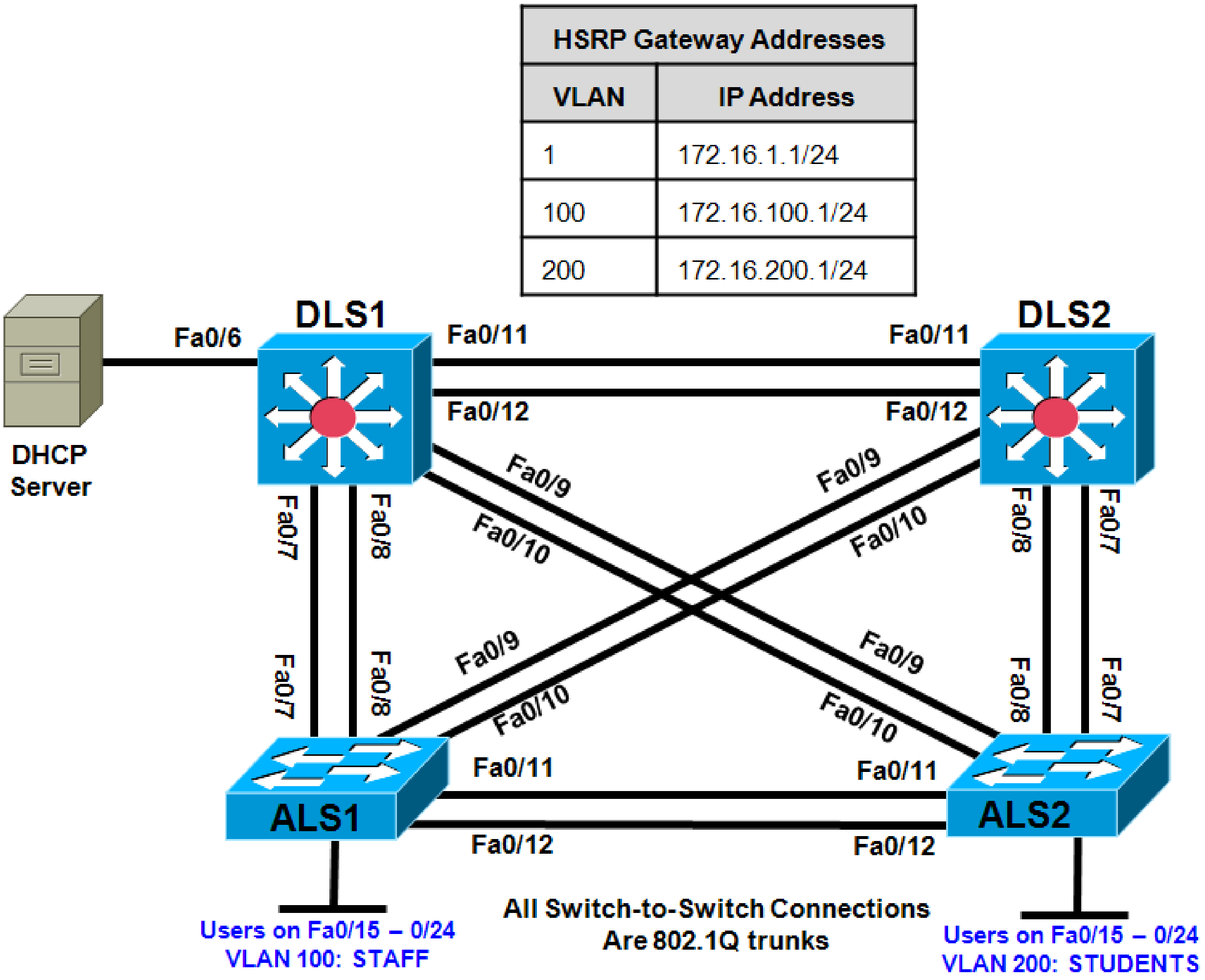
Chapter 6 Lab 6-1, Securing Layer 2 Switches

Topology



HSRP Gateway Addresses	
VLAN	**IP Address**
1	172.16.1.1/24
100	172.16.100.1/24
200	172.16.200.1/24

All Switch-to-Switch Connections Are 802.1Q trunks

Objectives

- Secure the Layer 2 network against MAC flood attacks.
- Prevent DHCP spoofing attacks.
- Prevent unauthorized access to the network using AAA and 802.1X.

Background

A fellow network engineer that you have known and trusted for many years has invited you to lunch this week. At lunch, he brings up the subject of network security and how two of his former co-workers had been arrested for using different Layer 2 attack techniques to gather data from other users in the office for their own personal gain in their careers and finances. The story shocks you because you have always known your friend to be very cautious with security on his network. His story makes you realize that your business network has been cautious with external threats, Layer 3–7 security, firewalls at the borders, and so on, but insufficient at Layer 2 security and protection inside the local network.

When you get back to the office, you meet with your boss to discuss your concerns. After reviewing the company's security policies, you begin to work on a Layer 2 security policy.

First, you establish which network threats you are concerned about and then put together an action plan to mitigate these threats. While researching these threats, you learn about other potential threats to Layer 2 switches that might not be malicious but could threaten network stability. You decide to include these threats in the policies as well.

Other security measures need to be put in place to further secure the network, but you begin with configuring the switches against a few specific types of attacks, including MAC flood attacks, DHCP spoofing attacks, and unauthorized access to the local network. You plan to test the configurations in a lab environment before placing them into production.

Note: This lab uses Cisco WS-C2960-24TT-L switches with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin, and Catalyst 3560-24PS with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. You can use other switches (such as 2950 or 3550) and Cisco IOS Software versions if they have comparable capabilities and features. Depending on the switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Required Resources

- 2 switches (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560-ADVIPSERVICESK9-mz image or comparable)
- Ethernet and console cables

Note: Be sure to save your final device configurations to use with the next lab. Because the VLAN and VTP commands do not display in the configs, you must re-enter them in the next lab.

Step 1: Prepare the switches for the lab.

Erase the startup config, delete the vlan.dat file, and reload the switches. Refer to Lab 1-1, "Clearing a Switch" and Lab 1-2, "Clearing a Switch Connected to a Larger Network" to prepare the switches for this lab. Cable the equipment as shown.

Step 2: Configure the basic switch parameters and trunking.

a. Configure the management IP addresses in VLAN 1. Configure the hostname, password, and Telnet access on all four switches. HSRP will be used later in the lab, so set up the IP addressing for VLAN 1 on DLS1 and DLS2. Because 172.16.1.1 will be the virtual default gateway for VLAN 1, use .3 and .4 for the IP addresses on DLS1 and DLS2, respectively.

b. Configure a default gateway on the access layer switches. The distribution layer switches are Layer 3 devices and do not need default gateways.

c. Configure 802.1q trunking between the switches according to the diagram. On the 2960 switches, only dot1q is supported, therefore the **switchport trunk encapsulation** command is unavailable.

```
Switch(config)# hostname ALS1
ALS1(config)# enable secret class
ALS1(config)# line vty 0 15
ALS1(config-line)# password cisco
ALS1(config-line)# login
```

```
ALS1(config-line)# exit
ALS1(config)# interface vlan 1
ALS1(config-if)# ip address 172.16.1.101 255.255.255.0
ALS1(config-if)# no shutdown
ALS1(config-if)# exit
ALS1(config)# ip default-gateway 172.16.1.1
ALS1(config)# interface range fastethernet 0/7 - 12
ALS1(config-if-range)# switchport mode trunk

Switch(config)# hostname ALS2
ALS2(config)# enable secret class
ALS2(config)# line vty 0 15
ALS2(config-line)# password cisco
ALS2(config-line)# login
ALS2(config-line)# exit
ALS2(config)# interface vlan 1
ALS2(config-if)# ip address 172.16.1.102 255.255.255.0
ALS2(config-if)# no shutdown
ALS2(config-if)# exit
ALS2(config)# ip default-gateway 172.16.1.1
ALS2(config)# interface range fastethernet 0/7 - 12
ALS2(config-if-range)# switchport mode trunk

Switch(config)# hostname DLS1
DLS1(config)# enable secret class
DLS1(config)# line vty 0 15
DLS1(config-line)# password cisco
DLS1(config-line)# login
DLS1(config-line)# exit
DLS1(config)# interface vlan 1
DLS1(config-if)# ip address 172.16.1.3 255.255.255.0
DLS1(config-if)# no shutdown
DLS1(config-if)# exit
DLS1(config)# interface range fastethernet 0/7 - 12
DLS1(config-if-range)# switchport trunk encapsulation dot1q
DLS1(config-if-range)# switchport mode trunk

Switch(config)# hostname DLS2
DLS2(config)# enable secret class
DLS2(config)# line vty 0 15
DLS2(config-line)# password cisco
DLS2(config-line)# login
DLS2(config-line)# exit
DLS2(config)# interface vlan 1
DLS2(config-if)# ip address 172.16.1.4 255.255.255.0
DLS2(config-if)# no shutdown
DLS2(config-if)# exit
DLS2(config)# interface range fastethernet 0/7 - 12
DLS2(config-if-range)# switchport trunk encapsulation dot1q
DLS2(config-if-range)# switchport mode trunk
```

d. Verify trunking and spanning-tree operations using the **show interfaces trunk** and **show spanning-tree** commands.

Which switch is the root bridge?

For ALS1 and ALS2, which trunks have a role of designated (Desg), Alternate (Altn), and Root?

Is trunk negotiation being used here? Which mode are the trunks in?

Step 3: Configure VTP on ALS1 and ALS2.

Set up the VLANs according to the diagram. Two VLANs are in use at this time: one for students, and one for faculty and staff. These VLANs will be created on DLS1, which is set up as a VTP server. DLS2 also remains in its default VTP mode and acts as a server as well. ALS1 and ALS2 are configured as VTP clients.

The user access ports for these VLANs also need to be configured on ALS1 and ALS2. Set up these ports as static access ports and activate spanning-tree PortFast. Configure these ports according to the diagram.

a. Configure ALS1 for the VTP client changes.

```
ALS1(config)# vtp mode client
Setting device to VTP CLIENT mode.
ALS1(config)# interface range fa0/15 - 24
ALS1(config-if-range)# switchport mode access
ALS1(config-if-range)# switchport access vlan 100
ALS1(config-if-range)# spanning-tree portfast

%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast will be configured in 10 interfaces due to the range command
 but will only have effect when the interfaces are in a non-trunking mode.
```

b. Configure ALS2 for the VTP client changes.

```
ALS2(config)# vtp mode client
Setting device to VTP CLIENT mode.
ALS2(config)# interface range fa0/15 - 24
ALS2(config-if-range)# switchport mode access
ALS2(config-if-range)# switchport access vlan 200
ALS2(config-if-range)# spanning-tree portfast

%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast will be configured in 10 interfaces due to the range command
 but will only have effect when the interfaces are in a non-trunking mode.
```

Step 4: Configure IP routing, the VLANs, VLAN SVIs, and HSRP on DLS1 and DLS2.

HSRP is a requirement for the network, and VLANs 100 and 200 are configured to use HSRP to provide redundancy at Layer 3. Use the **priority** command to make DLS1 the active router for VLANs 1 and 100, and DLS2 the active router for VLAN 200.

a. Configure VTP, VLANs, and IP routing on DLS1.

```
DLS1(config)# vtp domain SWPOD
DLS1(config)# vtp version 2
DLS1(config)# vlan 100
DLS1(config-vlan)# name Staff
DLS1(config-vlan)# vlan 200
DLS1(config-vlan)# name Student
DLS1(config-vlan)# exit

DLS1(config)# ip routing
```

b. Configure switch virtual interfaces (SVIs) and HSRP on DLS1.

```
DLS1(config)# interface vlan 1
DLS1(config-if)# standby 1 ip 172.16.1.1
DLS1(config-if)# standby 1 preempt
DLS1(config-if)# standby 1 priority 150

DLS1(config-if)# interface vlan 100
DLS1(config-if)# ip add 172.16.100.3 255.255.255.0
DLS1(config-if)# standby 1 ip 172.16.100.1
DLS1(config-if)# standby 1 preempt
DLS1(config-if)# standby 1 priority 150

DLS1(config-if)# interface vlan 200
DLS1(config-if)# ip add 172.16.200.3 255.255.255.0
DLS1(config-if)# standby 1 ip 172.16.200.1
DLS1(config-if)# standby 1 preempt
DLS1(config-if)# standby 1 priority 100
```

c. Configure IP routing, VLAN SVIs, and HSRP on DLS2.

```
DLS2(config)# ip routing
DLS2(config)# interface vlan 1
DLS2(config-if)# standby 1 ip 172.16.1.1
DLS2(config-if)# standby 1 preempt
DLS2(config-if)# standby 1 priority 100
DLS2(config-if)# interface vlan 100
DLS2(config-if)# ip add 172.16.100.4 255.255.255.0
DLS2(config-if)# standby 1 ip 172.16.100.1
DLS2(config-if)# standby 1 preempt
DLS2(config-if)# standby 1 priority 100

DLS2(config-if)# interface vlan 200
DLS2(config-if)# ip add 172.16.200.4 255.255.255.0
DLS2(config-if)# standby 1 ip 172.16.200.1
DLS2(config-if)# standby 1 preempt
DLS2(config-if)# standby 1 priority 150
```

d. Verify your configurations using the **show vlan brief**, **show vtp status**, **show standby brief**, and **show ip route** commands. Output from DLS1 is shown here.

```
DLS1# show vlan brief
```

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -----------------------------
--
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17,
Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21,
Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
100  Staff                            active
200  Student                          active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

How many VLANs are active in the VTP domain?

```
DLS1# show vtp status
VTP Version                     : running VTP2
Configuration Revision          : 2
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 : SWPOD
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x1A 0x33 0x4D 0xA1 0x18 0xE6 0xBE 0xBA
Configuration last modified by 172.16.1.3 at 3-1-93 00:41:51
Local updater ID is 172.16.1.3 on interface Vl1 (lowest numbered VLAN
interface
found)
```

```
DLS1# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl1         1    150 P Active  local           172.16.1.4      172.16.1.1
Vl100       1    150 P Active  local           172.16.100.4    172.16.100.1
Vl200       1    100 P Standby 172.16.200.4    local           172.16.200.1
```

What is the active router for VLANs 1 and 100? What is the active router for VLAN 200?

```
DLS1# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
```

```
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, Vlan1
C       172.16.100.0 is directly connected, Vlan100
C       172.16.200.0 is directly connected, Vlan200
```

What would be the effect on virtual interface VLAN 100 if VLAN 100 had not been created?

Step 5: Specify verification methods and mitigation techniques for attack types.

Complete the following table with the appropriate verification methods and mitigation approaches for the attack types specified in the left column.

Attack Type	Verification	Mitigation
MAC address spoofing or flooding		
DHCP spoofing		
Unauthorized LAN access		

Step 6: Configure port security.

To protect against MAC flooding or spoofing attacks, configure port security on the VLAN 100 and 200 access ports. Because the two VLANs serve different purposes—one for staff and one for students—configure the ports to meet the different requirements.

The student VLAN must allow MAC addresses assigned to a port to change, because most of the students use laptops and move around within the network. Set up port security so that only one MAC address is allowed on a port at a given time. This type of configuration does not work on ports that need to service IP phones with PCs attached. In this case, there would be two allowed MAC addresses. To enable security on a port, you must first issue the **switchport port-security** command by itself.

The staff MAC addresses do not change often, because the staff uses desktop workstations provided by the IT department. In this case, you can configure the staff VLAN so that the MAC address learned on a port is added to the configuration on the switch as if the MAC address were configured using the **switchport port-security mac-address** command. This feature, which is called sticky learning, is available on some switch platforms. It combines the features of dynamically learned and statically configured addresses. The staff ports also allow for a maximum of two MAC addresses to be dynamically learned per port.

a. Enter the configuration for the student access ports on ALS2. To enable basic port security, issue the **switchport port-security** command.

   Note: By default, issuing the **switchport port-security** command by itself sets the maximum number of MAC addresses to 1**,** and the violation mode to shutdown. It is not necessary to specify the maximum number of addresses, unless it is greater than 1.

   ```
   ALS2(config)# interface range fastethernet 0/15 - 24
   ALS2(config-if-range)# switchport port-security
   ```

b. Verify the configuration for ALS2 using the **show port-security** *interface* command.

```
ALS2# show port-security interface fa0/15
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

c. Enter the configuration of the staff ports on ALS1. First, enable port security with the **switchport port-security** command. Use the **switchport port-security maximum** *#_of_MAC_addresses* command to change the maximum number of MAC addresses to 2, and use the **switchport port-security mac-address sticky** command to allow the two addresses to be learned dynamically.

```
ALS1(config)# interface range fastethernet 0/15 - 24
ALS1(config-if-range)# switchport port-security
ALS1(config-if-range)# switchport port-security maximum 2
ALS1(config-if-range)# switchport port-security mac-address sticky
```

This time two MAC addresses are allowed. Both will be dynamically learned and then added to the running configuration.

d. Verify the configuration using the **show port-security** *interface* command.

```
ALS1# show port-security int fa0/15
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Step 7: Configure DHCP snooping.

DHCP spoofing is a type of attack primarily used to assign IP addressing and configuration information by an unauthorized device. This can lead to a denial of service or traffic interception. The attacker replies to a DHCP request, claiming to have valid gateway and DNS information. A valid DHCP server might also reply to the request, but if the attacker’s reply reaches the requestor first, the invalid information from the attacker is used.

To help protect the network from such an attack, you can use DHCP snooping. DHCP snooping is a Cisco Catalyst feature that determines which switch ports are allowed to respond to DHCP requests. Ports are identified as trusted or untrusted. Trusted ports permit all DHCP messages, while untrusted ports permit (ingress) DHCP requests only. Trusted ports can host a DHCP server or can be an uplink toward a DHCP server. If a rogue device on an untrusted port attempts to send a DHCP response packet into the network, the port is disabled. From a DHCP snooping perspective, untrusted access ports should not send any DHCP server responses, such as a DHCPOFFER, DHCPACK, or DHCPNAK.

a. Enable DLS1 and DLS2 to trust DHCP relay information from ALS1 and ALS2 so that the DHCP server can respond to the ALS1 and ALS2 trusted port requests. This is accomplished using the **ip dhcp relay information trust-all** command.

```
DLS1(config)# ip dhcp relay information trust-all

DLS2(config)# ip dhcp relay information trust-all
```

Note: It is not necessary to enable DHCP snooping on the distribution layer switches, although this would allow DLS1 and DLS2 to trust ALS1 and ALS2 as relay agents.

b. Configure ALS1 and ALS2 to trust DHCP information on the trunk ports only, and limit the rate that requests are received on the access ports.

Configuring DHCP snooping on the access layer switches involves the following process:

- Turn snooping on globally using the **ip dhcp snooping** command.
- Configure the trusted interfaces with the **ip dhcp snooping trust** command. By default, all ports are considered untrusted unless statically configured to be trusted.
- Configure a DHCP request rate limit on the user access ports to limit the number of DHCP requests that are allowed per second. This is configured using the **ip dhcp snooping limit rate** *rate_in_pps*. This command prevents DHCP starvation attacks by limiting the rate of the DHCP requests on untrusted ports.
- Configure the VLANs that will use DHCP snooping. In this scenario, DHCP snooping will be used on both the student and staff VLANs.

```
ALS1(config)# ip dhcp snooping
ALS1(config)# interface range fastethernet 0/7 - 12
ALS1(config-if-range)# ip dhcp snooping trust
ALS1(config-if-range)# exit
ALS1(config)# interface range fastethernet 0/15 - 24
ALS1(config-if-range)# ip dhcp snooping limit rate 20
ALS1(config-if-range)# exit
ALS1(config)# ip dhcp snooping vlan 100,200

ALS2(config)# ip dhcp snooping
ALS2(config)# interface range fastethernet 0/7 - 12
ALS2(config-if-range)# ip dhcp snooping trust
ALS2(config-if-range)# exit
ALS2(config)# interface range fastethernet 0/15 - 24
ALS2(config-if-range)# ip dhcp snooping limit rate 20
ALS2(config-if-range)# exit
ALS2(config)# ip dhcp snooping vlan 100,200
```

c. Verify the configurations on ALS1 and ALS2 using the **show ip dhcp snooping** command.

```
ALS2# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
100,200
DHCP snooping is operational on following VLANs:
100,200
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
```

```
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/7              yes         unlimited
FastEthernet0/8              yes         unlimited
FastEthernet0/9              yes         unlimited
FastEthernet0/10             yes         unlimited
FastEthernet0/11             yes         unlimited
FastEthernet0/12             yes         unlimited
FastEthernet0/15             no          20
FastEthernet0/16             no          20
FastEthernet0/17             no          20
FastEthernet0/18             no          20
FastEthernet0/19             no          20
FastEthernet0/20             no          20
FastEthernet0/21             no          20
FastEthernet0/22             no          20
FastEthernet0/23             no          20
FastEthernet0/24             no          20
```

Will DHCP replies be allowed on access ports assigned to VLAN 200?

How many DHCP packets will be allowed on Fast Ethernet 0/16 per second?

Step 8: Configure AAA.

The authentication portion of AAA requires a user to be identified before being allowed access to the network. Authentication is configured by defining a list of methods for authentication and applying that list to specific interfaces. If lists are not defined, a default list is used.

For this network, it has been decided that AAA using 802.1X will be used to control user access for the staff VLAN using a local list of usernames and passwords. When a radius server is added to the network, all user ports, including the student VLAN, will also be added to the configuration.

The IEEE 802.1X standard defines a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports. The authentication server authenticates each workstation that is connected to a switch port before making any services that are offered by the switch or the LAN available.

Until the workstation is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the workstation is connected. After authentication succeeds, normal traffic can pass through the port.

a. Enter the configuration for ALS1.

Use the **aaa new-model** command to turn on AAA authentication on ALS1. The **aaa authentication dot1x default local** command tells the switch to use a local database of usernames and passwords to authenticate the users. Users are assigned to the database using the **username** *username* **password** *password* command. The **dot1x system-auth-control** command activates global support for 802.1X authentication.

The Fast Ethernet interfaces used for VLAN 100 staff access are configured using the **dot1x port-control auto** command. The **auto** keyword allows the switch port to begin in the unauthorized state, and allows the negotiation between the client and server to authenticate the user. Once authenticated, the user is allowed access to the network resources.

```
ALS1(config)# username janedoe password 0 cisco
ALS1(config)# username johndoe password 0 cisco
ALS1(config)# username joesmith password 0 cisco
ALS1(config)# aaa new-model
ALS1(config)# aaa authentication dot1x default local
ALS1(config)# dot1x system-auth-control
ALS1(config)# int range fa 0/15 - 24
ALS1(config-if-range)# dot1x port-control auto
```

Note: For switches running Cisco IOS version 12.2(50)SE or later, the **dot1x port-control auto** command is replaced with the following interface-level commands:

```
authentication port-control auto
dot1x pae authenticator
```

b. Verify the AAA configuration using the **show dot1x interface** command.

```
ALS1#show dot1x interface fa0/15
Dot1x Info for FastEthernet0/15
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
Violation Mode            = PROTECT
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
```

If a user with a username frankadams attempts to connect to the staff VLAN access ports, will the user be allowed access? Will the user be allowed access to the student VLAN ports?

Note: Save your final device configurations for use with the next lab.

How will the configuration need to be changed when a radius server is added to the network?