**—Asymmetric DSL, carrierless amplitude phase (CAP) modulation
- **adsl-dmt**— Asymmetric DSL, discrete multitone (DMT)
- **async**—Asynchronous
- **cable**—Cable
- **ethernet**—Ethernet
- **fddi**—Fiber Distributed Data Interface
- **g3-fax**—G.3 Fax
- **hdlc-clear-channel**—HDLC Clear Channel
- **iapp**—Inter-Access Point Protocol (IAPP)
- **idsl**—ISDN DSL
- **isdn-sync**—ISDN Synchronous
- **isdn-v110**—ISDN Async V.110
- **isdn-v120**—ISDN Async V.120
- **piafs**—Personal Handyphone System (PHS) Internet Access Forum Standard
- **sdsl**—Symmetric DSL

- **sync**—Synchronous
- **token-ring**—Token Ring
- **virtual**—Virtual
- **wireless**—Other wireless
- **wireless-1x-ev**—Wireless 1xEV
- **wireless-cdma2000**—Wireless code division multiple access (CDMA) 2000
- **wireless-ieee80211**—Wireless 802.11
- **wireless-umts**—Wireless universal mobile telecommunications system (UMTS)
- **x25**—X.25
- **x75**—X.75
- **xdsl**—DSL of unknown type

Required Privilege Level

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

Related Documentation

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

options (Access Profile)

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;
    }
    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:
            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;
        nas-identifier;
    }
    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*

partition (Gx-Plus)

Syntax

```
partition partition-name {
  diameter-instance instance-name;
  destination-host hostname;
  destination-realm realm;
}
```

Hierarchy Level [edit access gx-plus]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure a Gx-Plus partition.

Options ***partition-name***—Name of the Gx-Plus partition.

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 Gx-Plus*
- *Configuring the Gx-Plus Partition*

port

Syntax port *port-number*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

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

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

Related Documentation

- *Configuring Router or Switch Interaction with RADIUS Servers*
- *Configuring Authentication and Accounting Parameters for Subscriber Access*

provisioning-order

Syntax provisioning-order (gx-plus | jsrc);

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

Release Information Statement introduced in Junos OS Release 9.6.
Support for Gx-Plus introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure AAA to use the specified application for subscriber service provisioning.

Options gx-plus—Specify Gx-Plus as the application used to communicate with a PCRF for subscriber service provisioning.

jsrc—Specify JSRC as the application used to communicate with the SAE for subscriber service provisioning. JSRC is used in an SRC environment to request services from the SAE for an authenticated subscriber. JSRC attempts to activate these services. If successful, JSRC returns an ACK message. If unsuccessful, the subscriber is denied access.

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

Related Documentation

- *Configuring JSRC*
- *Provisioning Subscribers with JSRC*
- *Configuring Gx-Plus*
- *Provisioning Subscribers with Gx-Plus*

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;
    }
    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;
        nas-identifier;
      }
      nas-port-type {
        ethernet {
          port-type;
        }
      }
      revert-interval interval;
      vlan-nas-port-stacked-format;
    }
    preauthentication-server ip-address;
}
```

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

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.

The remaining statements are explained separately.

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

Related Documentation

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

radius (System)

Syntax

```
radius {
  server {
    server-address {
      accounting-port port-number;
      secret password;
      source-address address;
      retry number;
      timeout seconds;
    }
  }
}
```

Hierarchy Level [edit system accounting destination]

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

Description Configure the RADIUS accounting server.

Options ***server-address***—Address of the RADIUS accounting server.

The remaining statements are explained separately.

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

Related Documentation
- *Configuring RADIUS System Accounting*

radius-options (Protocols 802.1X)

Syntax

```
radius-options {
  use-vlan-id;
  use-vlan-name;
}
```

Hierarchy Level [edit protocols dot1x authenticator]

Release Information Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

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

use-vlan-id—Include the VLAN ID in the packet sent to the RADIUS server to request authentication.

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.

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 102
- Specifying RADIUS Server Connections on Switches (CLI Procedure) on page 119
- authenticator on page 147

radius-options (Access)

Syntax

```
radius-options {
  revert-interval seconds;
}
```

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

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure RADIUS options.

Options The remaining statement is explained separately.

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

Related Documentation
- *Junos OS Security Configuration Guide*

radius-server (System)

Syntax

```
radius-server server-address {
  accounting-port port-number;
  port number;
  retry number;
  secret password;
  source-address source-address;
  timeout seconds;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure a RADIUS server for Point-to-Point Protocol (PPP).

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

Options ***server-address***—Address of the RADIUS authentication server.

The remaining statements are explained separately.

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

Related Documentation
- *Configuring RADIUS Authentication*

retry

Syntax retry *attempts*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

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

Description Specify the number of times that the router or switch is allowed to attempt to contact a RADIUS authentication or accounting server.

Options ***attempts***—Number of times that the router is allowed to attempt to contact a RADIUS server.

Range: 1 through 30

Default: 3

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

Related Documentation

- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Configuring Router or Switch Interaction with RADIUS Servers*
- *Example: Configuring CHAP Authentication with RADIUS*
- *Configuring RADIUS Authentication for L2TP*
- timeout on page 189

revert-interval

Syntax revert-interval *interval*;

Hierarchy Level [edit access profile *profile-name* 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 ***interval***—Amount of time to wait.

Range: 0 through 604800 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

- *Configuring RADIUS Server Options for Subscriber Access*
- *Configuring Authentication and Accounting Parameters for Subscriber Access*

routing-instance

Syntax routing-instance *routing-instance-name*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

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

Description Configure the routing instance used to send RADIUS packets to the RADIUS server.

Options ***routing-instance-name***—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

- *Configuring the PPP Authentication Protocol*
- *Configuring Authentication and Accounting Parameters for Subscriber Access*

secret

Syntax secret *password*;

Hierarchy Level [edit access profile *profile-name* radius-server *server-address*],
[edit access radius-disconnect *client-address*],
[edit access radius-server *server-address*]

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

Description 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

- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Configuring Router or Switch Interaction with RADIUS Servers*
- *Example: Configuring CHAP Authentication with RADIUS*
- *Configuring RADIUS Authentication for L2TP*
- *Configuring the RADIUS Disconnect Server for L2TP*
- *Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)*

send-acct-status-on-config-change (Access Profile)

Syntax send-acct-status-on-config-change;

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

Release Information Statement introduced in Junos OS Release 13.1.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure the router's authd process to send an Acct-On message when the first RADIUS server is added to an access profile, and to send an Acct-Off message when the last RADIUS server is removed from an access profile.

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*
- *Configuring Per-Subscriber Session Accounting*

server (RADIUS Accounting)

Syntax

```
server {
  server-address {
    accounting-port port-number;
    retry number
    secret password;
    source-address address;
    timeout seconds;
  }
}
```

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.

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

- *Configuring RADIUS System Accounting*

server-fail-voip

Syntax server-fail (deny | permit | use-cache | vlan-name);

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

Release Information Statement introduced in Junos OS Releases 14.1X53-D40 and 15.1R4 for EX Series switches.

Description Configure authentication fallback options to specify how VoIP clients sending voice traffic are supported if the RADIUS authentication server becomes unavailable. Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by a supplicant's initial attempt at authentication through the RADIUS server.

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

The **server-fail-voip** statement is specific to the VoIP-tagged traffic sent by clients. VoIP clients still require that the **server-fail** statement be configured for the un-tagged traffic that they generate. Therefore, when you configure the **server-fail-voip** statement you must also configure the **server-fail** statement.

NOTE: **An option other than server-fail deny must be configured for server-fail-voip to successfully commit.**

Default If the **server-fail-voip** statement is not configured, in the event that the RADIUS authentication server becomes unavailable, a VoIP client that begins authentication by sending voice traffic is not authenticated, and the voice traffic is dropped.

Options **deny**—Force fail the supplicant authentication. No traffic will flow through the interface.

permit—Force succeed the supplicant authentication. Traffic will flow through the interface as if it were successfully authenticated by the RADIUS server.

use-cache—Force succeed the supplicant authentication only if it was previously authenticated successfully. This action ensures that already authenticated supplicants are not affected. This option can be used only for reauthentication.

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. The VLAN must already be configured 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
- show dot1x on page 214
- Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to a Switch on page 66
- Example: Connecting a RADIUS Server for 802.1X to a Switch on page 27
- Configuring Server Fail Fallback (CLI Procedure) on page 114
- Understanding Server Fail Fallback and Authentication on Switches on page 20

service (Service Accounting)

Syntax
```
service {
  accounting-order (activation-protocol | radius);
}
```

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

Release Information
Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Define the subscriber service accounting configuration.

The remaining statement is 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 Service Accounting with JSRC*
- *Service Accounting with JSRC*

source-address

Syntax source-address *source-address*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

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

Description Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address.

Options ***source-address***—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

- *Configuring Router or Switch Interaction with RADIUS Servers*
- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Example: Configuring CHAP Authentication with RADIUS*
- *Configuring RADIUS Authentication for L2TP*

timeout (RADIUS)

Syntax timeout *seconds*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

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

Description Configure the amount of time that the local router or switch waits to receive a response from a RADIUS 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

- *Configuring Router or Switch Interaction with RADIUS Servers*
- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Example: Configuring CHAP Authentication with RADIUS*
- *Configuring RADIUS Authentication for L2TP*

vlan (VoIP)

Syntax vlan (*vlan-id* | *vlan-name* | untagged);

Hierarchy Level [edit ethernet-switching-options voip interface (VoIP) (all | [*interface-name* | access-ports])

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description For EX Series switches, specify the VLAN name or VLAN tag identifier associated with the VLAN to be sent from the authenticating server to the IP phone.

Options *vlan-name*—Name of a VLAN.

vlan-id—The VLAN tag identifier.

Range: 0 through 4095. Tags 0 and 4095 are reserved by Junos OS, and you should not configure them.

untagged—Allow untagged VLAN traffic.

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

Related Documentation

- *Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch*
- *Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication*
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 51

vlan-assignment

Syntax vlan-assignment (*vlan-id* | *vlan-name*);

Hierarchy Level [edit protocols dot1x authenticator authentication-profile-name static (Protocols 802.1X) *mac-address*],
[edit ethernet-switching-options authentication-whitelist],
[edit switch-options authentication-whitelist]

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.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description Configure the VLAN that is associated with the list of MAC addresses that are excluded from RADIUS authentication.

Options ***vlan-id*** | ***vlan-name***—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 routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- show dot1x static-mac-address on page 221
- Example: Configuring Static MAC Bypass of Authentication on a Switch on page 62
- *Example: Setting Up Captive Portal Authentication on an EX Series Switch*
- Understanding Authentication on Switches on page 6
- *Example: Setting Up Captive Portal Authentication on an EX Series Switch*
- *Configuring Captive Portal Authentication (CLI Procedure)*

vlan-nas-port-stacked-format

Syntax vlan-nas-port-stacked-format;

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.

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
- *Configuring RADIUS Server Options for Subscriber Access*
- *Configuring Authentication and Accounting Parameters for Subscriber Access*

voip

Syntax
```
voip {
  interface (all | [interface-name | access-ports]) {
    vlan vlan-name );
    forwarding-class <assured-forwarding | best-effort | expedited-forwarding |
      network-control>;
  }
}
```

Hierarchy Level [edit ethernet-switching-options],
[edit switch-options]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description Configure voice over IP (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
- *Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch*
- *Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication*
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support on page 51

wait-for-acct-on-ack (Access Profile)

Syntax wait-for-acct-on-ack;

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

Release Information Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure the router's **authd** process to wait for an Acct-On-Ack response message from RADIUS before sending new authentication and accounting updates to the RADIUS server. This configuration ensures that when a new subscriber session starts, the authentication and accounting information for the new session does not get deleted when RADIUS clears previously existing session state information.

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*
- *Configuring Per-Subscriber Session Accounting*

PART 3

Administration

CHAPTER 5

Routine Monitoring

Monitoring 802.1X Authentication

Purpose

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

J-Web Application package Release 14.1X53-A2 does not support 802.1X authentication on EX4600 switches.

Use the monitoring feature to display details of authenticated users and users that 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 number of connected users.
- A list of users that failed authentication.

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

Related Documentation

- *Configuring 802.1X Authentication (J-Web Procedure)*
- Configuring 802.1X Interface Settings (CLI Procedure) on page 102

- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37

Verifying 802.1X Authentication

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

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

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

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

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

- **Guest VLAN**—A nonresponsive host is granted Guest-VLAN access.
- **MAC Radius**—A nonresponsive host is authenticated based on its MAC address. The MAC address is configured as permitted on the RADIUS server, the RADIUS server lets the switch know that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected.

- **Server-fail deny**—If the RADIUS servers time out, all supplicants are denied access to the LAN, preventing traffic from flowing from the supplicant through the interface. This is the default.
- **Server-fail permit**—When the RADIUS server is unavailable, a supplicant is still permitted access to the LAN as if the supplicant had been successfully authenticated by the RADIUS server.
- **Server-fail use-cache**—If the RADIUS servers time out during reauthentication, previously authenticated supplicants are granted access, but new supplicants are denied LAN access.
- **Server-fail VLAN**—A supplicant is configured to be moved to a specified VLAN if the RADIUS server is unavailable to reauthenticate the supplicant. (The VLAN must already exist on the switch.)

Related Documentation

- Configuring 802.1X Interface Settings (CLI Procedure) on page 102
- *Configuring 802.1X Authentication (J-Web Procedure)*
- Configuring MAC RADIUS Authentication (CLI Procedure) on page 117
- Configuring Server Fail Fallback (CLI Procedure) on page 114

CHAPTER 6

Operational Commands

clear captive-portal

Syntax **clear captive-portal (firewall** [*interface-names*] **| interface (802.1X) (all |** [*interface-names*]) **| mac-address** [*mac-addresses*])

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

Description Reset the authentication state of a captive portal interface or captive portal firewall statistics on one or more interfaces.

Options

firewall [*interface-names*]—Resets captive portal statistics on all interfaces or on the specified interface.

interface (all | *interface-names*)—Resets the authentication state of users connected to all interfaces or the specified interfaces.

mac-address *mac-addresses*—Resets the authentication state for the specified MAC addresses.

Required Privilege Level view

Related Documentation

- show captive-portal authentication-failed-users on page 208
- show captive-portal interface on page 211
- show captive-portal firewall on page 209
- *Example: Setting Up Captive Portal Authentication on an EX Series Switch*
- *Configuring Captive Portal Authentication (CLI Procedure)*

List of Sample Output

clear captive-portal interface on page 203
clear captive-portal interface on page 203
clear captive-portal mac-address on page 203
clear captive-portal firewall on page 203

Output Fields Table 16 on page 202 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 16: clear captive-portal interface Output Fields

Field Name	Field Description
Interface	Interface on which captive portal has been configured.

Table 16: clear captive-portal interface Output Fields *(continued)*

Field Name	Field Description
State	The state of the port: • **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.
Support for **firewall** added in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.
Support for **eapol-block** introduced in Junos OS Release 14.1X53-D40 for EX Series switches.

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

eapol-block—Clear EAPOL block on the interface and allow the switch to receive EAPOL messages from a supplicant connected to that interface.

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 214
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37
- Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 105

List of Sample Output

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 dot1x eapol-block

```
user@switch> clear dot1x eapol-block
```

clear lldp neighbors

Syntax clear lldp neighbors
<interface *interface*>

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 *interface*—(Optional) Clear the remote neighbor information from one or more selected interfaces.

Required Privilege Level view

Related Documentation
- show lldp on page 226
- Configuring LLDP (CLI Procedure) on page 107
- Understanding 802.1X and LLDP and LLDP-MED on page 14

List of Sample Output

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 *interface*>

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

Description Clear LLDP statistics on one or more interfaces.

Options **none**—Clears LLDP statistics on all interfaces.

interface *interface-names*—(Optional) Clear LLDP statistics on one or more interfaces.

Required Privilege Level view

Related Documentation
- Configuring LLDP (CLI Procedure) on page 107
- Understanding 802.1X and LLDP and LLDP-MED on page 14

List of Sample Output
clear lldp statistics on page 207
clear lldp statistics interface ge-0/1/1.0 on page 207

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.

Description Display the users that have failed captive portal authentication.

Required Privilege Level view

Related Documentation

- show captive-portal interface on page 211
- show captive-portal firewall on page 209
- clear captive-portal on page 202
- *Example: Setting Up Captive Portal Authentication on an EX Series Switch*
- *Configuring Captive Portal Authentication (CLI Procedure)*

List of Sample Output show captive-portal authentication-failed-users on page 208

Output Fields Table 17 on page 208 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 17: 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@switch> 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
show captive-portal firewall
<brief | detail>
<*interface-name*>
<*interface-name* detail>

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

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
- show captive-portal authentication-failed-users on page 208
- show captive-portal interface on page 211
- clear captive-portal on page 202
- *Example: Setting Up Captive Portal Authentication on an EX Series Switch*
- *Configuring Captive Portal Authentication (CLI Procedure)*

List of Sample Output
show captive-portal firewall brief on page 209
show captive-portal firewall (Specific Interface) on page 210
show captive-portal firewall on page 210

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.

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
none—Display all captive portal interfaces.

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.

***interface-name* detail**—(Optional) Display the configured values of captive portal attributes on the specified captive portal interface.

Required Privilege Level
view

Related Documentation
- show captive-portal authentication-failed-users on page 208
- show captive-portal firewall on page 209
- *captive-portal*
- clear captive-portal on page 202
- *Example: Setting Up Captive Portal Authentication on an EX Series Switch*
- *Configuring Captive Portal Authentication (CLI Procedure)*

List of Sample Output
show captive-portal interface (Only Captive Portal Enabled) on page 213
show captive-portal interface (802.1X Authentication and Captive Portal Enabled) on page 213
show captive-portal interface detail (Only Captive Portal Enabled) on page 213
show captive-portal interface detail (802.1X Authentication and Captive Portal Enabled) on page 213

Output Fields
Table 18 on page 211 lists the output fields for the **show captive-portal interface** command. Output fields are listed in the approximate order in which they appear.

Table 18: 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 18: show captive-portal interface Output Fields *(continued)*

Field Name	Field Description	Level of Output
State	The state of the interface: • **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	Indicates when 802.1X authentication and captive portal are both enabled on an interface: • 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	Number of users connecting through the captive portal interface. Information for each user includes: • **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** ***interface-name***>

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

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 ***interface-name***—Display information for the specified port with a list of connected supplicants.

Required Privilege Level

view

Related Documentation

- clear dot1x on page 204
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on a Switch on page 37
- Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to a Switch on page 66
- Example: Configuring Fallback Options on Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 95
- Filtering 802.1X Supplicants By Using RADIUS Server Attributes on page 105
- Verifying 802.1X Authentication on page 198

List of Sample Output

show dot1x interface brief on page 217
show dot1x interface detail on page 217

Output Fields

Table 19 on page 214 lists the output fields for the **show dot1x** command. Output fields are listed in the approximate order in which they appear.

Table 19: show dot1x Output Fields

Field Name	Field Description	Level of Output
Interface	Name of a port.	All levels
MAC address	The MAC address of the connected supplicant on the port.	All levels

Table 19: show dot1x Output Fields *(continued)*

Field Name	Field Description	Level of Output
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	The state of the port: • **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 user name of the connected supplicant	**brief**
Administrative state	The administrative state of the port: • **auto**—Traffic is allowed through the port based on the authentication result. (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	The mode for the supplicant: • **single**—Authenticates only the first supplicant. All other supplicants who connect later to the port are allowed full access without any further authentication. They effectively “piggyback” on the first supplicant’s authentication. • **single-secure**—Allows only one supplicant to connect to the port. No other supplicant is allowed to connect until the first supplicant logs out. • **multiple**—Allows multiple supplicants to connect to the port. Each supplicant is authenticated individually.	**detail**
Quiet period	The number of seconds the port remains in the wait state following a failed authentication exchange with the supplicant before reattempting the authentication. The default value is 60 seconds. The range is 0 through 65,535 seconds.	**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 19: show dot1x Output Fields *(continued)*

Field Name	Field Description	Level of Output
MAC radius	MAC RADIUS authentication: • **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 using the MAC address. • **disabled**—The default. The switch will not attempt to authenticate the MAC address of the connecting host.	**detail**
MAC radius restrict	The authentication method is restricted to MAC RADIUS only. 802.1X authentication is not enabled.	**detail**
Reauthentication	The reauthentication state: • **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 retransmission times of an EAPOL request packet to the supplicant before the authentication session times out. The default value is 2. The range is 1 through 10.	**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: • **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 user name and MAC address of the connected supplicant.	**detail**

Table 19: show dot1x Output Fields *(continued)*

Field Name	Field Description	Level of Output
Authentication method	The 802.1X authentication method used for a supplicant: • **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. Indicates whether EAPOL block is in effect, and the amount of time remaining for EAPOL block (in seconds). • **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**

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 Strict: Disabled
Reauthentication: Enabled
Configured Reauthentication interval: 40 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 1
Guest VLAN member: <not configured>
Number of connected supplicants: 1
  Supplicant: abc, 00:30:48:8C:66:BD
    Operational state: Authenticated
    Authentication method: Radius
    Authenticated VLAN: v200
    Reauthentication due in 17 seconds
```

show dot1x authentication-failed-users

Syntax show dot1x authentication-failed-users

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description Display supplicants (users) that have failed 802.1X authentication.

Required Privilege Level view

Related Documentation
- clear dot1x on page 204
- Example: Configuring Static MAC Bypass of Authentication on a Switch on page 62
- Configuring 802.1X Interface Settings (CLI Procedure) on page 102

List of Sample Output show dot1x authentication-failed-users on page 219

Output Fields Table 20 on page 219 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 20: 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 show dot1x firewall <interface *interface-name*>

Release Information Command introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description Displays information about the firewall filters for each user or nonresponsive host that is authenticated on each 802.1X-enabled interface that is configured for multiple supplicants. For example, if the firewall filter is configured with a term for counters, the command shows the count for each user.

Options **none**—Display information for all interfaces.

interface *interface-names*—(Optional) Display information for the specified interface.

Required Privilege Level view

Related Documentation
- clear dot1x on page 204
- *Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication*

List of Sample Output show dot1x firewall on page 220
show dot1x firewall on page 220

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 show dot1x static-mac-address <(interface [*interface-name*])>

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description Displays 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 *interface-name*—(Optional) Display static MAC addresses for a specific interface.

Required Privilege Level view

Related Documentation

- clear dot1x on page 204
- Example: Configuring Static MAC Bypass of Authentication on a Switch on page 62
- *Adding a Static MAC Address Entry to the Ethernet Switching Table (CLI Procedure)*
- Configuring 802.1X Interface Settings (CLI Procedure) on page 102
- Understanding Authentication on Switches on page 6

List of Sample Output show dot1x static-mac-address on page 221
show dot1x static-mac-address interface (Specific Interface) on page 222

Output Fields Table 21 on page 221 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 21: 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 interface

Syntax

show ethernet-switching interface
<brief | detail | extensive>
<interface-name>

Release Information

Command introduced in Junos OS Release 12.3R2.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Command introduced in Junos OS Release 13.2x51 for QFX Series switches.

Description

Display Layer 2 learning information for all the interfaces.

Options

none—Display Ethernet-switching information for all interfaces.

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

interface-name—(Optional) Display Ethernet-switching information for the specified interface.

Required Privilege Level

view

Related Documentation

- *autostate-exclude*

List of Sample Output

show ethernet switching interface (Specific Interface) on page 224
show ethernet-switching interface detail on page 225
show ethernet-switching interface xe-0/0/2.0 (autostate-exclude enabled on QFX5100 switch) on page 225

Output Fields

Table 22 on page 223 describes the output fields for the **show ethernet-switching interface** command. Output fields are listed in the approximate order in which they appear.

Table 22: show ethernet-switching interface Output Fields

Field Name	Field Description
Logical interface	Name of the logical interface.
VLAN members	VLANs associated with this interface.
Tag	VLAN ID.
MAC limit	Number of MAC addresses that can be associated with the interface.
STP state	Spanning Tree protocol (STP) state.

Table 22: show ethernet-switching interface Output Fields *(continued)*

Field Name	Field Description
Logical interface flags	Status of Layer 2 learning properties for each interface: • **DL**—MAC learning is disabled. • **LH**—MAC interface limit has been reached. • **AD**—Packets are dropped after the MAC interface limit is reached. • **DN**—The MAC interface is down. • **MMAS**—The MAC interface is disabled after a MAC address move. • **SCTL**—The MAC interface is disabled after a configured storm-control level is exceeded. • **AS**—This interface is not included in the state calculation for VLAN members.
Tagging	Tagging state of the VLAN.

Sample Output

show ethernet switching interface (Specific Interface)

```
user@host> show ethernet-switching inerface ae10.0
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down)

Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ae10.0                        8192                                  tagged
             VLAN70..   701   1024     Forwarding

             VLAN70..   702   1024     Forwarding

             VLAN70..   703   1024     Forwarding

             VLAN70..   704   1024     Forwarding

             VLAN70..   705   1024     Forwarding

             VLAN70..   706   1024     Forwarding

             VLAN70..   707   1024     Forwarding

             VLAN70..   708   1024     Forwarding

             VLAN70..   709   1024     Forwarding

             VLAN71..   710   1024     Forwarding

             VLAN71..   711   1024     Forwarding

             VLAN71..   712   1024     Forwarding

             VLAN71..   713   1024     Forwarding

             VLAN71..   714   1024     Forwarding
```

```
                    VLAN71..   715
[...output truncated...]
```

show ethernet-switching interface detail

```
user@host> show ethernet-switching interface detail
Information for interface family:
Name: ge-1/0/3.0
  Type: IFF                              Handle: 0x8bba280
  Index: 331                             Generation: 159
                                         Flags: UP,
  IFD index: 141                         Routing/Vlan index: 4
  IFL index: 331                         Address family: 50
  Sequence number: 0                     MAC sequence number: 0
  MAC limit: 65535                       MACs learned: 0
  Static MACs learned: 0                 Non configured static MACs learned: 0
Name: ge-1/0/3.0
  Type: IFBD (static)                    Handle: 0x8bb6e00
  Index:                                 Generation: 129
  Trunk id: 0                            Flags: UP,
  IFD index:                             Routing/Vlan index: 2
  IFL index:                             Address family:
  Sequence number: 1                     MAC sequence number: 1
  MAC limit: 65535                       MACs learned: 0
  Static MACs learned: 0                 Non configured static MACs learned: 0
  VSTP index: 11                         Rewrite op:
Name: ge-1/0/3.0
  Type: IFBD (static)                    Handle: 0x8bb6f00
  Index:                                 Generation: 130
  Trunk id: 0                            Flags: UP,
  IFD index:                             Routing/Vlan index: 3
  IFL index:                             Address family:
  Sequence number: 1                     MAC sequence number: 1
  MAC limit: 65535                       MACs learned: 0
  Static MACs learned: 0                 Non configured static MACs learned: 0
  VSTP index: 11                         Rewrite op:
```

show ethernet-switching interface xe-0/0/2.0 (autostate-exclude enabled on QFX5100 switch)

```
user@switch> show ethernet-switching interface xe-0/0/2.0

Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down,
                         MMAS - Mac-move action shutdown, AS - Autostate-exclude enabled
                         SCTL - shutdown by Storm-control)

Logical          Vlan          TAG     MAC         STP         Logical           Tagging
interface        members               limit       state       interface flags
xe-0/0/2.0                             294912                   AS                tagged
                 v100          100     294912      Forwarding                    tagged
```

show lldp

Syntax
show lldp
<detail>

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

Description
Display information about Link Layer Discovery Protocol (LLDP) and Link Level Discovery Protocol–Media Endpoint Discovery (LLDP-MED) configuration and capabilities on the switch. LLDP and LLDP-MED are used to learn about and to distribute device information on network links.

NOTE: **LLDP-MED is not available on the QFX Series.**

Options
none—Display LLDP information for all interfaces.

detail—(Optional) Display detailed LLDP information for all interfaces.

Required Privilege Level
view

Related Documentation
- Configuring LLDP (CLI Procedure) on page 107
- Configuring LLDP-MED (CLI Procedure) on page 111
- Understanding 802.1X and LLDP and LLDP-MED on page 14
- *Configuring LLDP*
- *Understanding LLDP*

List of Sample Output
show lldp (EX3200 switches) on page 229
show lldp (EX4300 switches) on page 229
show lldp detail (EX4300 switches) on page 230

Output Fields
Table 23 on page 226 lists the output fields for the **show lldp** command. Output fields are listed in the approximate order in which they appear.

Table 23: 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 23: show lldp Output Fields *(continued)*

Field Name	Field Description	Level of Output
Advertisement interval	Frequency, in seconds, at which LLDP advertisements are sent. This value is set by the ***advertisement-interval*** configuration statement.	All levels
Transmit delay	Seconds of delay before advertisements are sent to neighbors following a change to a TLV (type, length, or value) element in the LLDP protocol or to the state of the local system, such as a change in hostname or management address. You can set this value to reduce the delay in notifying neighbors of a change in the local system. This value is set by the *transmit-delay* configuration statement.	All levels
Hold timer	On EX4300 switches, the hold timer shows the length of time LLDP information is held before it is discarded. The hold timer value is equal to the advertisement interval multiplied by the hold multiplier. On all other switches, the hold timer shows the value of the hold multiplier. The hold multipler value is set by the **hold-multiplier** configuration statement.	All levels
Notification interval	How often LLDP trap notifications are generated as a result of LLDP database changes. If the interval value is 0, LLDP trap notifications on database changes are disabled. This value is set by the ***lldp-configuration-notification-interval*** configuration statement.	All levels
Config Trap Interval	How often LLDP trap notifications are generated as a result of changes in topology—for example, when an endpoint connects or disconnects. If the interval value is 0, LLDP trap notifications on topology changes are disabled. This value is set by the ***ptopo-configuration-trap-interval*** configuration statement.	All levels
Connection Hold timer	Amount of time the system maintains dynamic topology entries. This value is set by the ***ptopo-configuration-maximum-hold-time*** configuration statement.	All levels
LLDP-MED	LLDP-MED operating state. The state can be **Enabled** or **Disabled**.	All levels
MED fast start count	Number of advertisements sent from a switch to a device, such as a VoIP telephone, when the device is first detected by the switch. These increased advertisements are temporary. After a device and a switch exchange information and can communicate, advertisements are reduced to one per second. This value is set by using the ***fast-start*** configuration statement. NOTE: **fast-start**is not available on the QFX Series.	All levels
Interface	Name of the interface for which LLDP configuration information is being reported.	All levels
Parent Interface	Name of the aggregated Ethernet interface, if any, to which the interface belongs.	All levels

Table 23: show lldp Output Fields *(continued)*

Field Name	Field Description	Level of Output
LLDP	LLDP operating state. The state can be **Enabled** or **Disabled**.	All levels
Power Negotiation	LLDP power negotiation operating state. The state can be **Enabled** or **Disabled**.	All levels
Neighbor count	Total number of new LLDP neighbors detected since the last switch reboot.	**detail**
Interface	Name of the interface that is advertising VLAN information.	All levels
Vlan-id	VLAN tag associated with the interface sending LLDP frames. If the interface is not a member of a VLAN, the VLAN ID is advertised as 0.	**detail**
Vlan-name	VLAN name associated with the VLAN ID.	**detail**
LLDP basic TLVs supported	Basic TLVs supported on the switch: • **Chassis identifier**—TLV that advertises the MAC address associated with the local system. • **Port identifier**—TLV that advertises the port identification for the specified port in the local system. • **Port description**—Interface name for the port. • **System name**—TLV that advertises the user-configured name of the local system. • **System description**—TLV that advertises the system description containing information about the software and current image running on the system. This information is taken from the software and is not configurable. • **System capabilities**—TLV that advertises the primary functions performed by the system—for example, bridge or router. • **Management address**—TLV that advertises the IP management address of the local system.	**detail**
Supported LLDP 802 TLVs	802.3 TLVs supported on the switch: • **MAC/PHY configuration status**—TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information is based on the physical interface structure and is not configurable. • **Power via MDI**—TLV that advertises MDI power support, PSE power pair, and power class information. • **Link aggregation**—TLV that advertises if the interface is aggregated and its aggregated interface ID. • **Maximum frame size**—TLV that advertises the maximum transmission unit (MTU) of the interface sending LLDP frames. • **Port VLAN tag**—TLV that advertises the VLAN tag configured on the interface. • **Port VLAN name**—TLV that advertises the VLAN name configured on the interface.	**detail**

Table 23: show lldp Output Fields *(continued)*

Field Name	Field Description	Level of Output

Supported LLDP MED TLVs	LLDP-MED TLVs supported on the switch:
	• **LLDP MED capabilities**—TLV that advertises the primary function of the port. The capabilities values range from 0 through 15:
	  ◦ **0**—Capabilities
	  ◦ **1**—Network Policy
	  ◦ **2**—Location Identification
	  ◦ **3**—Extended Power via MDI-PSE
	  ◦ **4**—Inventory
	  ◦ **5–15**—Reserved
	• **Network policy**—TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types—such as voice or streaming video—802.1Q VLAN tagging, and 802.1p priority bits and DiffServ code points.
	• **Endpoint location**—TLV that advertises the physical location of the endpoint.
	• **Extended power Via MDI**—TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.
		detail

Sample Output

show lldp (EX3200 switches)

```
user@switch> show lldp
LLDP                      : Enabled
Advertisement interval    : 30 seconds
Transmit delay            : 2 seconds
Hold timer                : 4 seconds
Notification interval     : 0 Second(s)
Config Trap Interval      : 0 seconds
Connection Hold timer     : 300 seconds

LLDP MED                  : Disabled
MED fast start count      : 3 Packets


Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
all            -                   Enabled     Enabled      Enabled
```

show lldp (EX4300 switches)

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

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

```
Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
all            -                   Enabled     Enabled      Enabled
```

show lldp detail (EX4300 switches)

```
user@switch> show lldp detail
LLDP                     : Enabled
Advertisement interval   : 30 seconds
Transmit delay           : 2 seconds
Hold timer               : 120 seconds
Notification interval    : 0 Second(s)
Config Trap Interval     : 0 seconds
Connection Hold timer    : 300 seconds

LLDP MED                 : Disabled
MED fast start count     : 3 Packets


Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
  Neighbor count
all            -                   Enabled     Enabled      Enabled
  8

Interface      Parent Interface    Vlan-id     Vlan-name
xe-3/0/0.0     ae31.0              100         v100
xe-3/0/0.0     ae31.0              101         v101
xe-3/0/0.0     ae31.0              4000        v4000
xe-3/0/1.0     ae31.0              100         v100
xe-3/0/1.0     ae31.0              101         v101
xe-3/0/1.0     ae31.0              4000        v4000
xe-3/0/2.0     ae31.0              100         v100
xe-3/0/2.0     ae31.0              101         v101
xe-3/0/2.0     ae31.0              4000        v4000

LLDP basic TLVs supported:
Chassis identifier, Port identifier, Port description, System name, System
description, System capabilities, Management address.

Supported LLDP 802 TLVs:
MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum frame
size, Port VLAN tag, Port VLAN name.

Supported LLDP MED TLVs:
LLDP MED capabilities, Network policy, Endpoint location, Extended power
Via MDI.
```

show lldp local-information

Syntax show lldp local-information

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

Description Display the information that the switch provides in Link Layer Discovery Protocol (LLDP) advertisements to its neighbors.

Required Privilege Level view

Related Documentation

- Configuring LLDP (CLI Procedure) on page 107
- Understanding 802.1X and LLDP and LLDP-MED on page 14
- *management-address*
- *Configuring LLDP*
- *Understanding LLDP*

List of Sample Output show lldp local-information (EX Series Switch) on page 232

Output Fields Table 24 on page 231 lists the output fields for the **show lldp local-information** command. Output fields are listed in the approximate order in which they appear.

Table 24: show lldp local-information Output Fields

Field Name	Field Description
LLDP Local Information details	Information about the local system (the switch): • **Chassis ID**—MAC address associated with the switch. • **System name**—User-configured name of the switch. • **System descr**—System description containing information about the switch model and the current software image running on the switch. This information is taken from the software and is not configurable.
System Capabilities	Capabilities (such as **bridge** or **router**) that are supported or enabled on the system.
Management Information	Details of the management information: **Port Name**, **Port Address** (such as **10.204.34.35**), **Address Type** (such as **ipv4** or **ipv6**), **Port ID** (SNMP interface index), **Port ID Subtype**, and **Port Subtype**. The **Port Subtype** displays: • **ifIndex(2)**— IP address of the switch's management Ethernet interface (**me0**) or virtual management Ethernet (**VME**) interface address (for a virtual chassis) is used to manage the switch. • **unknown(1)**—IP management address has been configured with set **protocols lldp management-address**.

Table 24: 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 107
- Understanding 802.1X and LLDP and LLDP-MED on page 14

List of Sample Output
show lldp neighbors on page 235
show lldp neighbors interface ge-0/0/2 on page 236
show lldp neighbors interface ge-0/0/0.0 (for a VoIP AvayaTelephone with LLDP-MED Support) on page 237
show lldp neighbors interface ge-0/0/5.0 (with NetBIOS Snooping Enabled on the Switch) on page 238

Output Fields Table 25 on page 233 lists the output fields for the **show lldp neighbors** command. Output fields are listed in the approximate order in which they appear.

Table 25: 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 25: 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 25: 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	Details of management information: **Type** (such as **IPv4** or **IPv6**), **Address** (such as **10.204.34.35**), **Port ID**, **Subtype**, **Interface Subtype**, and organization identifier (**OID**) (appears when the **interface** option is used). The **Interface Subtype** displays: • **ifIndex(2)**— IP address of the neighbor's management Ethernet interface (**me0**) or virtual management Ethernet (**VME**) interface address (for a Virtual Chassis) is used to manage the switch. • **unknown(1)**—Neighbor's IP management address has been configured with set **protocols lldp management-address**.
Media Info	Additional details about the endpoint device appear when a device that supports LLDP-MED is attached to the interface. The specific details depend upon the capabilities of the device. Details might include: **Media endpoint class** (such as Class 3 for communication devices such as IP phones), **MED Hardware revision**, **MED Firmware revision**, **MED Software revision**, **MED Serial number**, **MED Manufacturer name**, **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

LLLDP Neighbor Information:
Local Information:
Index: 1 Time to live: 240 Time mark: Wed Dec  1 10:23:24 2010 Age: 29 secs
Local Interface    : ge-0/0/2.0
Parent Interface   : -
Local Port ID      : 507
Ageout Count       : 0

Neighbour Information:
Chassis type       : Mac address
Chassis ID         : 00:1f:12:38:7f:c0
Port type          : Locally assigned
Port ID            : 507
Port description   : ge-0/0/2.0
System name        : bng-l48p5-dev


System Description : Juniper Networks, Inc. ex4200-48p , version 10.4I0 Build
date: 2010-11-30 09:32:17 UTC

System capabilities
        Supported  : Bridge Router
        Enabled    : Bridge Router

Management Info
        Type              : IPv4
        Address           : 10.204.96.235
        Port ID           : 34
        Subtype           : 1
        Interface Subtype : ifIndex(2)
        OID               : 1.3.6.1.2.1.31.1.1.1.1.34
Media endpoint class: Network Connectivity

Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
       Subtype  : MAC/PHY Configuration/Status (1)
       Info     : Autonegotiation [supported, enabled (0x3)], PMD Autonegotiation
 Capability (0x1d00), MAU Type (0x0)
       Index    : 1

Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
       Subtype  : MDI Power (2)
       Info     : MDI Power Support [PSE supported ], MDI Power Pair  (signal),
MDI Power Class (class0)
       Index    : 2
```

show lldp neighbors interface ge-0/0/0.0 (for a VoIP AvayaTelephone with LLDP-MED Support)

```
user@switch>show lldp neighbors interface ge-0/0/0.0

LLDP Neighbor Information:
Local Information:
Index: 20 Time to live: 120 Time mark: Thu Apr 15 22:26:22 2010 Age: 16 secs
Local Interface    : ge-0/0/0.0
Parent Interface   : -
Local Port ID      : 517
Ageout Count       : 0

Neighbour Information:
Chassis type       : Network address
Chassis ID         : 0.0.0.0
Port type          : Mac address
Port ID            : 00:04:0d:fc:55:48
System name        : AVAFC5548

System capabilities
        Supported  : Bridge Telephone
        Enabled    : Bridge

Management Info
        Type              : IPv4
        Address           : 0.0.0.0
        Port ID           : 1
        Subtype           : 1
        Interface Subtype : ifIndex(2)
        OID               : 1.3.6.1.2.1.31.1.1.1.1.1
Media endpoint class: Class III Device

MED Hardware revision : 4610D01A
MED Firmware revision : b10d01b2_9.bin
MED Software revision : a10d01b2_9.bin
MED Serial number     : 07N510103424
MED Manufacturer name : Avaya
MED Model name        : 4610

Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
       Subtype  : MAC/PHY Configuration/Status (1)
       Info     : Autonegotiation [supported, enabled (0x3)], PMD Autonegotiation
 Capability (0x1d00), MAU Type (0x0)
       Index    : 1

Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
       Subtype  : MDI Power (2)
       Info     : MDI Power Support [PSE supported ], MDI Power Pair  (signal),
MDI Power Class (class0)
       Index    : 2

Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
       Subtype  : Link Aggregation (3)
       Info     : Aggregation Status (supported ), Aggregation Port ID (0)
       Index    : 3

Organization Info
       OUI      : IEEE 802.3 Private (0x00120f)
```

```
        Subtype  : Maximum Frame Size (4)
        Info     : MTU Size (1514)
        Index    : 4

Organization Info
        OUI      : Ethernet Bridged (0x0080c2)
        Subtype  : Port Vid (1)
        Info     : VLAN ID (10),
        Index    : 5

Organization Info
        OUI      : Juniper Specific (0x009069)
        Subtype  : Chassis Serial Type (1)
        Info     : Juniper Slot Serial [BQ0208211462]
        Index    : 6

Organization Info
        OUI      : Ethernet Bridged (0x0080c2)
        Subtype  : VLAN Name (3)
        Info     : VLAN ID (10), VLAN Name (vtest)
        Index    : 7
```

show lldp neighbors interface ge-0/0/5.0 (with NetBIOS Snooping Enabled on the Switch)

```
user@switch> show lldp neighbors interface ge-0/0/5

Age: 299999 secs
Local Interface    : ge-0/0/5.0
Parent Interface   : -
Chassis ID         : 00:10:94:00:00:02
Port description   : 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.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description Display remote Link Layer Discovery Protocol (LLDP) global statistics.

Options This command has no options.

Required Privilege Level view

Related Documentation
- Configuring LLDP (CLI Procedure) on page 107
- Understanding 802.1X and LLDP and LLDP-MED on page 14

List of Sample Output show lldp remote-global-statistics on page 240

Output Fields Table 26 on page 239 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 26: 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 *interface*>

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 *interface*—(Optional) Display LLDP statistics for the specified interface.

Required Privilege Level

view

Related Documentation

- Configuring LLDP (CLI Procedure) on page 107
- Understanding 802.1X and LLDP and LLDP-MED on page 14

List of Sample Output

show lldp statistics on page 242
show lldp statistics interface xe-3/0/0.0 on page 242

Output Fields

Table 27 on page 241 lists the output fields for the **show lldp statistics** command. Output fields are listed in the approximate order in which they appear.

Table 27: 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
- *accounting-server*
- *accounting-stop-on-access-deny*
- *Configuring RADIUS Accounting*

List of Sample Output show network-access aaa statistics accounting on page 243

Output Fields Table 28 on page 243 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 28: 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
- *authentication-server*
- Example: Connecting a RADIUS Server for 802.1X to a Switch on page 27

List of Sample Output
show network-access aaa statistics authentication on page 244
show network-access aaa statistics authentication (in QFX Series Switches) on page 244

Output Fields Table 29 on page 244 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 29: 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@lf0> show network-access aaa statistics authentication
Authentication module statistics
  Requests received: 2
  Accepts: 1
```

```
Rejects: 0
Challenges: 1
```

show network-access aaa statistics dynamic-requests

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
- *authentication-server*
- Example: Connecting a RADIUS Server for 802.1X to a Switch on page 27

List of Sample Output show network-access aaa statistics authentication on page 246

Output Fields Table 30 on page 246 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 30: 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
```