Arago, Amienz

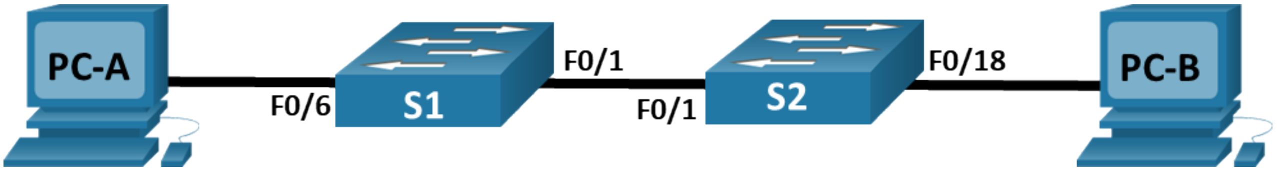
Bolima, Dave

Go, Aldrich

Lim, Shaun

Lab 3.1 - Configure VLANs and Trunking

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Create VLANs and Assign Switch Ports

Part 3: Maintain VLAN Port Assignments and the VLAN Database

Part 4: Configure an 802.1Q Trunk between the Switches

Part 5: Delete the VLAN Database

Background / Scenario

Modern switches use virtual local-area networks (VLANs) to improve network performance by separating large Layer 2 broadcast domains into smaller ones. VLANs can also be used as a security measure by controlling which hosts can communicate. In general, VLANs make it easier to design a network to support the goals of an organization.

VLAN trunks are used to span VLANs across multiple devices. Trunks allow the traffic from multiple VLANS to travel over a single link, while keeping the VLAN identification and segmentation intact.

In this lab, you will create VLANs on both switches in the topology, assign VLANs to switch access ports, verify that VLANs are working as expected, and then create a VLAN trunk between the two switches to allow hosts in the same VLAN to communicate through the trunk, regardless of which switch the host is actually attached to.

Required Resources

- 2 Switches (Cisco 2960)
- 2 PCs
- Ethernet cables as shown in the topology

Instructions

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and switches.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each switch.

a. Console into the switch and enable privileged EXEC mode.

b. Enter configuration mode.

c. Assign a device name to the switch.

d. Disable DNS lookup to prevent the switches from attempting to translate incorrectly entered commands as though they were host names.

e. Assign **class** as the privileged EXEC encrypted password.

f. Assign **cisco** as the console password and enable login.

g. Assign **cisco** as the vty password and enable login.

h. Encrypt the plaintext passwords.

i. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

j. Configure the IP address listed in the Addressing Table for VLAN 1 on the switch.

k. Save the running configuration to the startup configuration file.

Step 3: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Step 4: Test connectivity.

Verify that the PC hosts can ping one another.

Note: It may be necessary to disable the PCs firewall to ping between PCs.

Can PC-A ping PC-B?	Yes
Can PC-A ping S1?	No
Can PC-B ping S2?	No
Can S1 ping S2?	Yes

If you answered no to any of the above questions, why were the pings unsuccessful?

As there is no router, these are in different networks and thus PCs pinging Switches are unsuccessful. For the pings to work, there has to be a default gateway t route traffic from one subnet to another

Part 2: Create VLANs and Assign Switch Ports

In Part 2, you will create Management, Operations, Parking_Lot, and Native VLANs on both switches. You will then assign the VLANs to the appropriate interface. The **show vlan** command is used to verify your configuration settings.

Step 1: Create VLANs on the switches.

a. Create the VLANs on S1.

```
S1(config)# vlan 10
S1(config-vlan)# name Operations
S1(config-vlan)# vlan 20
S1(config-vlan)# name Parking_Lot
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# vlan 1000
S1(config-vlan)# name Native
S1(config-vlan)# end
```

b. Create the same VLANs on S2.

c. Issue the **show vlan brief** command to view the list of VLANs on S1.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                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
10   Operations                       active
20   Parking_Lot                      active
99   Management                       active
1000 Native                           active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

What is the default VLAN?	VLAN 1

What ports are assigned to the default VLAN?	All ports are assigned to VLAN 1

Step 2: Assign VLANs to the correct switch interfaces.

a. Assign VLANs to the interfaces on S1.

1) Assign PC-A to the Operation VLAN.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

2) Move the switch IP address VLAN 99.

```
S1(config)# interface vlan 1
S1(config-if)# no ip address
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# end
```

b. Issue the **show vlan brief** command and verify that the VLANs are assigned to the correct interfaces.

c. Issue the **show ip interface brief** command.

What is the status of VLAN 99? Explain.

Up because the vlan exists in the database but down because it has not been assigned an active port yet

d. Assign PC-B to the Operations VLAN on S2.

e. Remove the IP address for VLAN 1 on S2.

f. Configure an IP address for VLAN 99 on S2 according to the Addressing Table.

g. Use the **show vlan brief** command to verify that the VLANs are assigned to the correct interfaces.

Is S1 able to ping S2? Why or why not?

Not able to because the IP addresses for the switches resides in VLAN 99 which is not connected to any port

Is PC-A able to ping PC-B? Why or why not?

No. because the interface isn’t assigned to VLAN 10.

Part 3: Maintain VLAN Port Assignments and the VLAN Database

In Part 3, you will change VLAN assignments to ports and remove VLANs from the VLAN database.

Step 2: Assign a VLAN to multiple interfaces.

a. On S1, assign interfaces F0/11 – 24 to VLAN99.

```
S1(config)# interface range f0/11-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 99
S1(config-if-range)# end
```

b. Issue the **show vlan brief** command to verify VLAN assignments.

c. Reassign F0/11 and F0/21 to VLAN 10.

d. Verify that VLAN assignments are correct.

Step 3: Remove a VLAN assignment from an interface.

a. Use the **no switchport access vlan** command to remove the VLAN 99 assignment to F0/24.

```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```

b. Verify that the VLAN change was made.

Which VLAN is F0/24 now associated with?

It is now associated with vlan 1, default vlan

Step 4: Remove a VLAN ID from the VLAN database.

a. Add VLAN 30 to interface F0/24 without issuing the global VLAN command.

```
S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

Note: Current switch technology no longer requires that the **vlan** command be issued to add a VLAN to the database. By assigning an unknown VLAN to a port, the VLAN will be created and added to the VLAN database.

b. Verify that the new VLAN is displayed in the VLAN table.

What is the default name of VLAN 30?

VLAN0030

c. Use the **no vlan 30** command to remove VLAN 30 from the VLAN database.

```
S1(config)# no vlan 30
S1(config)# end
```

d. Issue the **show vlan brief** command. F0/24 was assigned to VLAN 30.

After deleting VLAN 30 from the VLAN database, what VLAN is port F0/24 assigned to? What happens to the traffic destined to the host attached to F0/24?

When you delete a vlan, any ports assigned to it becomes inactive. In this case, port f0/24 is still associated with vlan 30 but is no longer shown in the output. It does not exist in the vlan database after being deleted thus making it inactive. Any port associated with vlan30 thusly will not transfer any traffic

e. Issue the **no switchport access vlan** command on interface F0/24.

f. Issue the **show vlan brief** command to determine the VLAN assignment for F0/24.

To which VLAN is F0/24 assigned?

It is assigned to the default vlan

Note: Before removing a VLAN from the database, it is recommended that you reassign all the ports assigned to that VLAN.

Why should you reassign a port to another VLAN before removing the VLAN from the VLAN database?

Because if the vlan is removed, an error occurs where the port is missing and this makes it difficult to troubleshoot since trunked interfaces don’t show up in the port list

Part 4: Configure an 802.1Q Trunk Between the Switches

In Part 4, you will configure interface F0/1 to use trunk mode so that traffic from multiple VLANs may be exchanged between S1 and S2 over a single physical connection.

Step 1: Configure trunking on F0/1.

The default DTP mode of a 2960 switch port is dynamic auto. This allows the interface to convert the link to a trunk if the neighboring interface is set to trunk or dynamic desirable mode.

a. Set F0/1 on S1 to trunk mode. You should receive link status messages on S1.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
Sep 19 02:51:47.257: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
Sep 19 02:51:47.291: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
```

b. Do the same for F0/1 on S2. You should also receive link status messages on S2.

```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
Sep 19 02:42:19.424: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Sep 19 02:42:21.454: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
Sep 19 02:42:22.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

c. Issue the **show vlan brief** command on S1 and S2. Interface F0/1 is no longer assigned to VLAN 1. Trunked interfaces are not listed in the VLAN table.

d. Issue the **show interfaces trunk** command to view trunked interfaces. Notice that the mode on S1 is set to desirable, and the mode on S2 is set to auto.

```
S1# show interfaces trunk


S2# show interfaces trunk
```

Note: By default, all VLANs are allowed on a trunk. The **switchport trunk** command allows you to control what VLANs have access to the trunk. For this lab, keep the default settings which allows all VLANs to traverse F0/1.

e. Verify that VLAN traffic is traveling over trunk interface F0/1.

Can PC-A ping PC-B?	Yes
Can PC-A ping S1?	Yes
Can PC-B ping S2?	No
Can S1 ping S2?	No

If you answered no to any of the above questions, explain below.

The switches are in vlan99 and the pcs in vlan10 and so, pings between the vlans were unsuccesful

f. Modify the trunk configuration on **both** switches by changing the native VLAN from VLAN 1 to VLAN 1000.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 1000
```

g. Issue the show interfaces trunk command to view the trunk. Notice the Native VLAN information is updated.

```
S2# show interfaces trunk
```

Why might you want to change the native VLAN on a trunk?

Using vlan 1 is a security risk. All different control protocols are exchanged between switches and this is done through the use of vlan1 untagged. This information could be exposed if default settings are used on ports that users connect to

Part 5: Delete the VLAN Database

In Part 5, you will delete the VLAN Database from the switch. It is necessary to do this when initializing a switch back to its default settings.

Step 1: Determine if the VLAN database exists.

Issue the **show flash** command to determine if a **vlan.dat** file exists in flash.

```
S1# show flash:
```

Note: If there is a **vlan.dat** file located in flash, then the VLAN database does not contain its default settings.

Step 2: Delete the VLAN database.

a. Issue the **delete vlan.dat** command to delete the vlan.dat file from flash and reset the VLAN database back to its default settings. You will be prompted twice to confirm that you want to delete the vlan.dat file. Press Enter both times.

```
S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
```

b. Issue the **show flash** command to verify that the vlan.dat file has been deleted.

```
S1# show flash:
```

To initialize a switch back to its default settings, what other commands are needed?

You need to run erase startup-config and reload commands need to be issued after running “delete vlan.dat”

Reflection Questions

1. What is needed to allow hosts on VLAN 10 to communicate to hosts on VLAN 99?

A layer 3 device, this being a router because vlan10 and vlan99 are on different networks thus necessitating the use of a router to get them to communicate.

2. Why would it be recommended to allocate a separate VLAN for the management interfaces of network devices?

For security, so regular users in the network don’t need to access the management, This VLAN can be used as a separate network for management purposes

3. What are some primary benefits that an organization can receive through effective use of VLANs?

For better security, costs saving., decreased broadcast domain size, better performance, broadcast storm mitigation, easier management (project-wise and application-wise) thus leading to higher IT staff efficiency.