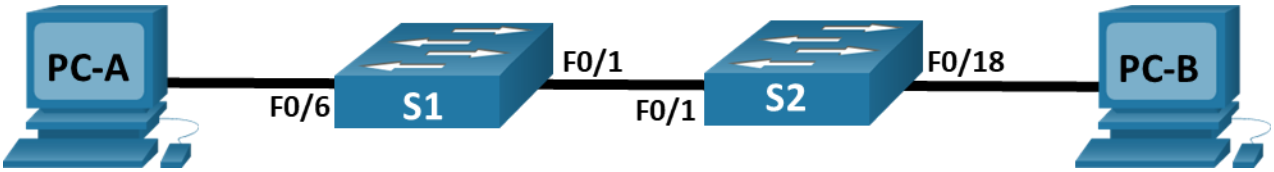
Baraocor, Jalanie
Flores, Leann Christian
Mosqueda, Christine Reisa
Tilan, Sherri Nicole
Viernes, Jhon Lloyd
Fuentes, Christian
Tabacoan, Harold Adrian
Villalobos, James
Calma, Leonar

Lab - Implement VLANs and Trunking

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 10	192.168.10.11	255.255.255.0
	VLAN 20	192.168.20.11	255.255.255.0
	VLAN 30	192.168.30.11	255.255.255.0
S2	VLAN 10	192.168.10.12	255.255.255.0
PC-A	NIC	192.168.20.13	255.255.255.0
PC-B	NIC	192.168.30.13	255.255.255.0

VLAN Table

VLAN	Name	Interface Assigned
10	Management	S1: VLAN 10 S2: VLAN 10
20	Sales	S1: VLAN 20 and F0/6
30	Operations	S1: VLAN 30 S2: F0/18
999	ParkingLot	S1: F0/2-5, F0/7-24, G0/1-2 S2: F0/2-17, F0/19-24, G0/1-2
1000	Native	N/A

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Create VLANs and Assign Switch Ports

Part 3: Configure an 802.1Q Trunk between the Switches

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 address scalability, security, and network management. In general, VLANs make it easier to design a network to support the goals of an organization. Communication between VLANs requires a device operating at Layer 3 of the OSI model.

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 create VLAN trunks between the two switches.

Note: The switches used with CCNA hands-on labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Ensure that the switches have been erased and have no startup configurations. If you are unsure contact your instructor.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 2 PCs (Windows with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- 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.

- `enable`

b. Assign a device name to the switch.

- `hostname S1`
- `hostname S2`

c. Disable DNS lookup.

- `no ip domain-lookup`

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

- `enable secret class`

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

- `line con 0`

```
password cisco
login
```

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

- `line vty 0 4`

  `password cisco`

  `login`

g. Encrypt the plaintext passwords.

- `service password-encryption`

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

- `banner motd #`
  `Unauthorized access is prohibited. #`

i. Copy the running configuration to the startup configuration.

- `copy running-config startup-running config`

Step 3: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Part 2: Create VLANs and Assign Switch Ports

In Part 2, you will create VLANs as specified in the table above on both switches. You will then assign the VLANs to the appropriate interface. The **show vlan brief** command is used to verify your configuration settings. Complete the following tasks on each switch.

Step 1: Create VLANs on both switches.

a. Create and name the required VLANs on each switch from the table above.

- Vlan 10 - **Management**
- Vlan 20 - **Sales**
- Vlan 30 - **Operations**
- Vlan 999 - **ParkingLot**
- Vlan 1000 - **Native**

b. Configure the management interface on each switch using the IP address information in the Addressing Table.

- `s1(config)# int vlan 10`

  `s1(config-if)# ip address 192.168.10.11 255.255.255.0`

  - ***Switch 1***
    - *Vlan 10 -* ***192.168.10.11***
    - *Vlan 20 -* ***192.168.20.11***
    - *Vlan 30 -* ***192.168.30.11***
  - ***Switch 2***
    - *Vlan 10 -* ***192.168.10.12***

c. Assign all unused ports on the switch to the ParkingLot VLAN, configure them for static access mode, and administratively deactivate them.

- **s2(config)# interface range FastEthernet 0/2 - 17**

  s2(config-if-range)# switchport access mode

  s2(config-if-range)# switchport access vlan 999

  s2(config-if-range)# exit

  s2(config-if-range)# shutdown s2(config-if-range)# do write memory

```
s2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   Management                        active
30   Operations                        active    Fa0/18
999  ParkingLot                        active    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
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
1000 Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
s2#
```

Step 2: Assign VLANs to the correct switch interfaces.

a. Assign used ports to the appropriate VLAN (specified in the VLAN table above) and configure them for static access mode.

- **s2(config)# interface fastEthernet 0/18**

  s2(config-if)# switchport access mode

  s2(config-if)# switchport access vlan 30

  s2(config-if)# do write memory

b. Verify that the VLANs are assigned to the correct interfaces.

```
s2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   Management                        active
30   Operations                        active    Fa0/18
999  ParkingLot                        active    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
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
1000 Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
s2#
```

Part 3: Configure an 802.1Q Trunk Between the Switches

In Part 3, you will manually configure interface F0/1 as a trunk.

Step 1: Manually configure trunk interface F0/1.

a. Change the switchport mode on interface F0/1 to force trunking. Make sure to do this on both switches.

- **s2(config)# interface FastEthernet 0/1**
  s2(config-if)# switchport mode trunk

b. Set the native VLAN to 1000 on both switches.

- **s2(config-if)# switchport trunk native vlan 1000**

c. As another part of trunk configuration, specify that only VLANs 10, 20, 30, and 1000 are allowed to cross the trunk.

- **s2(config-if)# switchport trunk allowed vlan 10,20,30,1000**

d. Issue the **show interfaces trunk** command to verify trunking ports, the native VLAN and allowed VLANs across the trunk.

```
s2#show interfaces trun
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1000

Port        Vlans allowed on trunk
Fa0/1       10,20,30,1000

Port        Vlans allowed and active in management domain
Fa0/1       10,30,1000

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,30,1000

s2#
```

Step 2: Verify connectivity.

Verify connectivity within a VLAN. For example, PC-A should be able to ping S1 VLAN 20 successfully.

```
C:\>ping 192.168.20.11

Pinging 192.168.20.11 with 32 bytes of data:

Reply from 192.168.20.11: bytes=32 time<1ms TTL=255
Reply from 192.168.20.11: bytes=32 time<1ms TTL=255
Reply from 192.168.20.11: bytes=32 time<1ms TTL=255
Reply from 192.168.20.11: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.20.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

PC-A able to ping S1 VLAN 2

```
C:\>ping 192.168.10.12

Pinging 192.168.10.12 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Were the pings from PC-B to S2 successful? Explain.

- **PC-B is not able to ping S1 VLAN 10, since they are on different VLANs and have different network addresses, communication between them requires an Inter-VLAN routing protocol to facilitate interaction across VLANs.**