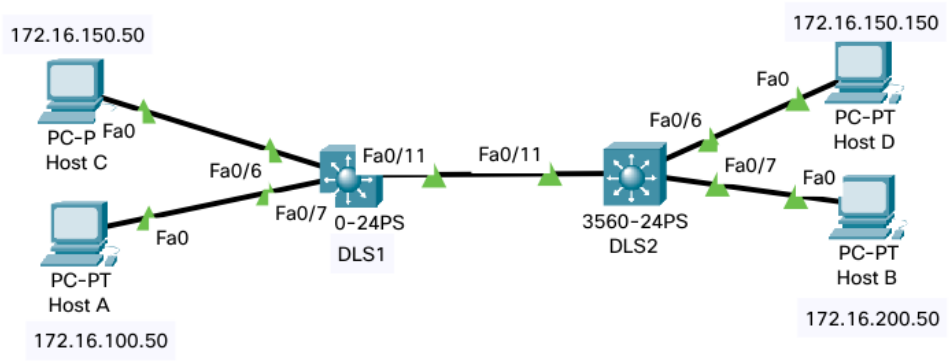
Securing VLANs

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

VLAN	Purpose
150	Server-farm
151	Isolated
152	Community



Introduction

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 (Host C) by using private VLANs. 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.

Required Resources

- 2 switches (Cisco 3560)
- 4 PCs
- Ethernet and console cables

Prepare the switches for the lab

Reset both switches if needed:

erase startup-config

delete vlan.dat

reload

Copy and paste the configuration in Appendix A on both switches.

Part 1: Configure private VLANs.

Private VLANs are an option when you have multiple devices in the same broadcast domain, but need to prevent them from communicating from each other. A good example is in a server farm where the servers do not need to receive other server's broadcast traffic.

In a sense, private VLANs allow you to sub-divide the layer 2 broadcast domain. You are able to associate a primary VLAN with multiple secondary VLANs, while using the same IP address space for all of the devices.

Secondary VLANs are defined as one of two types; either COMMUNITY or ISOLATED. A secondary community VLAN allows the hosts within the VLAN to communicate with one another and the primary VLAN. A secondary isolated VLAN does not allow hosts to communicate with others in the same isolated VLAN. They can only communicate with the primary VLAN.

A primary VLAN can have multiple secondary community VLANs associated with it, but only one secondary isolated VLAN.

Step 1: Configure the Primary Private VLAN

a. Based on the topology diagram, VLAN 150 will be used as the VLAN for the new server farm. On all switches, add VLAN 150, and name the VLAN **server-farm**. In addition, configure DLS1 as the root bridge for VLANs 150, 151, and 152.

```
DLS1(config)# vtp mode transparent
DLS1(config)# vlan 150
DLS1(config-vlan)# name SERVER-FARM
DLS1(config-vlan)# exit
DLS1(config)# spanning-tree vlan 150-152 root primary
```

b. Once this is complete, verify that VLAN 150 is preset in the database of both switch.

Step 2: Configure interface VLAN 150 at DLS1 and DLS2:

```
DLS1(config)# interface vlan 150
DLS1(config-if)# ip address 172.16.150.1 255.255.255.0

DLS2(config)# interface vlan 150
DLS2(config-if)# ip add 172.16.150.2 255.255.255.0
```

Step 3: Create the PVLANs

a. Configure the new PVLANs on both switches. Secondary PVLAN 151 is an isolated VLAN, while secondary PVLAN 152 is used as a community PVLAN. Configure these new PVLANs and associate them 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
DLS1(config-vlan)# exit
```

b. Verify the PVLANs on the switches.

```
DLS2# show vlan brief  | include active
```

c. 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.

```
DLS1#show vlan private-vlan
```

Step 4: Configure support for routing of PVLANs

The **private-vlan mapping** interface configuration command permits PVLAN traffic to be switched through Layer 3. Normally you would include all the secondary VLANs to allow for HSRP to work, but for this example we will not include a mapping VLAN 151 on DLS2 so we can demonstrate the isolation of VLAN 151. Configure these commands 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 152
DLS2(config-if)# end
```

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

_____

Step 5: Configure host access to PVLANs

a. On DLS1, configure interface FastEthernet 0/6 so it is in private-vlan host mode and has association to VLAN 150:

```
DLS1(config)# interface fastethernet 0/6
DLS1(config-if)# switchport mode private-vlan host
DLS1(config-if)# switchport private-vlan host-association 150 152
DLS1(config-if)# exit
```

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

```
DLS1#show vlan private-vlan
```

c. 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.

_____

_____

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

```
DLS2# show vlan private-vlan
```

e. Configure HOST C on DLS1 interface f0/6 with the IP address 172.16.150.50/24. Use 172.16.150.1 as the default gateway address.

f. Configure HOST D on DLS2 interface f0/6 with the IP address 172.16.150.150/24. Use 172.16.150.1 as the default gateway address.

Step 6: Verify PVLANs are working

a. From HOST C, try to ping 172.16.150.1 (DLS1), 172.16.150.2 (DLS2).

b. From HOST C, try to ping HOST D (172.16.150.150).

c. From HOST D, try to ping 172.16.150.1 (DLS1).

d. From HOST D, try to ping 172.16.150.2 (DLS2).

Part 3: RACLs.

You can use router access control lists (RACLs) to separate the student and staff VLANs. In this lab scenario, write an ACL that allows the staff VLAN (100) to access the student VLAN (200), and deny student VLAN access to the staff VLAN.

Step 1: Write an extended IP access list

Write an ACL that meets the requirement and assign the access list to the appropriate VLAN interfaces on DLS1 and DLS2 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 200
DLS1(config-if)# ip access-group 100 in
DLS1(config-if)# exit

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
DLS2(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 200
DLS2(config-if)# ip access-group 100 in
DLS2(config-if)# exit
```

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

```
DLS1# show access-lists

DLS1# show ip interface vlan 200
```

f. Configure Port F0/7 on both switches and set IP addresses of both Hosts A and B. noting that host A is a member of VLAN 100 and host B is a member of VLAN 200.

g. After the access list has been applied verify the configuration by pinging host B from host A.

Appendix A: start configuration of both switches

DLS1:

```
hostname DLS1
enable secret pass
ip routing
no ip domain-lookup
ip domain-name SEC.LAB
vlan 99
name Management
vlan 100
name STAFF
vlan 200
name STUDENTS
vlan 666
name NATIVE_DO_NOT_USE
exit
spanning-tree mode pvst
spanning-tree vlan 99-100 priority 24576
spanning-tree vlan 200 priority 28672
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 666
 switchport mode trunk
 switchport nonegotiate
interface Vlan1
 ip address 172.16.1.3 255.255.255.0
 standby 1 preempt
 standby 1 ip 172.16.1.1
 standby 1 priority 150
interface Vlan99
 ip address 172.16.99.3 255.255.255.0
 standby 99 preempt
 standby 99 ip 172.16.99.1
 standby 99 priority 150
interface Vlan100
 ip address 172.16.100.3 255.255.255.0
 standby 100 ip 172.16.100.1
 standby 100 priority 150
 standby 100 preempt
interface Vlan200
 ip address 172.16.200.3 255.255.255.0
 standby 200 ip 172.16.200.1
 standby 200 preempt
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 15
 password pass
 login
end
```

DLS2:

```
hostname DLS2
enable secret pass
ip routing
no ip domain-lookup
ip domain-name SEC.LAB
vlan 99
name Management
vlan 100
name STAFF
vlan 200
name STUDENTS
vlan 666
name NATIVE_DO_NOT_USE
exit
spanning-tree mode pvst
spanning-tree vlan 99-100 priority 28672
spanning-tree vlan 200 priority 24576
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 666
 switchport mode trunk
 switchport nonegotiate
interface Vlan1
 ip address 172.16.1.4 255.255.255.0
 standby 1 preempt
 standby 1 ip 172.16.1.1
interface Vlan99
 ip address 172.16.99.4 255.255.255.0
 standby 99 preempt
 standby 99 ip 172.16.99.1
interface Vlan100
 ip address 172.16.100.4 255.255.255.0
 standby 100 ip 172.16.100.1
 standby 100 preempt
interface Vlan200
 ip address 172.16.200.4 255.255.255.0
 standby 200 ip 172.16.200.1
 standby 200 priority 150
 standby 200 preempt
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 15
 password pass
 login
end
```