

## 3.6.2 Lab – Implement VLANs and Trunking (Answers)

 [itexamanswers.net/3-6-2-lab-implement-vlans-and-trunking-answers.html](https://itexamanswers.net/3-6-2-lab-implement-vlans-and-trunking-answers.html)

September 29, 2020

### Lab – Implement VLANs and Trunking (Instructor Version)

#### Topology



#### Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 10	192.168.10.11	255.255.255.0

Device	Interface	IP Address	Subnet Mask
	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.

b. Assign a device name to the switch.

```
switch(config)# hostname S1
```

```
switch(config)# hostname S2
```

c. Disable DNS lookup.

```
S1(config)# no ip domain-lookup
```

```
S2(config)# no ip domain-lookup
```

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

```
S1(config)# enable secret class
```

```
S2(config)# enable secret class
```

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

```
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
```

```
S2(config)# line console 0
S2(config-line)# password cisco
S2(config-line)# login
```

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

```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
```

```
S2(config)# line vty 0 15
S2(config-line)# password cisco
S2(config-line)# login
```

g. Encrypt the plaintext passwords.

```
S1(config)# service password-encryption
```

```
S2(config)# service password-encryption
```

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

```
S1(config)# banner motd $ Authorized Users Only! $
```

```
S2(config)# banner motd $ Authorized Users Only! $
```

i. Copy the running configuration to the startup configuration.

```
S1# copy running-config startup-config
```

```
S2# copy running-config startup-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.

```

S1(config)# vlan 10
S1(config-vlan)# name Management
S1(config-vlan)# vlan 20
S1(config-vlan)# name Sales
S1(config-vlan)# vlan 30
S1(config-vlan)# name Operations
S1(config-vlan)# vlan 999
S1(config-vlan)# name ParkingLot
S1(config-vlan)# vlan 1000
S1(config-vlan)# name Native

```

```

S2(config)# vlan 10
S2(config-vlan)# name Management
S2(config-vlan)# vlan 20
S2(config-vlan)# name Sales
S2(config-vlan)# vlan 30
S2(config-vlan)# name Operations
S2(config-vlan)# vlan 999
S2(config-vlan)# name ParkingLot
S2(config-vlan)# vlan 1000
S2(config-vlan)# name Native

```

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

```

S1(config)# interface vlan 10
S1(config-if)# ip address 192.168.10.11 255.255.255.0
S1(config-if)# interface vlan 20
S1(config-if)# ip address 192.168.20.11 255.255.255.0
S1(config-if)# interface vlan 30
S1(config-if)# ip address 192.168.30.11 255.255.255.0

S2(config)# interface vlan 10
S2(config-if)# ip address 192.168.10.12 255.255.255.0

```

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

```

S1(config)# interface range f0/2 - 5, f0/7 - 24, g0/1 - 2
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown

S2(config)# interface range f0/2 - 17, f0/19 - 24, g0/1 - 2
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 999
S2(config-if-range)# shutdown

```

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.

```

S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20

S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 30

```

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

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1
10	Management	active	
20	Sales	active	Fa0/6
30	Operations	active	
999	Parking_Lot	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 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
1000	Native	active	

<output omitted>

```
S2# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1
10	Management	active	
20	Sales	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, Gi0/1, Gi0/2

<output omitted>

### Part 3: Configure an 802.1Q Trunk Between the Switches

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

Step 1: Manually configure trunk interface Fo/1.

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

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```

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

```
S1(config-if)# switchport trunk native vlan 1000
```

```
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.

```
S1(config-if)# switchport trunk allowed vlan 10,20,30,1000
```

```
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.

```
S1# show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	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	10,20,30,1000			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa0/1	10,20,30,1000			

Step 2: Verify connectivity.

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

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

The pings were not successful because they are not in the same VLAN. A router is needed to communicate between VLANs.

## **Device Configs – Final**

---

### **Switch S1**

---

```

S1# show run
Building configuration...

Current configuration : 3310 bytes
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$qZwa$0nq3ruS0CBIH0izu35Xyg1
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
switchport trunk allowed vlan 10,20,30,1000
switchport trunk native vlan 1000
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/3
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/4
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/5
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/6
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/8
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/9
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/10
switchport access vlan 999
switchport mode access
shutdown

```

```

!
interface FastEthernet0/11
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/12
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/13
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/14
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/15
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/16
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/17
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/18
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/19
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/20
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/21
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/22
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/23
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/24
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface GigabitEthernet0/1
  switchport access vlan 999
  switchport mode access
  shutdown
!

```



```
interface GigabitEthernet0/2
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface Vlan1
  no ip address
!
interface Vlan10
  ip address 192.168.10.11 255.255.255.0
!
interface Vlan20
  ip address 192.168.20.11 255.255.255.0
!
interface Vlan30
  ip address 192.168.30.11 255.255.255.0
!
ip http server
ip http secure-server
!
banner motd ^C Authorized Users Only! ^C
!
line con 0
  password 7 045802150C2E
  login
line vty 0 4
  password 7 045802150C2E
  login
line vty 5 15
  login
!
end
```

## Switch S2

---

```

S2# show run
Building configuration...

Current configuration : 3192 bytes
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$7PUn$ac4H.MnZig5S0QiNJUH4j/
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
switchport trunk allowed vlan 10,20,30,1000
switchport trunk native vlan 1000
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/3
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/4
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/5
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/6
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/7
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/8
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/9
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/10
switchport access vlan 999
switchport mode access

```

```

shutdown
!
interface FastEthernet0/11
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/12
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/13
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/14
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/15
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/16
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/17
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/18
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/20
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/21
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/23
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/24
switchport access vlan 999
switchport mode access
shutdown
!
interface GigabitEthernet0/1
switchport access vlan 999
switchport mode access
shutdown
!

```

```
interface GigabitEthernet0/2
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan10
  ip address 192.168.10.12 255.255.255.0
!
ip http server
ip http secure-server
!
banner motd ^C Authorized Users Only! ^C
!
line con 0
  password 7 1511021F0725
  login
line vty 0 4
  password 7 1511021F0725
  login
line vty 5 15
  login
!
end
```

**Download PDF & PKT file Completed 100% Score:**

---

[sociallocker id="54558"][/sociallocker]