

Example: Configuring Static MAC Bypass of Authentication on an EX Series Switch

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

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

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

- Requirements on page 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 9.0 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:

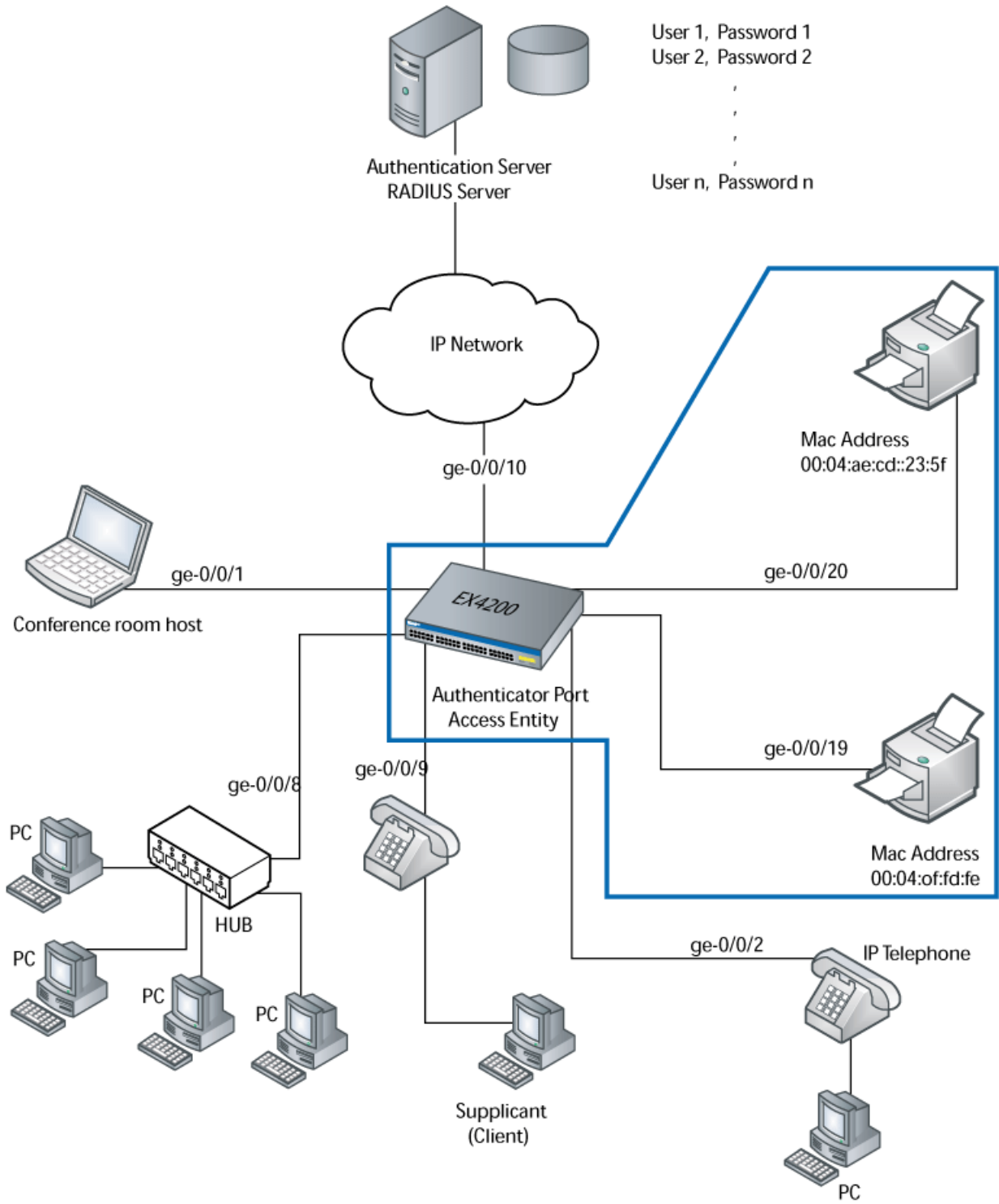
- Performed basic bridging and VLAN configuration on the switch. See Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.

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 1 shows the two printers connected to the EX4200.

Figure 1: Topology for Static MAC Authentication Configuration



The interfaces shown in Table 1 will be configured for static MAC authentication.

Table 1: 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

To configure static MAC authentication, perform these tasks:

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

Step-by-Step Procedure Configure static MAC authentication:

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

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

2. 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]
```

3. Configure the 802.1X authentication method:

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

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 4

Verifying Static MAC Bypass of Authentication

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

Action Use 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 Topics**
- Configuring 802.1X Authentication (J-Web Procedure)
 - Configuring Static MAC Bypass of Authentication (CLI Procedure)
 - Configuring 802.1X Interface Settings (CLI Procedure)
 - Understanding MAC RADIUS Authentication on EX Series Switches

Published: 2009-07-21