Example: Setting Up 802.1X for Nonresponsive Hosts on an EX-series Switch and a RADIUS Server

If a device is not 802.1X-enabled, it is known as a nonresponsive host. To permit nonresponsive hosts access to the LAN, you can configure MAC RADIUS authentication on the switch interfaces to which the nonresponsive hosts are connected.

This example describes how to configure MAC RADIUS authentication for two nonresponsive hosts:

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

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

- Configured basic access between the EX-series switch and the RADIUS server. See Example: Connecting a RADIUS Server for 802.1X to an EX-series Switch.
- Performed basic bridging and VLAN configuration on the switch. See Example: Setting Up Basic Bridging and a VLAN for an EX-series Switch.
- Performed basic 802.1X configuration. See Configuring 802.1X Authentication (CLI Procedure).

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). If a device is not 802.1X-enabled, it is known as a nonresponsive host. To permit nonresponsive hosts access to the LAN, you can configure MAC RADIUS authentication on the interfaces to which the nonresponsive hosts are connected. When the MAC address of the nonresponsive host 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 nonresponsive host is configured as permitted on the RADIUS server, the switch opens LAN access to the nonresponsive host.

MAC RADIUS authentication can be one of several 802.1X authentication methods used on a single interface configured for multiple supplicants. However, you can configure the switch to immediately identify that the interface is only connected to a nonresponsive host and eliminate other authentication possibilities when they are not necessary for LAN security.

Figure 1 shows the two printers connected to the switch.

Figure 1: Topology for MAC RADIUS Authentication Configuration

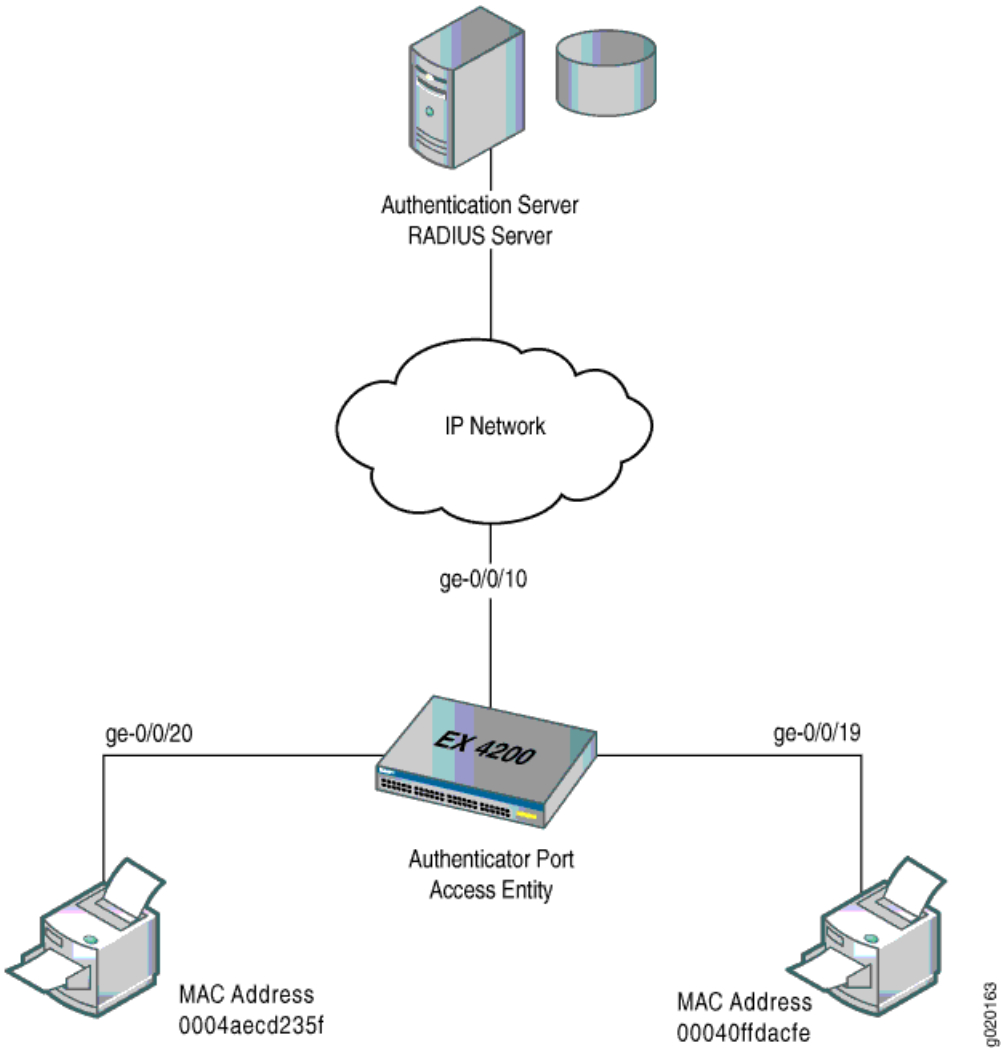

Table 1 shows the components in the example for MAC RADIUS authentication.

Table 1: Components of the MAC RADIUS Authentication Configuration Topology

Property	Settings
Switch hardware	EX 4200 24T, 24 Gigabit Ethernet ports: 8 PoE ports (ge-0/0/0 through ge-0/0/7) and 16 non-PoE ports (ge-0/0/8 through ge-0/0/23)

Table 1: Components of the MAC RADIUS Authentication Configuration Topology *(continued)*

VLAN name	default
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 90-second delay it takes the switch to determine whether the connected device is a nonresponsive host; MAC RADIUS authentication is the only 802.1X authentication needed on this interface.

Configuration

To configure MAC RADIUS authentication on the switch, perform these tasks:

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 in 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 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:=Local, User-Password = "00040ffdacfe"
0004aecd235f Auth-type:=Local, 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 4

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:

```
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 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: 00040ffdacfe, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: MAC Radius
      Authenticated VLAN: v200
     Reauthentication due in 17 seconds
user@switch> show dot1x interface ge-0/0/20.0 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 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: 0004aecd235f, 00:04:ae:cd:23:5f
      Operational state: Authenticated
      Authentication method: MAC Radius
      Authenticated VLAN: v200
     Reauthentication due in 23 seconds
```

Meaning The sample output from the show dot1x interface detail command displays the MAC address of the connected supplicant 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 Topics

- Configuring MAC RADIUS Authentication (CLI Procedure)
- Configuring 802.1X Authentication (CLI Procedure)
- Configuring 802.1X Authentication (J-Web Procedure)