Example: Connecting a RADIUS Server for 802.1X to an EX-series Switch

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 providing credentials that have been verified against a user database are allowed access to the network. You can use a RADIUS server as the user database.

This example describes how to connect a RADIUS server to an EX-series switch. and configure it for 802.1X:

Requirements

This example uses the following hardware and software components:

- JUNOS Release 9.0 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:

- 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

The EX-series switch acts as an authenticator Port Access Entity (PAE). It blocks all traffic and acts as a control gate until the supplicant (client) is authenticated by the server. All other users and devices are denied access.

Figure 1 shows one EX 4200 switch that is connected to the devices listed in Table 1.

Figure 1: Topology for Configuration

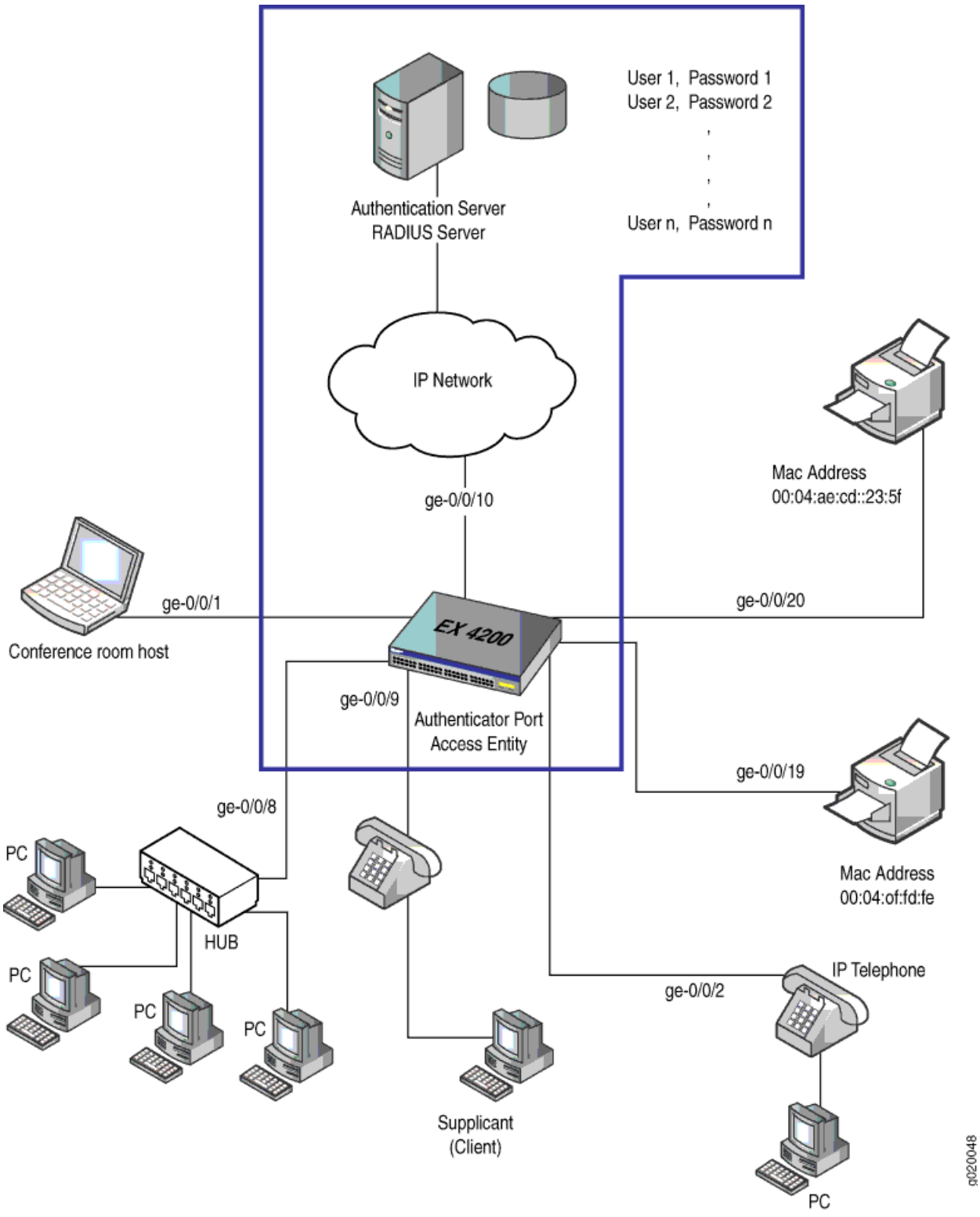

Table 1: Components of the Topology

Property	Settings
Switch hardware	EX 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)
VLAN name	default
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, connect the RADIUS server to access port ge-0/0/10 on the EX 4200 switch. The switch acts as the authenticator and forwards credentials from the supplicant to the user database on the RADIUS server. You must configure connectivity between the EX 4200 and the RADIUS server by specifying the address of the server and configuring the secret password. This information is configured in an access profile on the switch.

NOTE: *JUNOS Software System Basics Configuration Guide*.

For more information about authentication, authorization, and accounting (AAA) services, please see the *JUNOS Software System Basics Configuration Guide* at http://www.juniper.net/techpubs/software/junos/

Configuration

CLI Quick Configuration

To quickly connect the RADIUS server to the switch, copy the following commands and paste them into the switch terminal window:

```
[edit]
set access radius-server 10.0.0.100 secret juniper
set access profile profile1 authentication-order radius
set access profile profile1 radius authentication-server 10.0.0.100 10.2.14.200
```

Step-by-Step Procedure

To connect the RADIUS server to the switch:

1. Define the address of the server, and configure the secret password. The secret password on the switch must match the secret password on the server:

   ```
   [edit access]
   user@switch# set radius-server 10.0.0.100 secret juniper
   ```

2. Configure the authentication order, making radius the first method of authentication:

   ```
   [edit access profile]
   user@switch# set profile1 authentication-order radius
   ```

3. Configure a list of server IP addresses to be tried in order to authenticate the supplicant:

```
[edit access profile]
user@switch# set profile1 radius authentication-server 10.0.0.100
10.2.14.200
```

Results Display the results of the configuration:

```
user@switch> show configuration access
radius-server {
    10.0.0.100
        port 1812;
        secret "$9$qPT3ApBSrv69rvWLVb.P5"; ## SECRET-DATA
        }
    }
    profile profile1{
        authentication-order radius;
        radius {
            authentication-server 10.0.0.100 10.2.14.200;
        }
    }
}
```

Verification

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

- Verify That the Switch and RADIUS Server are Properly Connected on page 4

Verify That the Switch and RADIUS Server are Properly Connected

Purpose Verify that the RADIUS server is connected to the switch on the specified port.

Action Ping the RADIUS server to verify the connection between the switch and the server:

```
user@switch> ping 10.0.0.100
PING 10.0.0.100 (10.0.0.100): 56 data bytes
64 bytes from 10.93.15.218: icmp_seq=0 ttl=64 time=9.734 ms
64 bytes from 10.93.15.218: icmp_seq=1 ttl=64 time=0.228 ms
```

Meaning ICMP echo request packets are sent from the switch to the target server at 10.0.0.100 to test whether it is reachable across the IP network. ICMP echo responses are being returned from the server, verifying that the switch and the server are connected.

Related Topics

- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on 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

- Example: Setting Up 802.1X for Nonresponsive Hosts on an EX-series Switch
- Configuring 802.1X RADIUS Accounting (CLI Procedure)
- Filtering 802.1X Supplicants Using Vendor-Specific Attributes (CLI Procedure)