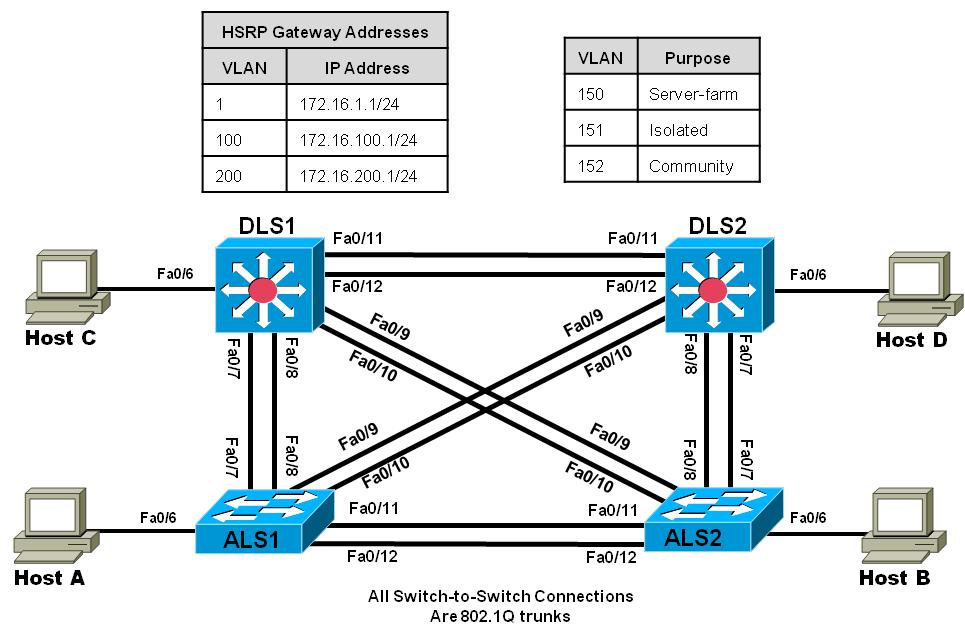
CCNPv7.1 SWITCH

Chapter 10 Lab 10-2, Securing VLANs

Topology



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 (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.

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 Catalyst 3560 and 2960 switches running Cisco IOS 15.0(2) IP Services and LAN Base images, respectively. The 3560 and 2960 switches are configured with the SDM templates “dual-ipv4-and-ipv6 routing” and “lanbase-routing”, respectively. 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. Catalyst 3650 switches (running any Cisco IOS XE release) and Catalyst 2960-Plus switches (running any supported Cisco IOS image) can be used in place of the Catalyst 3560 switches and the Catalyst 2960 switches.

Required Resources

* 2 switches (Cisco 2960 with the Cisco IOS Release 15.0(2)SE6 C2960-LANBASEK9-M image or comparable)
* 2 switches (Cisco 3560 with the Cisco IOS Release 15.0(2)SE6 C3560-ipservicesK9-M image or comparable)
* 4 PCs
* Ethernet and console cables

### Prepare the switches for the lab

The instructions in this lab assume that the switches are running using the final configuration from Lab 10-1 "Securing Layer 2 Switches".

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.

* 1. Configure VTP

VTP version 2 does not support PVLANs, so any switches that must host a PVLAN port have to be in transparent mode and the PVLANs have to be manually configured. VTP version 3 does support PVLANs, so the configuration only has to be done in one place.

* + 1. Convert all switches to VTP version 3, and configure a VTP password of cisco123. Configure all four switches. An example of DLS1 configuration follows:

DLS1(config)# **vtp version 3**

Aug 4 12:39:11.944: %SW\_VLAN-6-OLD\_CONFIG\_FILE\_READ: Old version 2 VLAN configuration file detected and read OK. Version 3

files will be written in the future.

DLS1(config)# **vtp password cisco123**

Setting device VTP password to cisco123

DLS1(config)# **exit**

* + 1. Configure DLS1 to be the primary switch for VLANs.

DLS1# **vtp primary vlan**

This system is becoming primary server for feature vlan

No conflicting VTP3 devices found.

Do you want to continue? [confirm]

DLS1#

Aug 4 12:40:44.680: %SW\_VLAN-4-VTP\_PRIMARY\_SERVER\_CHG: e840.406f.7280 has become the primary server for the VLAN VTP feature

DLS1#

* 1. Configure the Primary Private VLAN

1. Based on the topology diagram, VLAN 150 will be used as the VLAN for the new server farm. On VTP server DLS1, add VLAN 150, name the VLAN **server-farm** and exit vlan config mode. This allows VLAN 150 to be propagated to the other switches in the network. In addition, configure DLS1 as the root bridge for VLANs 150, 151, and 152.

DLS1(config)# **vlan 150**

DLS1(config-vlan)# **name SERVER-FARM**

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

DLS1(config)# **spanning-tree vlan 150-152 root primary**

* + 1. Once this is complete, verify that VLAN 150 is preset in the database on DLS2.
  1. 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**

* 1. Create the PVLANs on the VTP server

1. Configure the new PVLANs on DLS1. 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**

DLS1(config)#

1. Verify the PVLANs propagate to the other switches.

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

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

99 Management active

100 STAFF active

150 SERVER-FARM active

151 VLAN0151 active

152 VLAN0152 active

200 STUDENTS active

666 NATIVE\_DO\_NOT\_USE active

1. 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.

DLS1#**show vlan private-vlan**

Primary Secondary Type Ports

------- --------- ----------------- ------------------------------------------

150 151 isolated

150 152 community

DLS2# **show vlan private-vlan**

Primary Secondary Type Ports

------- --------- ----------------- -----------------------------------------

150 151 isolated

150 152 community

* 1. 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?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Configure host access to PVLANs

1. 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**

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

DLS1#**show vlan private-vlan**

Primary Secondary Type Ports

------- --------- ----------------- ------------------------------------------

150 151 isolated

150 152 community Fa0/6

1. 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.

1. 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

1. 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.
2. 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.
   1. Verify PVLANs are working
3. From HOST C, try to ping the following addresses - they should all work: 172.16.150.1 (DLS1), 172.16.150.2 (DLS2), 172.16.99.5 (ALS1).
4. From HOST C, try to ping HOST D (172.16.150.150). This should NOT work.
5. From HOST D, try to ping the following addresses - they should all work: 172.16.150.1 (DLS1), 172.16.99.5 (ALS1).
6. From HOST D, try to ping 172.16.150.2 (DLS2). This should NOT work.
7. 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.

* 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**

1. 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>

1. 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**:

Lab 10-1 finished with ALS1 F0/6 assigned to VLAN 200. Change this assignment to VLAN 100. Host A should be connected to ALS1 F0/6 and assigned the IP address 172.16.100.50/24 with default gateway 172.16.100.1 from Lab 10-1. If not, set Host A up with those parameters.

Host B should be connected to ALS2 F0/6 from Lab 10-1 as well, but its last configuration in that lab was to use DHCP, so assign a static IP address  Connect host PC-B to ALS2 port Fa0/6 in student VLAN 200 and assign it IP address 172.16.200.50/24 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**

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?

1. 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).

For this scenario, Host C (DLS1 Fast Ethernet 0/6) will act as a temporary staff PC, therefore the VACL must be placed on DLS1.

* 1. Configure DLS1 F0/6 and Host C

1. Change the configuration of DLS1 F0/6 so that the interface is associated with VLAN 100. To keep things tidy, also remove the private vlan mapping on the interface as well:

DLS1(config)#**interface f0/6**

DLS1(config-if)#**switchport mode access**

DLS1(config-if)#**switchport access vlan 100**

DLS1(config-if)#**no switchport private-vlan host-association 150 152**

DLS1(config-if)#**exit**

1. Change the configuration of HOST C so that it is using the IP address 172.16.100.150/24 with the default gateway set as 172.16.100.1
   1. Configure and apply the VACL
2. 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. Note that you must be explicit about what traffic to match -- this isn't a traffic *filtering* ACL, it is a traffic *matching* ACL. If you were to leave the second line of the example below out, pings would work.

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**

DLS1(config-ext-nacl)# **permit icmp host 172.16.100.150 172.16.100.0 0.0.0.255**

DLS1(config-ext-nacl)# **exit**

1. 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**

1. 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**

1. 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

* 1. Test the VACL

1. From HOST C, try to ping to HOST A on ALS1 (172.16.100.50). The ping should fail.
2. From HOST C, try to ping the default gateway (172.16.100.1). The ping should fail.
3. From HOST C, try to ping Host D (172.16.200.50). The ping should succeed.
   1. End of Lab

Do not save your configurations. The equipment will be reset for the next lab.