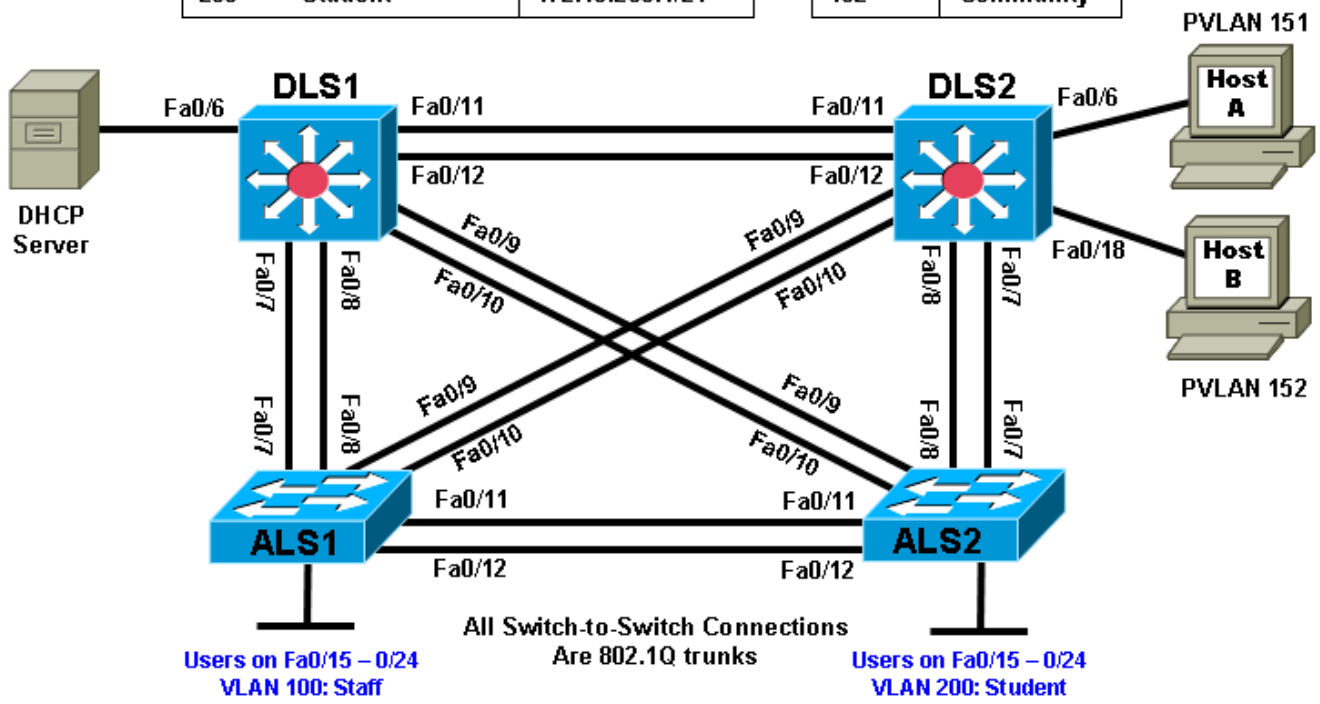
Chapter 6 Lab 6-3, Securing VLANs with Private VLANs, RACLs, and VACLs

Topology

HSRP Gateway Addresses		
VLAN		IP Address
1	Management	172.16.1.1/24
100	Staff	172.16.100.1/24
150	Server-farm	172.16.150.1/24
200	Student	172.16.200.1/24

PVLAN	Purpose
150	Primary
151	Isolated
152	Community



Objectives

- Secure the server farm using private VLANs.
- Secure the staff VLAN from the student VLAN.
- Secure the staff VLAN when temporary staff personnel are used.

Background

In this lab, you will configure the network to protect the VLANs using router ACLs, VLAN ACLs, and private VLANs. First, you will secure the new server farm by using private VLANs so that broadcasts on one server VLAN are not heard by the other server VLAN. Service providers use private VLANs to separate different

customers' traffic while utilizing the same parent VLAN for all server traffic. The private VLANs provide traffic isolation between devices, even though they might exist on the same VLAN.

You will then secure the staff VLAN from the student VLAN by using a RACL, which prevents traffic from the student VLAN from reaching the staff VLAN. This allows the student traffic to utilize the network and Internet services while keeping the students from accessing any of the staff resources.

Lastly, you will configure a VACL that allows a host on the staff network to be set up to use the VLAN for access but keeps the host isolated from the rest of the staff machines. This machine is used by temporary staff employees.

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 switches 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)
- 2 PCs (Windows OS) PC-A and PC-B (plus an optional PC for testing, if available)
- Ethernet and console cables

Step 1: Load and verify the configurations from lab 6-2.

a. Verify that the configurations from Lab 6-2 are loaded on the devices by issuing the **show vtp status** command. The output should show that the current VTP domain is SWPOD, and VLANs 100 and 200 should be represented in the number of existing VLANs. The output from switch ALS1 is shown as an example. If the switches are not configured properly, erase the startup config, delete the vlan.dat file, and load the configurations saved at the end of lab 6-2.

Note: If you are loading the configurations from Lab 6-2, they do not include VLAN and VTP commands. You must first configure ALS1 and ALS2 as VTP clients and then create VLANs 100 (staff) and 200 (student) and the VTP domain name on DLS1. Refer to Lab 6-1 for assistance if necessary.

```
ALS1# show vtp status
VTP Version                     : running VTP2
Configuration Revision          : 4
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Client
VTP Domain Name                 : SWPOD
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x18 0x59 0xE2 0xE0 0x28 0xF3 0xE7 0xD1
Configuration last modified by 172.16.1.3 at 3-12-93 19:46:16
```

Will VLAN information be stored in NVRAM when this device is rebooted? Explain.

_____

b. Issue the **show vlan** command on DLS1. The student and staff VLANs should be listed in the output of this command.

```
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 of these VLANs are present by default?

_____

c. Issue the **show interfaces trunk** command on each switch. If trunking was configured properly in Labs 6-1 and 6-2, Fast Ethernet 0/7–0/12 should be in trunking mode on all switches.

```
DLS1# show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/7       on           802.1q         trunking      1
Fa0/8       on           802.1q         trunking      1
Fa0/9       on           802.1q         trunking      1
Fa0/10      on           802.1q         trunking      1
Fa0/11      on           802.1q         trunking      1
Fa0/12      on           802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/7       1-4094
Fa0/8       1-4094
Fa0/9       1-4094
Fa0/10      1-4094
Fa0/11      1-4094
Fa0/12      1-4094

Port        Vlans allowed and active in management domain
Fa0/7       1,100,200
Fa0/8       1,100,200
Fa0/9       1,100,200
Fa0/10      1,100,200
Fa0/11      1,100,200

Port        Vlans allowed and active in management domain
Fa0/12      1,100,200

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/7       1,100,200
Fa0/8       1,100,200
```

```
Fa0/9       1,100,200
Fa0/10      1,100,200
Fa0/11      1,100,200
Fa0/12      1,100,200
```

What is the native VLAN for these trunk ports?

_____

Note: You can change the native VLAN to something other than VLAN 1 on trunk ports using the **switchport trunk native vlan** *vlan-id* command in interface configuration mode. Changing the native VLAN for trunk ports to an unused VLAN can help prevent VLAN hopping attacks. The unused VLAN (for example, VLAN 999) must exist on each switch and be specified on the trunked switch ports.

d. Issue the **show standby brief** command on DLS2.

```
DLS2# show standby brief

Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl1         1   100  P Standby  172.16.1.3      local           172.16.1.1
Vl100       1   100  P Standby  172.16.100.3    local           172.16.100.1
Vl200       1   150  P Active   local           172.16.200.3    172.16.200.1
```

For which VLANs is DLS2 the active router?

_____

What is the priority of the current root bridge for VLAN 200?

_____

Step 2: Configure private VLANs.

Within the server farm VLAN, all servers should be allowed access to the router or gateway but not be able to listen to each other's broadcast traffic. Private VLANs solve this problem. When you use a private VLAN, the primary VLAN (normal VLAN) can be logically associated with unidirectional, or secondary, VLANs. Servers or hosts in the secondary VLANs can communicate with the primary VLAN but not with another secondary VLAN. You can define the secondary VLANs as either isolated or community.

Stations attached to a port in a secondary VLAN can communicate with trunk ports and promiscuous ports associated with the appropriate primary VLAN. A host on an isolated secondary VLAN can communicate with the primary VLAN (for example, the default gateway SVI), but not hosts in any other secondary VLAN. In addition, the host associated with the isolated port cannot communicate with any other device on the same isolated secondary VLAN. It is essentially isolated from everything except the primary VLAN.

Hosts on ports in a community VLAN cannot communicate with hosts in other secondary VLANs. However, hosts on ports in this type of private VLAN can communicate with hosts on other ports within the community. This lets you have workgroups within an organization while keeping them isolated from each other.

a. The first step is to configure the switches for the primary VLAN. Based on the topology diagram, VLAN 150 will be used for the new server farm. On VTP server DLS1, add VLAN 150, name the VLAN **server-farm** and exit vlan config mode.

```
DLS1(config)# vlan 150
DLS1(config-vlan)# name server-farm
```



```
DLS1(config-vlan)# exit
```

b. Add HSRP information for the new VLAN on DLS1 and DLS2. Make DLS2 the primary router, and make DLS1 the standby router.

```
DLS1(config)# interface vlan 150
DLS1(config-if)# ip address 172.16.150.3 255.255.255.0
DLS1(config-if)# standby 1 ip 172.16.150.1
DLS1(config-if)# standby 1 priority 100
DLS1(config-if)# standby 1 preempt

DLS2(config)# interface vlan 150
DLS2(config-if)# ip add 172.16.150.4 255.255.255.0
DLS2(config-if)# standby 1 ip 172.16.150.1
DLS2(config-if)# standby 1 priority 150
DLS2(config-if)# standby 1 preempt
```

c. Verify the HSRP configuration for VLAN 150 using the **show standby vlan 150 brief** command on DLS2.

```
DLS2# show standby vlan 150 brief

                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl150       1   150  P Active   local           172.16.150.3    172.16.150.1
```

The command output shows that DLS2 is the active router for VLAN 150.

d. Set up the primary and secondary private VLAN (PVLAN) information on DLS1 and DLS2. Configure both switches in transparent mode for VTP using the **vtp mode transparent** global configuration command.

Note: To define PVLANs on DLS1 and DLS2, it is necessary for the switch VTP mode to be set to transparent.

```
DLS1(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.

DLS2(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
```

e. Configure DLS1 and DLS2 to contain the new PVLANs. Secondary PVLAN 151 is an isolated VLAN used for Fast Ethernet port 0/6, while secondary PVLAN 152 is used as a community PVLAN for Fast Ethernet ports 0/18–0/20. Configure these new PVLANs in global configuration mode. You also need to associate these secondary VLANs with primary VLAN 150.

```
DLS1(config)# vlan 151
DLS1(config-vlan)# private-vlan isolated
DLS1(config-vlan)# exit
DLS1(config)# vlan 152
DLS1(config-vlan)# private-vlan community
DLS1(config-vlan)# exit
DLS1(config)# vlan 150
DLS1(config-vlan)# private-vlan primary
DLS1(config-vlan)# private-vlan association 151,152

DLS2(config)# vlan 151
DLS2(config-vlan)# private-vlan isolated
DLS2(config-vlan)# exit
DLS2(config)# vlan 152
DLS2(config-vlan)# private-vlan community
```

```
DLS2(config-vlan)# exit
DLS2(config)# vlan 150
DLS2(config-vlan)# private-vlan primary
DLS2(config-vlan)# private-vlan association 151,152
```

f. The **private-vlan mapping** interface configuration command permits PVLAN traffic to be switched through Layer 3. Configure this command for interface VLAN 150 on DLS1 and DLS2.

```
DLS1(config)# interface vlan 150
DLS1(config-if)# private-vlan mapping 151-152
DLS1(config-if)# end

DLS2(config)# interface vlan 150
DLS2(config-if)# private-vlan mapping 151-152
DLS2(config-if)# end
```

g. Verify the creation of the secondary PVLANs and their association with the primary VLAN using the **show vlan private-vlan** command. Note that no ports are currently associated with these VLANs. This is expected behavior.

```
DLS2# show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ----------------------------------------
150     151       isolated
150     152       community
```

Will hosts assigned to ports on private VLAN 151 be able to communicate directly with each other?

_____

h. On DLS2, configure the Fast Ethernet ports that are associated with the server farm private VLANs. Fast Ethernet port 0/6 is used for the secondary isolated PVLAN 151, and ports 0/18–0/20 are used for the secondary community VLAN 152. The **switchport mode private-vlan host** command sets the mode on the interface and the **switchport private-vlan host-association** *primary-vlan-id secondary-vlan-id* command assigns the appropriate VLANs to the interface. The following commands configure the PVLANs on DLS2.

```
DLS2(config)# interface fastethernet 0/6
DLS2(config-if)# switchport mode private-vlan host
DLS2(config-if)# switchport private-vlan host-association 150 151
DLS2(config-if)# exit
DLS2(config)# interface range fa0/18 - 20
DLS2(config-if-range)# switchport mode private-vlan host
DLS2(config-if-range)# switchport private-vlan host-association 150 152
```

As servers are added to Fast Ethernet 0/18–20, will these servers be allowed to hear broadcasts from each other? Explain.

_____

_____

i. Use the **show vlan private-vlan** command and note that the ports configured are currently associated with these VLANs.

```
DLS2# show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ---------------------------------------
150     151       isolated          Fa0/6
150     152       community         Fa0/18, Fa0/19, Fa0/20
```

j. Configure host PC-A on DLS2 port Fa0/6 with an IP address in VLAN 150 (for example: 172.16.150.6/24). Use the VLAN 150 HSRP address (172.16.150.1) as the default gateway. This PC represents a server in isolated PVLAN 151.

k. (optional) If you have two additional PCs, attach one to DLS2 port Fa0/18 and the other to port Fa0/19 in the community PVLAN 152. Configure each host with an IP address in VLAN 150 (for example: 172.16.150.18/24 and 172.16.150.19/24). Use the VLAN 150 HSRP address (172.16.150.1) as the default gateway.

l. From PC-A in isolated PVLAN 151 on DLS2 ping the primary VLAN 150 default gateway HSRP virtual IP address 172.16.150.1 and other IP addresses in the network, including PC-B if connected to DLS2 port Fa0/18 in PVLAN 152. Which pings should succeed and which should fail?

_____

_____

_____

_____

_____

Step 3: Configure RACLs between VLANs.

Configure router access control lists (RACLs) to separate the student and staff VLANs. The staff VLAN (100) can access the student VLAN (200), but the student VLAN does not have access to the staff VLAN for security purposes.

a. To deny the student subnet, use an extended IP access list on DLS1 and DLS2, and assign the access list to the appropriate VLAN interfaces using the **ip access-group** *acl-num* {**in** | **out**} command.

```
DLS1(config)# access-list 100 permit tcp 172.16.200.0 0.0.0.255 172.16.100.0
0.0.0.255 established
DLS1(config)# access-list 100 permit icmp 172.16.200.0 0.0.0.255 172.16.100.0
0.0.0.255 echo-reply
DLS1(config)# access-list 100 deny ip 172.16.200.0 0.0.0.255 172.16.100.0
0.0.0.255
DLS1(config)# access-list 100 permit ip any any
DLS1(config)# interface vlan 100
DLS1(config-if)# ip access-group 100 in
DLS1(config)# interface vlan 200
DLS1(config-if)# ip access-group 100 in

DLS2(config)# access-list 100 permit tcp 172.16.200.0 0.0.0.255 172.16.100.0
0.0.0.255 established
DLS2(config)# access-list 100 permit icmp 172.16.200.0 0.0.0.255 172.16.100.0
0.0.0.255 echo-reply
DLS(config)# access-list 100 deny ip 172.16.200.0 0.0.0.255 172.16.100.0
0.0.0.255
```



```
DLS2(config)# access-list 100 permit ip any any
DLS2(config)# interface vlan 100
DLS2(config-if)# ip access-group 100 in
DLS2(config)# interface vlan 200
DLS2(config-if)# ip access-group 100 in
```

b. Check the configuration using the **show ip access-list** and **show ip interface vlan** *vlan-id* commands.

```
DLS1# show access-lists
Extended IP access list 100
    10 permit tcp 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255 established
    20 permit icmp 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255 echo-reply
    30 deny ip 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255
    40 permit ip any any

DLS1# show ip interface vlan 100
Vlan100 is up, line protocol is up
  Internet address is 172.16.100.3/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.2
  Outgoing access list is not set
  Inbound  access list is 100
  <output omitted>
```

c. After the access list has been applied verify the configuration in one of the following ways. Option 1 using real hosts is preferred.

Option 1: Connect host PC-A to ALS1 port Fa0/15 in staff VLAN 100 and assign it IP address 172.16.100.15/24 with default gateway 172.16.100.1. Connect host PC-B to ALS2 port Fa0/15 in student VLAN 200 and assign it IP address 172.16.200.15/24 with default gateway 172.16.200.1. Ping the staff host from the student host. This ping should fail. Then ping the student host from the staff host. This ping should succeed.

Option 2: On ALS1 set up a simulated host in VLAN 100 and one in VLAN 200 by creating a VLAN 100 and 200 interface on the switch. Give the VLAN 100 interface an IP address in VLAN 100. Give the VLAN 200 interface an IP address in VLAN 200. The following is a sample configuration on ALS1.

```
ALS1(config)# int vlan 100
ALS1(config-if)# ip address 172.16.100.100 255.255.255.0

ALS1(config)# int vlan 200
ALS1(config-if)# ip address 172.16.200.200 255.255.255.0
```

d. Ping the interface of the gateway for the staff VLAN (172.16.100.1) with a source of staff VLAN 100 (172.16.100.100) and then ping with a source of student VLAN 200. The pings from the student VLAN should fail.

```
ALS1# ping 172.16.100.1 source vl100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.100.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.100.100
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/205/1007 ms

ALS1# ping 172.16.100.1 source vl200
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.100.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.200.200
.U.U.
Success rate is 0 percent (0/5)
```

What does a U signify in the output of the **ping** command?

_____

_____

_____

_____

Step 4: Configure VACLs.

Configure the network so that the temporary staff host cannot access the rest of the staff VLAN, yet still be able to use the default gateway of the staff subnet to connect to the rest of the network and the ISP. You can accomplish this task by using a VLAN ACL (VACL).

Because the temporary staff PC is located on DLS1 Fast Ethernet 0/3, the VACL must be placed on DLS1.

a. Configure an access list on DLS1 called temp-host using the **ip access-list extended** *name* command. This list defines the traffic between the host and the rest of the network. Then define the traffic using the **permit ip host** *ip-address subnet wildcard-mask* command.

```
DLS1(config)# ip access-list extended temp-host
DLS1(config-ext-nacl)# permit ip host 172.16.100.150 172.16.100.0 0.0.0.255
```

b. The VACL is defined using a VLAN access map. Access maps are evaluated in a numbered sequence. To set up an access map, use the **vlan access-map** *map-name seq#* command. The following configuration defines an access map named block-temp, which uses the **match** statement to match the traffic defined in the access list and denies that traffic. You also need to add a line to the access map that allows all other traffic. If this line is not added, an implicit deny catches all other traffic and denies it.

```
DLS1(config)# vlan access-map block-temp 10
DLS1(config-access-map)# match ip address temp-host
DLS1(config-access-map)# action drop
DLS1(config-access-map)# vlan access-map block-temp 20
DLS1(config-access-map)# action forward
DLS1(config-access-map)# exit
```

c. Define which VLANs the access map should be applied to using the **vlan filter** *map-name* **vlan-list** *vlan-ID* command.

```
DLS1(config)# vlan filter block-temp vlan-list 100
```

d. Verify the VACL configuration using the **show vlan access-map** command on DLS1.

```
DLS1# show vlan access-map
Vlan access-map "block-temp"  10
  Match clauses:
    ip  address: temp-host
  Action:
    drop
Vlan access-map "block-temp"  20
  Match clauses:
  Action:
    forward
```

e. (Optional) If possible, connect a PC to the Fast Ethernet 0/3 port of DLS1 and assign the host an IP address of 172.16.100.150/24. Configure the Fast Ethernet 0/3 port as an access port in VLAN 100. Try to ping to another staff host. The ping should not be successful.