Lab 04: VLAN Configuration and Inter-VLAN Routing

4.1 Objectives:

- Define and describe the concept of VLAN
- Describe the advantages of VLAN
- Design and implement VLAN and inter-VLAN routing

4.2 Theory:

As with other labs, this lab will also build up on the concepts and techniques of previous labs. So, make sure you have properly understood the previous lab contents.

VLAN
VLAN or Virtual LAN (Local Area Network) is a logical grouping of networking devices. When we create VLAN, we actually break a large broadcast domain into smaller broadcast domains. Consider VLAN as a subnet. Just as two different subnets cannot communicate with each other without a router, different VLANs also require a router to communicate.

Advantages of VLAN
VLAN provides the following advantages:

- Solve the broadcast problem.
- Reduce the size of broadcast domains.
- Allow us to add an additional layer of security.
- Make device management easier.
- Allow us to implement the logical grouping of devices by function instead of location.

Solves the broadcast problem.
When we connect devices to the switch ports, the switch creates a single broadcast domain for all ports. Switch forwards a broadcast frame from all possible ports. In a large network, having hundreds of computers could create performance issues. Of course, we could use routers to solve the broadcast problem, but that would be a costly solution since each broadcast domain requires its own port on the router. Switch has a unique solution to broadcast issues known as VLAN. In the practical environment, we use VLAN to solve broadcast issues instead of a router.
Each VLAN has a separate broadcast domain. Logically, VLANs are also subnets. Each VLAN requires a unique network number known as VLAN ID. Devices with the same VLAN ID are the members of the same broadcast domain and receive all broadcasts. These broadcasts are filtered from all ports on a switch that aren't members of the same VLAN.

Reduces the size of broadcast domains.
VLANs increase the number of broadcast domains while reducing their size. For example, let's consider that we have a network of 100 devices. Without any VLAN implementation, we have a single broadcast domain that contains 100 devices. We create 2 VLANs and assign 50 devices

to each VLAN. Now, we have two broadcast domains with fifty devices in each. Thus, more VLAN means more broadcast domains with fewer devices.

Allows us to add an additional layer of security.
VLANs enhance the network security. In a typical layer-2 network, all users can see all devices by default. Any user can see a network broadcast and respond to it. Users can access any network resources located on that specific network. Users could join a workgroup by just attaching their system to the existing switch. This could create real trouble on the security platform. Properly configured VLANs give us total control over each port and user. With VLANs, you can prevent users from gaining unwanted access to resources. We can put the group of users that need high-level security into their own VLAN so that users outside of that VLAN can't communicate with them.

Makes device management easier.
Device management is easier with VLANs. Since VLANs are a logical approach, a device can be located anywhere in the switched network and still belong to the same broadcast domain. We can move a user from one switch to another switch in the same network while keeping his original VLAN. For example, a company has a five-storied building and a single layer-2 network. In this scenario, VLAN allows to move the users from one floor to another floor while keeping their original VLAN ID. The only limitation is that the device must still be connected to the same layer-2 network.

Allows us to implement the logical grouping of devices by function instead of location.
VLANs allow us to group the users by their function instead of their geographic locations. Switches maintain the integrity of your VLANs. Users will see only what they are supposed to see regardless of their physical location.

VLAN Example
To understand VLAN more clearly, let's take an example.

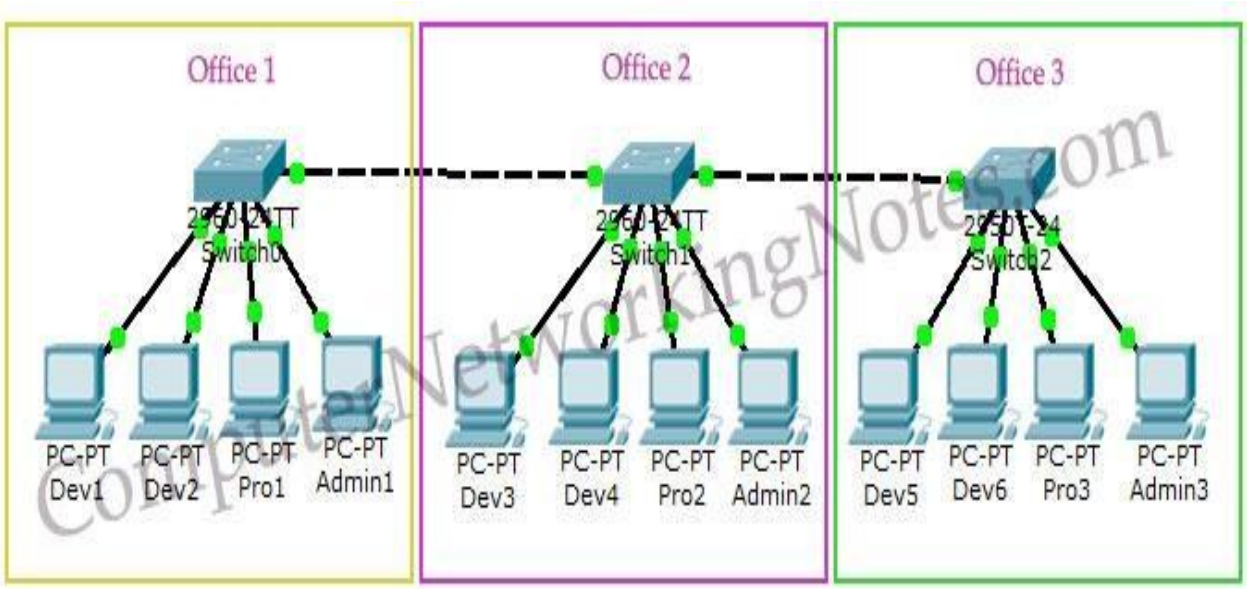

Figure 1: A Sample Network with VLANs

- Our company has three offices.
- All offices are connected with back-links (links connecting switches).
- The company has three departments: Development, Production, and Administration.
- The Development department has six computers (PCs).
- The Production and the Administration department has three PCs separately.
- Each office has two PCs from the Development department and one from both the Production and the Administration departments.
- The Production and the Administration departments have sensitive information that must be separated from the Development department.

With the default configuration, all computers connected to the same switch share a single broadcast domain. The Development department can access the administration or the production department resources.
With VLAN, we can create logical boundaries over the physical network. Assume we created three VLANs for our network and assigned them to the related computers.

- VLAN **Admin** for the Administration department.
- VLAN **Dev** for the Development department.
- VLAN **Pro** for the Production department.

Physically, we changed nothing, but logically, we grouped devices according to their function. These groups [VLANs] need routers of a layer-3 switch to communicate with each other. Logically, our network looks like the one shown in Figure 2.

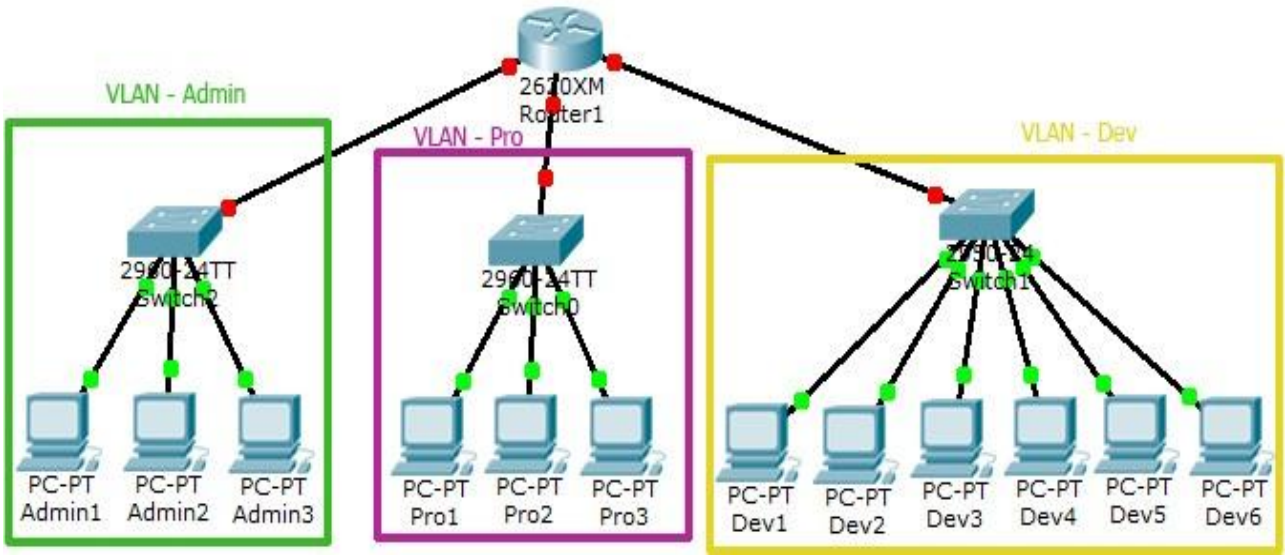

Figure 2: A logical representation of VLANs.

With the help of VLAN, we have separated our single network into three small networks (sub-networks). These networks do not share their broadcast domains with each other, which improves network performance and enhances security. Now, the Development department cannot access the Administration and the Production departments directly.

VLAN Connections

During the configuration of VLAN on ports, we need to know what type of connection it has. Switch supports two types of VLAN connection:

1. Access link
2. Trunk link

Access link

An access link is a connection where a switch port is connected to a device that has a standardized Ethernet NIC. Standard NIC only understands IEEE 802.3 or Ethernet II frames. Access link connection can only be assigned with a single VLAN. That means all devices connected to this port will be in the same broadcast domain.

For example, if twenty users are connected to a hub, and we connect that hub with an access link port on a switch, then all of these users belong to the same VLAN. If we want to keep ten users in another VLAN, then we have to purchase another hub. We must plug in those ten users in that hub and then connect it with another access link port on the switch.

Trunk link

A Trunk link is a connection where a switch port is connected to a device that is capable of understanding multiple VLANs. Usually, a trunk link connection is used to connect two switches or switches to a router. Remember when we said that VLAN could span anywhere in the network? That is basically due to the trunk link connection. Trunking allows us to send or receive VLAN information across the network. To support trunking, the original Ethernet frame is modified to carry VLAN information.

Figure 3 demonstrates access links and trunk links in a VLAN.

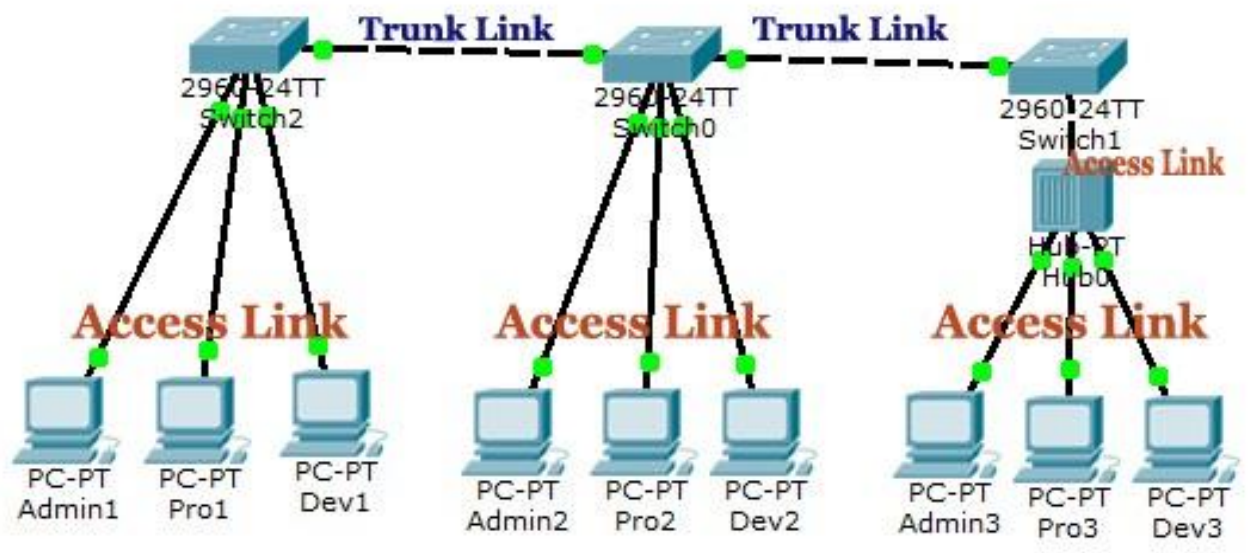

Figure 3: Access links and trunk links in a sample VLAN.

Inter-VLAN Routing

Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another using a layer-3 device. Two common approaches to inter-VLAN routing are the router-on-a-stick approach and the layer-3 switch, which uses switch virtual interfaces (SVIs).

In the router-on-a-stick approach, one of the router's physical interfaces is configured as an 802.1Q trunk port so it can understand VLAN tags. Note that VLAN tags are used to identify packets belonging to different VLANs so that they can be routed to the appropriate VLAN members. Separate logical subinterfaces are created for each VLAN on that trunk port. Each subinterface is configured with an IP address from the VLAN it represents. The configured subinterfaces are software-based virtual interfaces. VLAN members (hosts) are configured to use the subinterface address as a default gateway. When VLAN-tagged traffic enters the router interface, it is forwarded to the VLAN subinterface. After a routing decision is made based on the destination IP network address, the router determines the exit interface for the traffic and sends out the packet through that interface. The router-on-a-stick method of inter-VLAN routing does not scale beyond 50 VLANs. For this reason, a layer-3 switch using SVIs is used for a scalable solution. Figure 4 is an example of a router-on-a-stick approach to inter-Vlan routing.

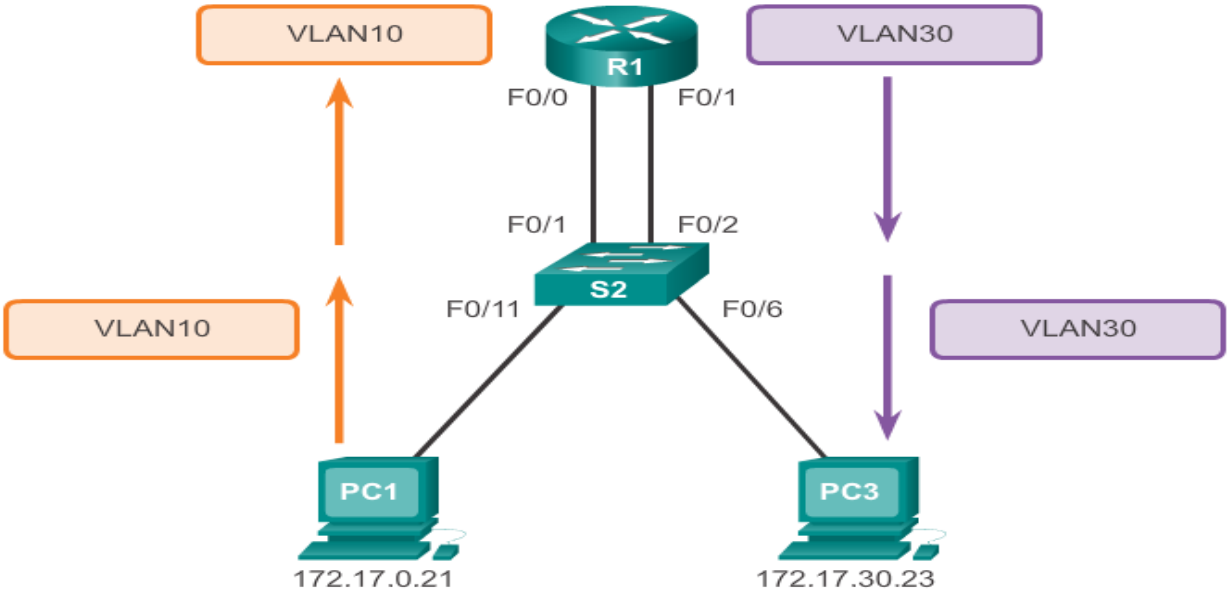

Figure 4: An example of a Router-on-a-Stick approach to inter-VLAN routing.

A layer-3 switch is also known as a Multi-Layer Switch (MLS) as it operates both in layer-2 and layer-3. A switch virtual interface (SVI) is created for each VLAN i.e. one SVI is for one VLAN. The function of a SVI is the same as the router interface in case of the router-on-a-stick approach. It processes the incoming and outgoing packets of the VLANs and routes them accordingly. As the packets do not leave the switch to be routed to a different network, the latency is very low compared to router-on-a-stick approach. This MLS approach is employed in most modern enterprise systems due to its scalability and faster routing. Figure 5 is an example of an MLS approach to inter-VLAN routing.

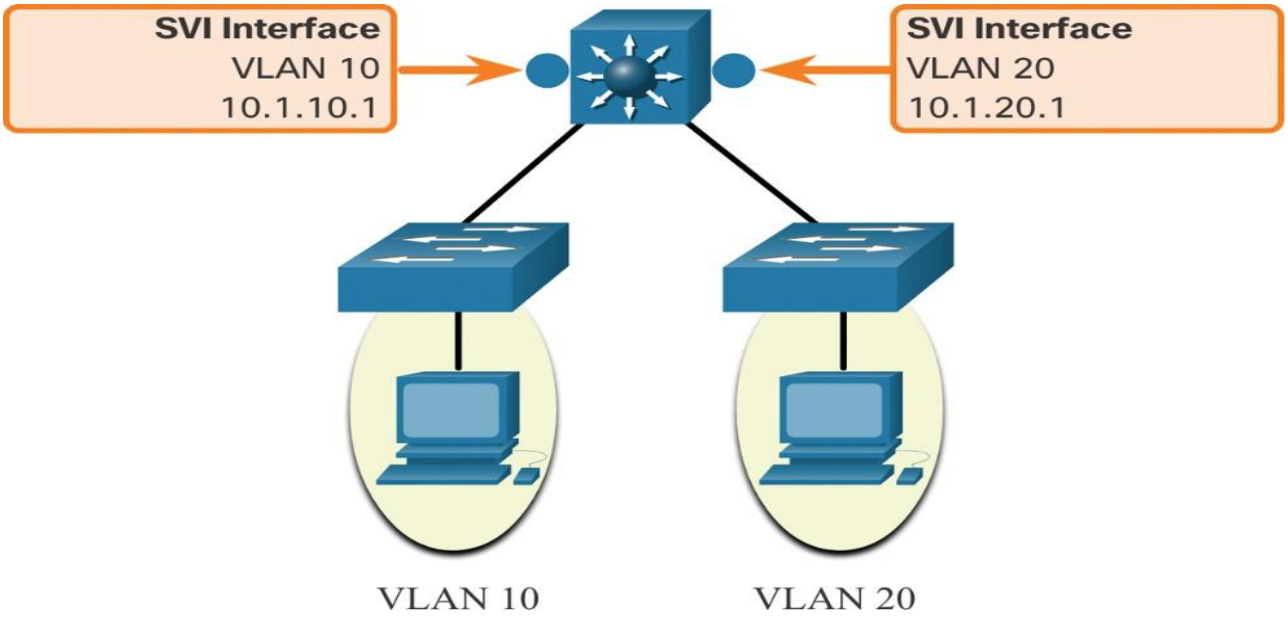

Figure 5: An example of an MLS approach to inter-VLAN routing.

4.3 Configure inter-VLAN routing using Router-on-a-Stick approach:

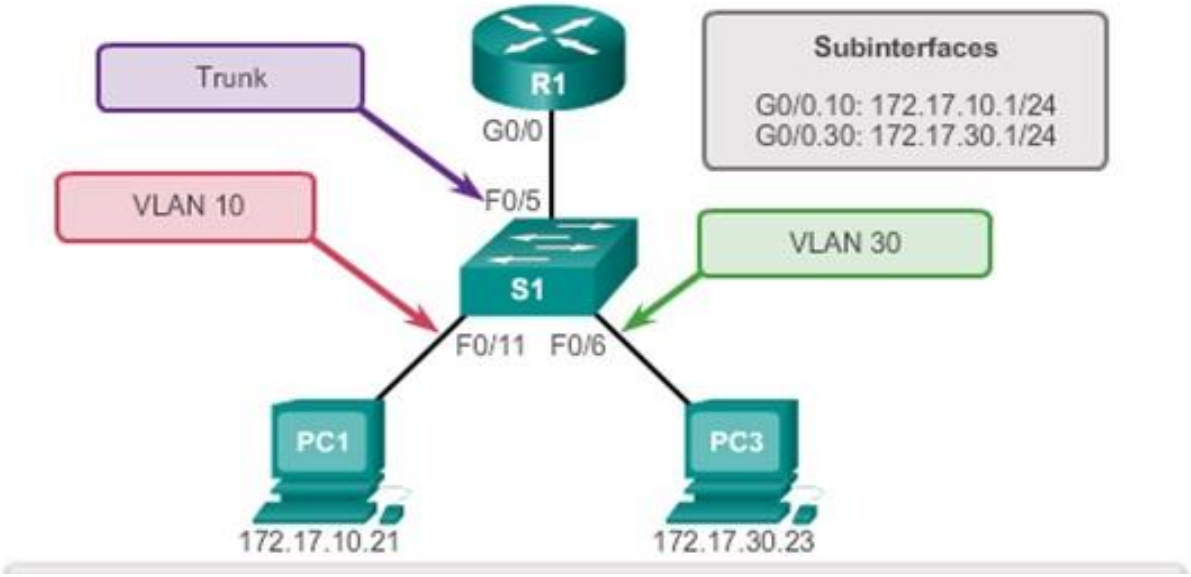

Figure 6: A sample network topology for configuring inter-Vlan routing using the router-on-a-stick approach.

In this section, we will configure the network topology in Figure 6 consisting of two VLANs using the router-on-a-stick approach.

a. At first, configure two (2) Vlans with VLAN ID 10 and 30 inside the switch.

```
S1(config)# vlan 10
S1(config-vlan)# exit
S1(config)# vlan 30
S1(config-vlan)# exit
S1(config)# exit
S1# show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 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, Gig0/1, Gig0/2
10   VLAN0010                          active    Fa0/11
30   VLAN0030                          active    Fa0/6
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

```
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

b. Now, configure the interfaces of the switch belonging to each VLAN.
The interfaces that connect PCs will be the access link.

```
S1(config)# interface Fast-Ethernet 0/11
S1(config-if)# switchport mode access
```

This command configures the interface as an access link (see the theory section to understand an access link).

```
S1(config-if)# switchport access vlan 10
```

This command assigns VLAN 10 to access ports.

```
S1(config-if)# no shutdown

S1(config)# interface Fast-Ethernet 0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 30
S1(config-if)# no shutdown
```

The interface connected to the router will be the trunk link.

```
S1(config)# interface Fast-Ethernet 0/5
S1(config-if)# switchport mode trunk
```

This command configures the interface as a trunk link (see the theory section to understand a trunk link).

```
S1(config-if)# switchport trunk allowed vlan all
```

This command specifies the list of VLANs on the trunk link. In this case, we have allowed all the VLANs.

```
S1(config-if)# no shutdown
```

c. Finally, configure the router subinterfaces.

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface g0/0
R1(config-if)# no shutdown
```

The command `encapsulation dot1q ##` enables IEEE 802.1Q encapsulation of network traffic on the specified subinterface. Also remember to specify the VLAN id after the interface identifier e.g., `interface g0/0.10`

d. Now, verify the inter-Vlan routing configuration and subinterfaces by issuing the command `show ip route`.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L       172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C       172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L       172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

4.4 Tasks:

1. The task description for this task is provided in 4.4.1. In this task, you need to implement inter-VLAN routing using a layer-3 switch or MLS approach. You have also been given a .pka file for this task.
2. You will implement inter-VLAN routing using a router-on-a-stick approach. The task description is provided in 4.4.2. You will need to create the network topology yourself, as no .pka file has been provided for this task.
3. After completing the previous two tasks, you can start task 3. In this task, you have to design and implement VLANs for IUT. You can use your previous solution for task 3 of lab3. The description is provided in 4.4.3.

4.4.1 Task 1 - Configure Layer 3 Switching and Inter-VLAN Routing

Objectives
Part 1: Configure Layer 3 Switching
Part 2: Configure Vlan
Part 3: Configure Inter-Vlan Routing

Background / Scenario
A multilayer switch like the Cisco Catalyst 3650 is capable of both Layer 2 switching and Layer 3 routing. One of the advantages of using a multilayer switch is this dual functionality. A benefit for a small to medium-sized company would be the ability to purchase a single multilayer switch instead of separate switching and routing network devices. Capabilities of a multilayer switch include the ability to route from one VLAN to another using multiple switched virtual interfaces (SVIs), as well as the ability to convert a Layer 2 switchport to a Layer 3 interface.

Addressing Table

Device	Interface	IP Address/Prefix
MLS	VLAN 10	192.168.10.1/24
	VLAN 20	192.168.20.1/24
	VLAN 30	192.168.30.1/24
	VLAN 99	192.168.99.254/24
	G0/2	209.165.200.225/30
PC0	NIC	192.168.10.2/24
PC1	NIC	192.168.20.2/24
PC2	NIC	192.168.30.2/24
PC3	NIC	192.168.10.3/24
PC4	NIC	192.168.20.3/24
PC5	NIC	192.168.30.3/24
Switch1	VLAN 99	192.168.99.1/24
Switch2	VLAN 99	192.168.99.2/24
Switch3	VLAN 99	192.168.99.3/24

Table 1: The Addressing Table for the task 2 of Lab 4

Instructions
Part 1: Configure Layer 3 Switching
In Part 1, you will configure the GigabitEthernet 0/2 port on switch MLS as a routed port and verify that you can ping another Layer 3 address.

a. On MLS, configure G0/2 as a routed port and assign an IP address according to the Addressing Table.

```
MLS(config)# interface g0/2
MLS(config-if)# no switchport
MLS(config-if)# ip address 209.165.200.225 255.255.255.252
```

b. Verify connectivity to **Cloud** by pinging 209.165.200.226.

```
MLS# ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Part 2: Configure Vlan

Add VLANs to Switch1, Switch2, Switch3, and MLS according to the table below. Packet Tracer scoring is case-sensitive, so type the names exactly as shown.

VLAN Number	VLAN Name
10	Stuff
20	Student
30	Faculty
99	Native

Table 2: The VLAN Table for the Task 2 of Lab 4

Part 3: Configure Inter-Vlan Routing

Step 1: Configure SVI on switches

a. On MLS, configure and activate the SVI interfaces for VLANs 10, 20, 30, and 99 according to the Addressing Table. The configuration for VLAN 10 is shown below as an example.

```
MLS(config)# interface vlan 10
MLS(config-if)# ip address 192.168.10.1 255.255.255.0
```

b. On other switches, configure and activate the SVI interface for VLAN 99 according to the Addressing Table.

Step 2: Configure Trunking on MLS

Trunk configuration differs slightly on a Layer 3 switch. On the Layer 3 switch, the trunking interface needs to be encapsulated with the dot1q protocol, however it is not necessary to specify VLAN numbers as it is when working with a router and subinterfaces.

a. On MLS, configure interface **g0/1**.

b. Make the interface a static trunk port.

```
MLS(config-if)# switchport mode trunk
```

c. Specify the native VLAN as 99.

```
MLS(config-if)# switchport trunk native vlan 99
```

d. Encapsulate the link with the dot1q protocol.

```
MLS(config-if)# switchport trunk encapsulation dot1q
```

Note: Packet Tracer may not score the trunk encapsulation.

Step 3: Configure Trunking on other Switches

a. Configure respective ports of other switches as static trunks.

b. Configure the native VLAN on the trunk.

Step 4: Enable Routing on MLS

a. Use the **show ip route** command. Are there any active routes?

b. Enter the **ip routing** command to enable routing in global configuration mode.
`MLS(config)# ip routing`

c. Use the **show ip route** command to verify routing is enabled.

```
MLS# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.10.0/24 is directly connected, Vlan10
C 192.168.20.0/24 is directly connected, Vlan20
C 192.168.30.0/24 is directly connected, Vlan30
C 192.168.99.0/24 is directly connected, Vlan99
209.165.200.0/30 is subnetted, 1 subnets
C 209.165.200.224 is directly connected, GigabitEthernet0/2
```

Step 5: Verify end-to-end connectivity.

a. From PC0, ping PC3 or MLS to verify connectivity within VLAN 10.

b. From PC1, ping PC4 or MLS to verify connectivity within VLAN 20.

c. From PC2, ping PC5 or MLS to verify connectivity within VLAN 30.

d. From S1, ping S2, S3, or MLS to verify connectivity with VLAN 99.

e. To verify inter-VLAN routing, ping devices outside the sender's VLAN.

4.4.2 Task 2 - Implement Inter-VLAN Routing using Router-on-a-Stick Approach

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
Part 4: Configure Inter-VLAN Routing on the Router
Part 5: Verify Inter-VLAN Routing is working

Backgroun / 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 separating sensitive data traffic from the rest of the network. 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. Adding an inter-VLAN router allows the organization to segregate and separate broadcast domains while simultaneously allowing them to communicate with each other.

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. A particular kind of inter-VLAN routing, called "Router-on-a-Stick", uses a trunk from the router to the switch to enable all VLANs to pass to the router.

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, create VLAN trunks between the two switches and between S1 and R1, and configure Inter-VLAN routing on R1 to allow hosts in different VLANs to communicate, regardless of which subnet the host resides.

Topology

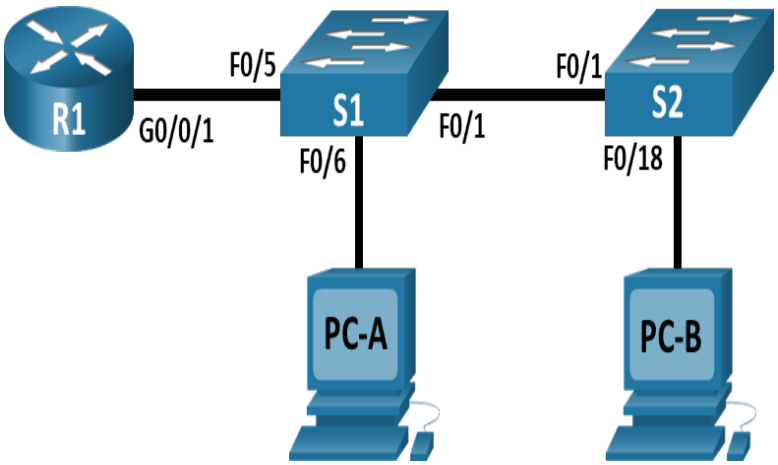

Figure 7: A Sample Network Topology for Vlan Configuration

Required Resources

- 1 Router (Cisco 4321)
- 2 Switches (Cisco 2960)
- 2 PCs
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/1.10	192.168.10.1	255.255.255.0	N/A
	G0/0/1.20	192.168.20.1	255.255.255.0	
	G0/0/1.30	192.168.30.1	255.255.255.0	
	G0/0/1.1000	N/A	N/A	
S1	VLAN 10	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 10	192.168.10.12	255.255.255.0	192.168.10.1
PC-A	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC-B	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Table 3: The Addressing Table for the task 1 of Lab 4

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 the router.

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

b. Enter configuration mode.

c. Assign a hostname to the router.

d. Disable DNS lookup to prevent the router 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. Save the running configuration to the startup configuration file.

Step 3: Configure basic settings for each switch.

a. Assign a hostname to the switches.

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

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

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

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

f. Encrypt the plaintext passwords.

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

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

Step 4: Configure PC hosts.
Refer to the Addressing Table for PC host address information and configure accordingly.

Part 2: Create VLANs and Assign Switch Ports.
In Part 2, you will create VLANs as specified in the VLAN Table on both switches. You will then assign the VLANs to the appropriate interface and verify your configuration settings. Complete the following tasks on each switch.

VLAN Table

VLAN	Name	Interface Assigned
10	Management	S1: VLAN 10 S2: VLAN 10
20	Sales	S1: F0/6
30	Operations	S2: F0/18
999	Parking_Lot	S1: F0/2-4, F0/7-24, G0/1-2 S2: S2: F0/2-17, F0/19-24, G0/1-2
1000	Native	N/A

Table 4: The VLAN Table for the Task 1 of Lab 4

Step 1: Create VLANs on both switches.

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

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

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.

b. Assign all unused ports on the switch to the Parking_Lot VLAN, configure them for static access mode, and administratively deactivate them.
Note: The interface range command is helpful to accomplish this task with as few commands as necessary.

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

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 on switches S1 and S2.

a. Configure static trunking on interface F0/1 for both switches.

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

c. Specify that VLANs 10, 20, 30, and 1000 are allowed to cross the trunk.

d. Verify trunking ports, the Native VLAN and allowed VLANs across the trunk.

Step 2: Manually configure S1's trunk interface F0/5

a. Configure S1's interface F0/5 with the same trunk parameters as F0/1. This is the trunk to the router.

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

c. Verify trunking.

Part 4: Configure Inter-VLAN Routing on the Router

Step 1: Configure the router.

a. Activate interface G0/0/1 as necessary on the router.

b. Configure sub-interfaces for each VLAN as specified in the IP addressing table. All sub-interfaces use 802.1Q encapsulation. Ensure the sub-interface for the native VLAN does not have an IP address assigned. Include a description for each sub-interface.

c. Verify the sub-interfaces are operational.

Step 2: Complete the following tests from PC-A. All should be successful.

a. Ping from PC-A to its default gateway.

b. Ping from PC-A to PC-B.

c. Ping from PC-A to S2.

Step 3: Complete the following test from PC-B.
From the Command Prompt window on PC-B, issue the **tracert** command to the address of PC-A.

Question:
What intermediate IP addresses are shown in the results?

4.4.3 Task 3 - Design and Implement Vlan and Inter-Vlan Routing for IUT

IUT has six departments: CSE, EEE, MCE, CEE, BTM, and TVE. Each department can further be divided into, at most, two sections. The student capacity of each department is 60. IUT wants to add a new department, BTHT. Initially, a total of 20 students will be enrolled under the BTHT department, but this number can be increased to 30 if needed.
You have been hired to provide a network solution for IUT. The institution is allowed to use the network address 192.168.0.0/16. Assume that the IP addresses for the six existing departments have already been assigned from 192.168.0.0/23. Your task is to design the given network address into a suitable number of subnets.

Instructions:

a. Find a suitable subnetwork address for each section/department.

b. Provide the subnet mask, first address, and last address for each subnet.

c. For each section/department, consider 2 PCs as end devices. Assign the first two addresses from the selected subnet to these end devices.

d. The end devices of departments are to be connected to switches separately. All switches should be connected to a single router.

e. Configure each section/department as a separate VLAN. Assume and configure other VLANs if necessary.

f. Configure inter-Vlan routing for the communication among VLANs. You can choose any approach between Router-on-a-Stick or with layer-3 Switching.

g. Verify the connectivity.

Note: You can use your previous solution (or any modification to the solution) of task 3 from lab 3.