

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX-series Switch

802.1X on EX-series 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 on page 1
- Overview and Topology on page 1
- Configuration of a Guest VLAN That Includes 802.1X Authentication 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 4200 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:

- 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*.

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 to 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 supplicants that fail 802.1X authentication to a corporate LAN with access to a VLAN with limited resources.

Figure 1 shows the conference room connected to the switch at interface `ge-0/0/1`.

Figure 1: Topology for Guest VLAN Example

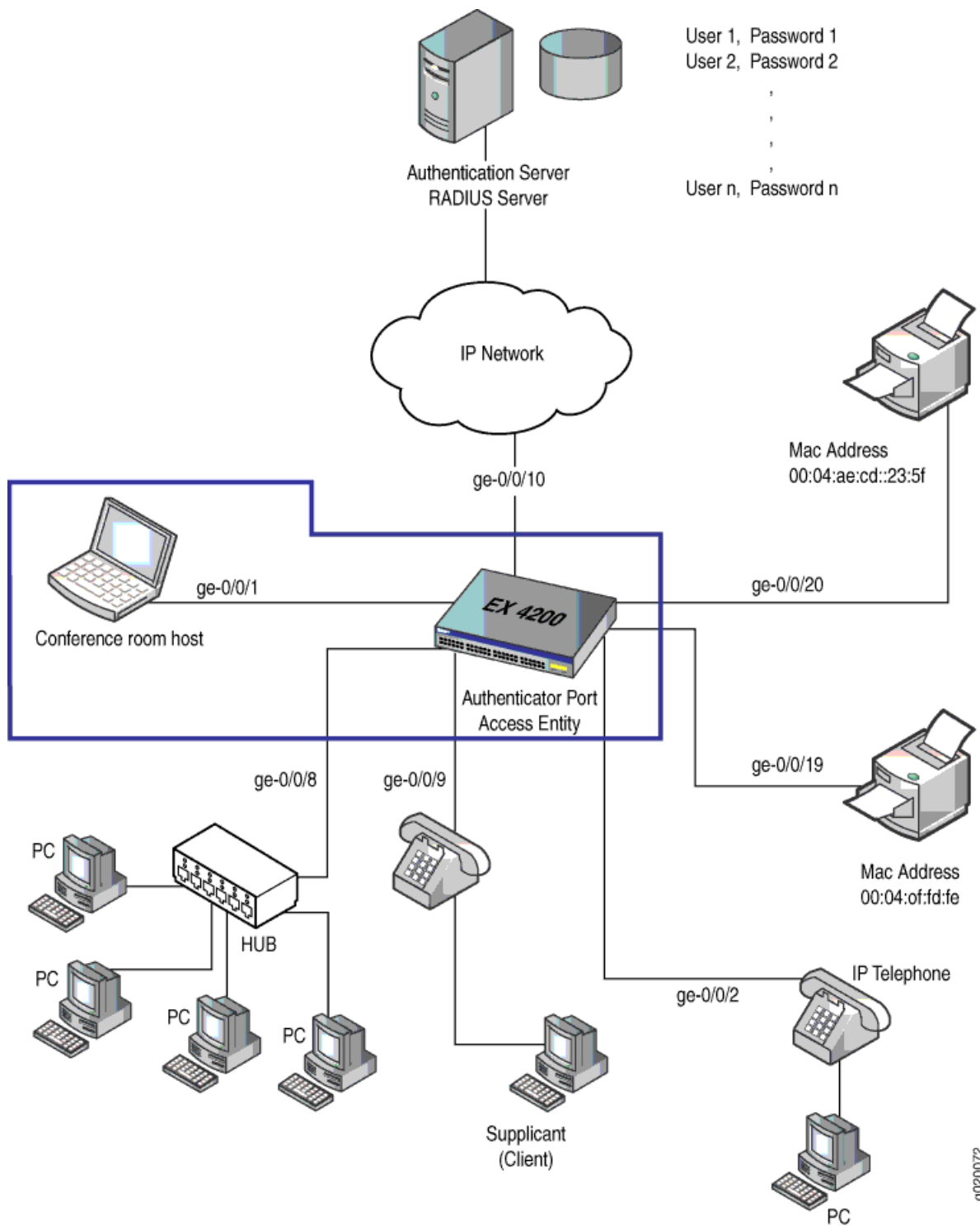


Table 1: Components of the Guest VLAN Topology

Property	Settings
Switch hardware	EX 4200 switch, 24 Gigabit Ethernet interfaces: 8 PoE interfaces (<i>ge-0/0/0</i> through <i>ge-0/0/7</i>) and 16 non-PoE interfaces (<i>ge-0/0/8</i> through <i>ge-0/0/23</i>)
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 <i>ge-0/0/10</i>

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

To create a guest VLAN and configure 802.1X authentication, perform these tasks:

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 an EX-series 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 {
```

```
vlan {  
    guest-vlan {  
        vlan-id 300;  
    }  
}
```

Verification

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

- Verifying That the Guest VLAN is Configured on page 4

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.

Action Use 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: Multiple
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Guest VLAN membership: guest-vlan
Reauthentication: Enabled Reauthentication interval: 3600 seconds
Supplicant timeout: 30 seconds
Supplicant: user1, 00:00:00:00:13:23
    Operational state: Authenticated
    Reauthentication due in 3307 seconds
```

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

The output from 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 Topics**
- Example: Connecting a RADIUS Server for 802.1X to an EX-series Switch
 - Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX-series Switch
 - Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX-series Switch
 - Configuring 802.1X Authentication (CLI Procedure)

