

Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to an EX-series 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 an EAP Access-Reject message.

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 (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 1
- Overview and Topology on page 1
- Configuration on page 3
- Verification on page 4

Requirements

This example uses the following hardware and software components:

- JUNOS Release 9.3 or later for EX-series switches
- One EX 4200 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 Example: Setting Up Basic Bridging and a VLAN for an EX-series Switch.
- Set up a connection between the switch and the RADIUS server. See Example: Connecting a RADIUS Server for 802.1X to an EX-series Switch.
- 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 1 on page 2 shows the topology used for this example. The RADIUS server is connected to the EX 4200 switch on access port `ge-0/0/10`. The switch acts as the authenticator Port Access Entity (PAE) and forwards credentials from the supplicant to the user database on the RADIUS server. The switch blocks all traffic and acts as a control gate until the supplicant is authenticated by the authentication server. A supplicant is connected to the switch through interface `ge-0/0/1`.

Figure 1: Topology for Configuration

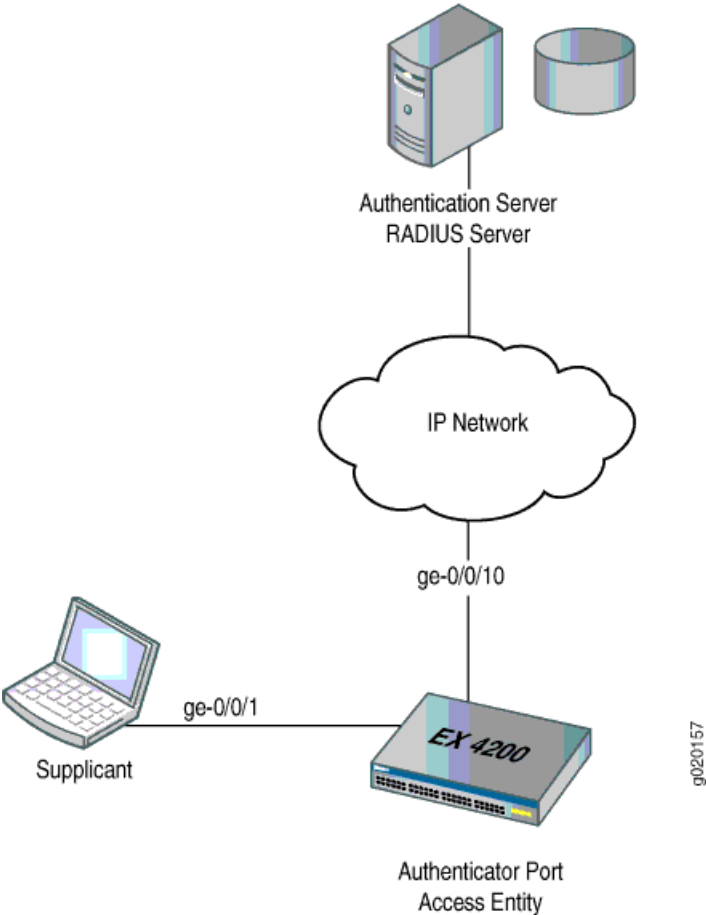


Table 1 on page 2 describes the components in this topology.

Table 1: Components of the Topology

Property	Settings
Switch hardware	EX 4200 access switch, 24 Gigabit Ethernet ports: 8 PoE ports.

Table 1: Components of the Topology (continued)

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 the *JUNOS Software System Basics Configuration Guide* at <http://www.juniper.net/techpubs/software/junos/>.

Configuration

To configure server fail fallback on the switch:

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 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 4

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.

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
v2         None
vlan-sf   50
vlan-sf    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 Topics**
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX-series Switch
 - Configuring Server Fail Fallback (CLI Procedure)
 - Configuring 802.1X RADIUS Accounting (CLI Procedure)
 - Filtering 802.1X Supplicants Using Vendor-Specific Attributes (CLI Procedure)
 - Understanding Server Fail Fallback and 802.1X Authentication on EX-series Switches

