Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX-series Switch

802.1x Port-Based Network Access Control (PNAC) authentication on EX-series switches provides three types of authentication to meet the access needs of your enterprise LAN:

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

This example configures an EX-series 4200 switch to use IEEE 802.1X to authenticate supplicants that use three different administrative modes:

Requirements

This example uses the following hardware and software components:

- JUNOS Release 9.0 or later for EX-series switches
- One EX-series 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 configure the ports for 802.1X authentciation, be sure you have:

- Installed your EX-series switch. See Installing and Connecting an EX 3200 or EX 4200 Switch.
- Performed the initial switch configuration. See Connecting and Configuring an EX-series Switch (J-Web Procedure).
- Performed basic bridging and VLAN configuration on the switch. See Example: Setting Up Basic Bridging and a VLAN for an EX-series Switch.
- Configured users on the authentication server.

Overview and Topology

As shown in Figure 1 on page 3, the topology contains an EX 4200 access switch connected to the authentication server on port ge-0/0/10. Interfaces ge-0/0/8, ge-0/0/9, and ge-0/0/11 will be configured for three different administrative modes.

Figure 1: Topology for Configuring Supplicant Modes

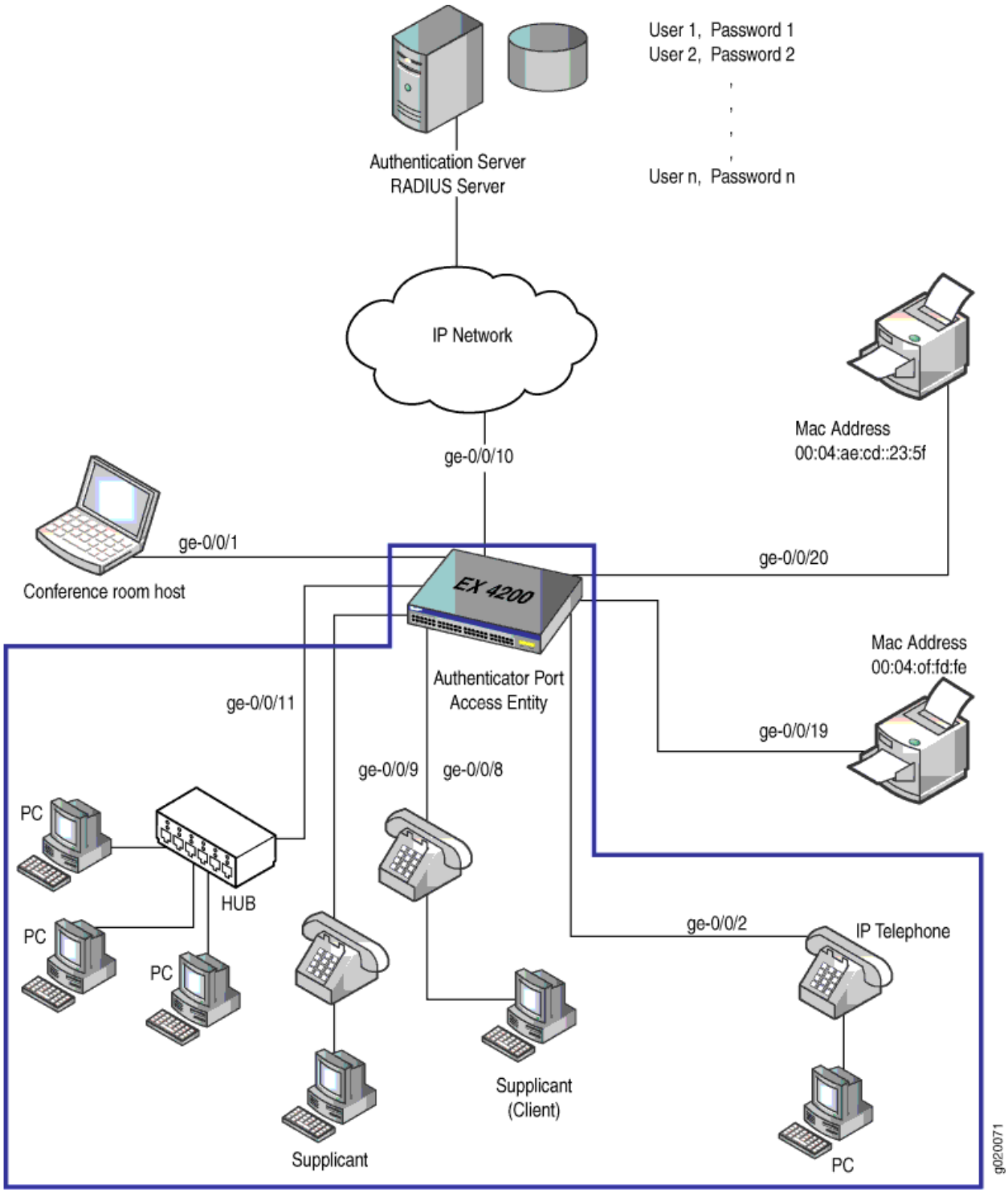

Table 1: Components of the Supplicant Mode Configuration Topology

Property	Settings
Switch hardware	EX-series 4200 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)
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 supplicant that connects to an authenticator port. All other supplicants connecting to the authenticator port after the first supplicant has connected successfully, whether they are 802.1X-enabled or not, are permitted free access to the port without further authentication. If the first authenticated supplicant logs out, all other supplicants are locked out until a supplicant authenticates.

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

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

Configuration of 802.1X to Support Multiple Supplicant Modes

To configure 802.1X authentication to support multiple supplicants, perform these tasks:

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 5

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 with 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
  Reauthentication: Enabled Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
      Supplicant: user100, 00:00:00:00:22:22
      Operational state: Authenticated
      Reauthentication due in 506 seconds
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
  Reauthentication: Enabled Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Supplicant timeout: 30 seconds
      Supplicant: user101, 00:13:00:00:28:22
      Operational state: Authenticated
      Reauthentication due in 917 seconds
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
  Reauthentication: Enabled Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
      Supplicant: user102, 00:10:12:e0:28:22
      Operational state: Authenticated
      Reauthentication due in 1788 seconds
```

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 Topics

- Understanding 802.1X Authentication on EX-series Switches
- Example: Connecting a RADIUS Server for 802.1X to an EX-series Switch
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX-series Switch
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX-series Switch
- Configuring 802.1X RADIUS Accounting (CLI Procedure)
- Filtering 802.1X Supplicants Using Vendor-Specific Attributes (CLI Procedure)