

CSE 4512 [Computer Networks Lab]

Lab # 03

1. Objectives:

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

2. Theory:

As with other labs, this lab will also build up on the concepts and techniques of previous labs. So, make sure you've 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 large broadcast domain in smaller broadcast domains. Consider VLAN as a subnet. Same as two different subnets cannot communicate with each other without router, different VLANs also requires router to communicate.

Advantages of VLAN

VLAN provides following advantages:-

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

Solves broadcast problem

When we connect devices into the switch ports, switch creates single broadcast domain for all ports. Switch forwards a broadcast frame from all possible ports. In a large network having hundreds of computers, it could create performance issues. Of course, we could use routers to solve broadcast problem, but that would be costly solution since each broadcast domain requires its own port on router. Switch has a unique solution to broadcast issue known as VLAN. In practical environment, we use VLAN to solve broadcast issue instead of 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 same VLAN ID are the members of 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 numbers of broadcast domain while reducing their size. For example, lets consider we have a network of 100 devices. Without any VLAN implementation, we have single broadcast domain that contain 100 devices. We create 2 VLANs and assign 50 devices in each VLAN. Now we have two broadcast domains with fifty devices in each. Thus, more VLAN means more broadcast domain with less devices.

Allows us to add 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 network broadcast and responds to it. Users can access any network resources located on that specific network. Users could join a workgroup by just attaching their system in existing switch. This could create real trouble on security platform. Properly configured VLANs gives us total control over each port and users. With VLANs, you can control the users from gaining unwanted access over the resources. We can put the group of users that need high level security into their own VLAN so that users outside from VLAN can't communicate with them.

Makes device management easier

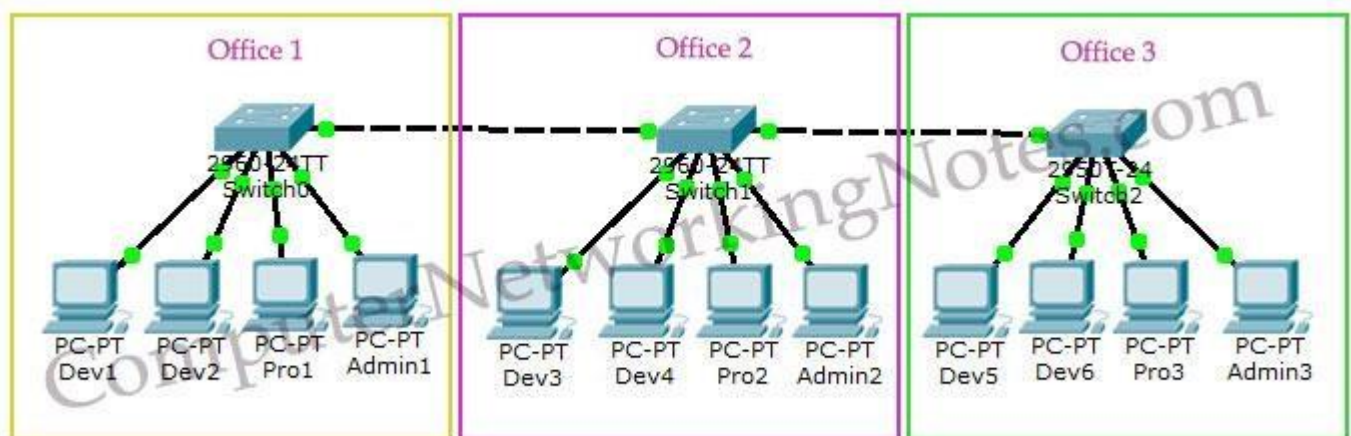
Device management is easier with VLANs. Since VLANs are a logical approach, a device can be located anywhere in the switched network and still belong to the same broadcast domain. We can move a user from one switch to another switch in same network while keeping his original VLAN. For example, a company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

VLAN Examples

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



- Our company has three offices.
- All offices are connected with back links (links connecting switches).
- Company has three departments Development, Production and Administration.

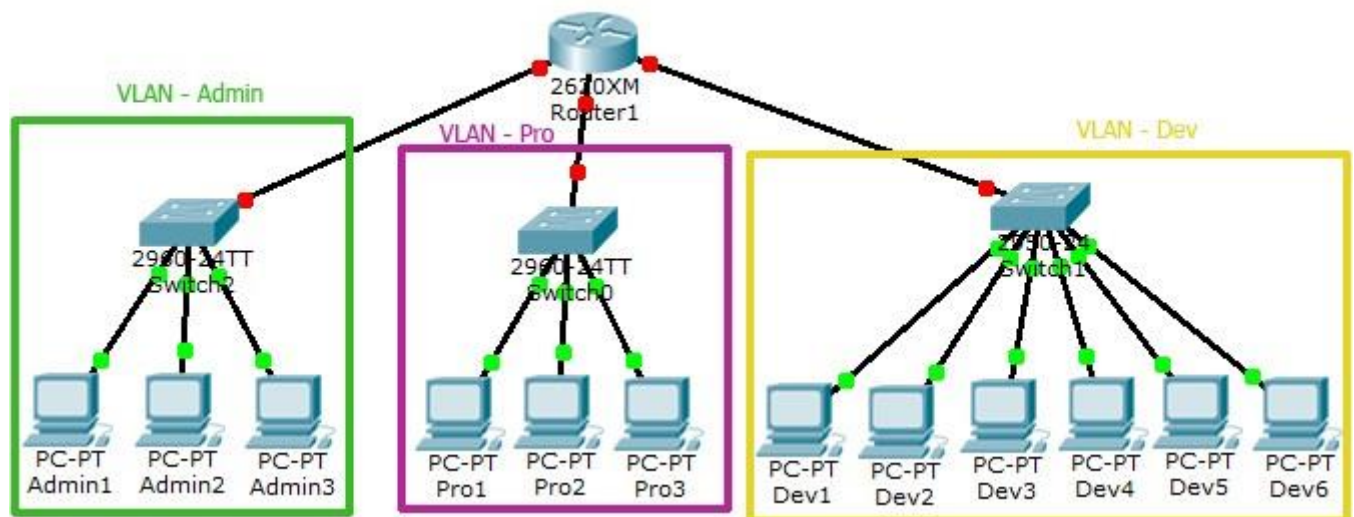
- Development department has six computers.
- Production department has three computers.
- Administration department also has three computers.
- Each office has two PCs from development department and one from both production and administration department.
- Administration and production department have sensitive information and need to be separate from development department.

With default configuration, all computers connected to the same switch share same broadcast domain. Development department can access the administration or production department resources.

With VLAN we could create logical boundaries over the physical network. Assume that we created three VLANs for our network and assigned them to the related computers.

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

Physically we changed nothing but logically we grouped devices according to their function. These groups [VLANs] need router to communicate with each other. Logically our network look likes following diagram.



With the help of VLAN, we have separated our single network in three small networks. These networks do not share broadcast with each other improving network performance and enhancing security. Now Development department cannot access the Administration and Production department directly.

VLAN Connections

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

- Access link
- Trunk link

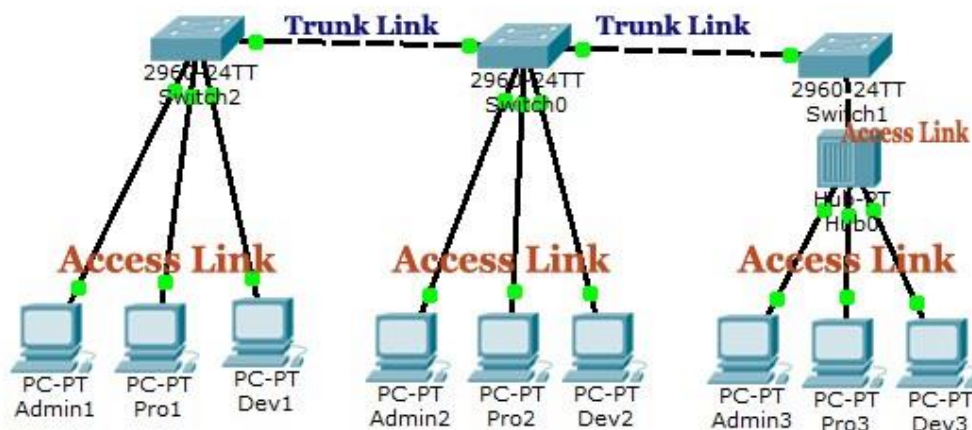
Access link

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

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

Trunk link

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

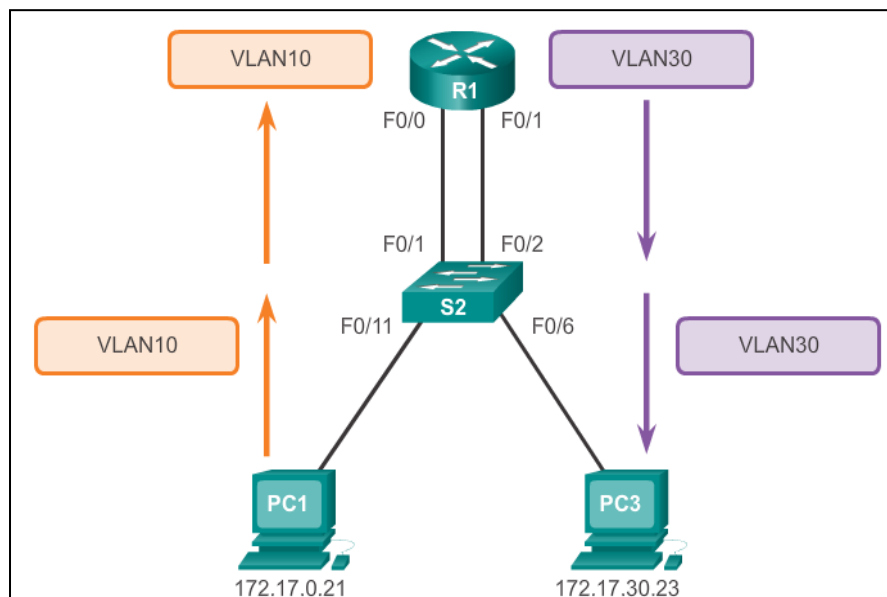


Inter-VLAN Routing:

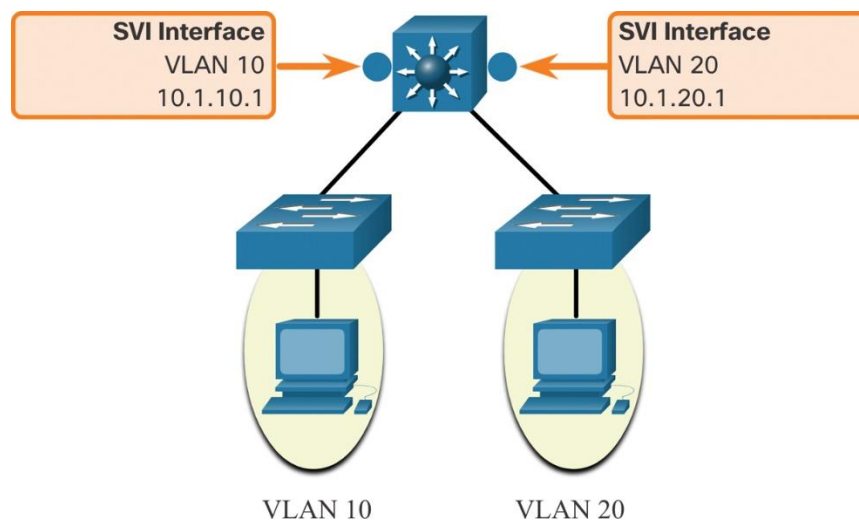
Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another, using a layer 3 device. Two common approaches to inter-VLAN routing are, router-on-a stick approach and layer 3 switch using switch virtual interfaces (SVIs).

In router-on-a-stick approach, one of the router's physical interfaces is configured as a 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 send 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 are used for a scalable solution. The following figure is an example of a router-on-a-stick approach inter-vlan routing.

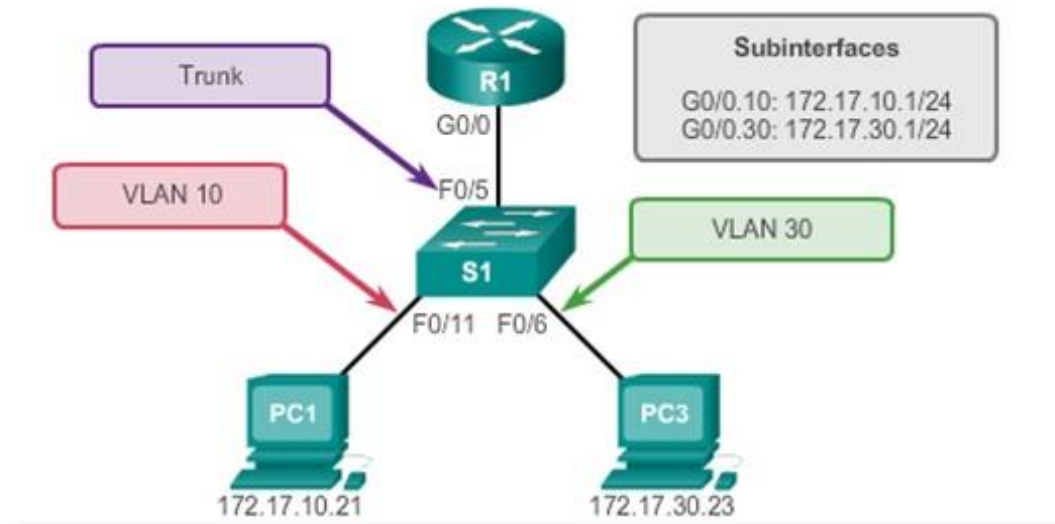


A layer 3 switch is also known as Multi Layer Switch (MLS) as it operates both in layer 2 and 3. A switch virtual interface or SVI is created for each VLAN i.e. one SVI for one VLAN. The function of a SVI is the same as the router interface in case of router-on-a-stick approach. It processes the incoming 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. Following is an example of a MLS approach to inter-VLAN routing.



3. Configure inter-VLAN routing using router-on-a-stick approach:

In this section, we'll configure the following network topology consisting of two VLANs using a router-on-a-stick approach.



- I.** At first, configure 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
```

- II.** Now, configure the Interfaces belonging to each VLAN:

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

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

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

This command assigns VLAN 10 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 port.

```
S1(config)# interface Fast-Ethernet 0/5
```

```
S1(config-if)# switchport mode trunk
```

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

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

This command specifies the list of VLANs specified on the trunk port. In this case, we've allowed *all* the VLANs.

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

III. Finally, configure the router subinterface.

```
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)# 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)# interface g0/0
R1(config-if)# no shutdown

*Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to up
```

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 like this, interface **g0/0.10**

IV. Now, verify the subinterfaces by issuing the commands as given in the following screenshots.

```
R1# show vlans
<output omitted>
Virtual LAN ID: 10 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interface: GigabitEthernet0/0.10

  Protocols Configured: Address:      Received:  Transmitted:
        IP             172.17.10.1      11          18
<output omitted>
Virtual LAN ID: 30 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interface: GigabitEthernet0/0.30

  Protocols Configured: Address:      Received:  Transmitted:
        IP             172.17.30.1      11          8
<output omitted>
```

```
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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP,
       l - LISP
       + - replicated route, % - next hop override

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
```

V. Setup the PCs like below:

PC-1:

IP Address: 172.17.10.21

Subnet Mask: 255.255.255.0

Gateway: 172.17.10.1

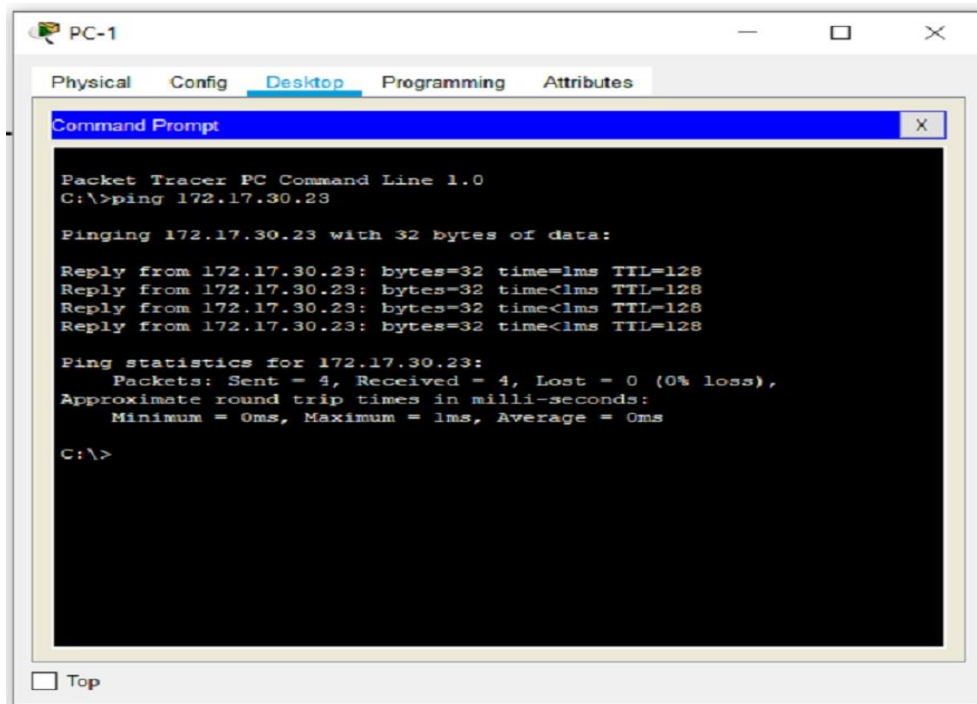
PC-2:

IP Address: 172.17.30.23

Subnet Mask: 255.255.255.0

Gateway: 172.17.30.1

VI. Finally, verify the routing is working properly by pinging *PC-2* from *PC-1*.



The screenshot shows a Packet Tracer interface for PC-1. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command to the IP address 172.17.30.23. The output indicates that the ping was successful, with four replies received, each with a time of less than 1ms and a TTL of 128. The ping statistics show 4 packets sent, 4 received, and 0% loss.

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.17.30.23

Pinging 172.17.30.23 with 32 bytes of data:

Reply from 172.17.30.23: bytes=32 time<1ms TTL=128
Reply from 172.17.30.23: bytes=32 time<1ms TTL=128
Reply from 172.17.30.23: bytes=32 time<1ms TTL=128
Reply from 172.17.30.23: bytes=32 time<1ms TTL=128

Ping statistics for 172.17.30.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

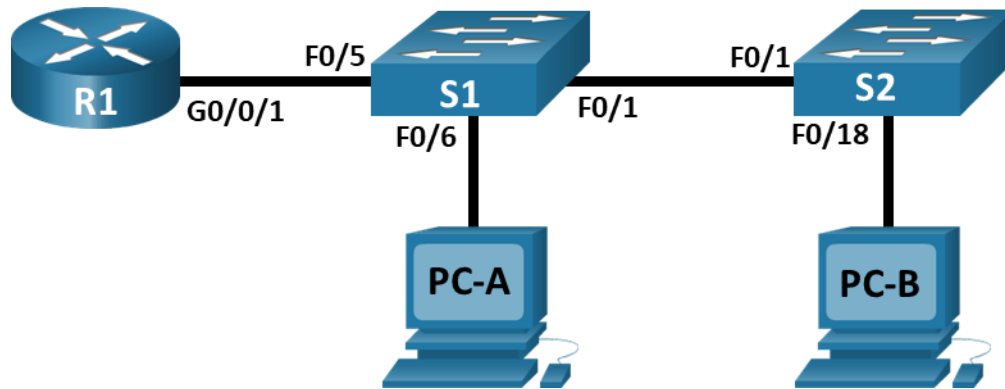
C:\>
```

4. Tasks:

- I. You will implement inter-VLAN routing using router-on-a-stick approach. The task description is provided in the *Task-1_implement-inter-vlan-routing-using-router-on-a-stick-approach* pdf. You'll need to create the network topology by yourself as there's no .pka file provided for this task.
- II. The task description for this task is provided in the *Task-2_configure-layer-3-switching-and-inter-vlan-routing* pdf. In this task, you need to implement inter-VLAN routing using layer-3 switch or MLS approach. You're also given a .pka file for this task.

Lab - Implement Inter-VLAN Routing

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

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: 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

Part 4: Configure Inter-VLAN Routing on the Router

Part 5: Verify Inter-VLAN Routing is working

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 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.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other routers, 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 routers and switches have been erased and have no startup configurations. If you are unsure contact your instructor.

Required Resources

- 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 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 the router.

- Console into the router and enable privileged EXEC mode.
- Enter configuration mode.
- Assign a device name to the router.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the vty password and enable login.
- Encrypt the plaintext passwords.
- Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- Save the running configuration to the startup configuration file.
- Set the clock on the router.

Step 3: Configure basic settings for each switch.

- Assign a device name to the switch.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- 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. Set the clock on the switch.
- i. Save the running configuration to the startup configuration.

Step 4: 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 and 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.
- b. Configure the management interface and default gateway on each switch using the IP address information in the Addressing Table.
- c. 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.

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. 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 switch 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.

What happens if G0/0/1 on R1 is down?

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.

Note: You may have to disable the PC firewall for pings to work 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.

What intermediate IP addresses are shown in the results?

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Packet Tracer - Configure Layer 3 Switching and Inter-VLAN Routing

Addressing Table

Device	Interface	IP Address / Prefix
MLS	VLAN 10	192.168.10.254 /24
		2001:db8:acad:10::1/64
	VLAN 20	192.168.20.254 /24
		2001:db8:acad:20::1/64
	VLAN 30	192.168.30.254/24
		2001:db8:acad:30::1/64
	VLAN 99	192.168.99.254/24
	G0/2	209.165.200.225
		2001:db8:acad:a::1/64
PC0	NIC	192.168.10.1
PC1	NIC	192.168.20.1
PC2	NIC	192.168.30.1
PC3	NIC	192.168.10.2/24
		2001:db8:acad:10::2/64
PC4	NIC	192.168.20.2/24
		2001:db8:acad:20::2/64
PC5	NIC	192.168.30.2
		2001:db8:acad:10::2/64
S1	VLAN 99	192.168.99.1
S2	VLAN 99	192.168.99.2
S3	VLAN 99	192.168.99.3

Objectives

Part 1: Configure Layer 3 Switching

Part 2: 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.

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.

- 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
```

- 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 Inter-VLAN Routing

Step 1: Add VLANs.

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

VLAN Number	VLAN Name
10	Staff
20	Student
30	Faculty

Step 2: Configure SVI 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 192.168.10.254 255.255.255.0
```

Step 3: 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 4: Configure trunking on S1.

- a. Configure interface **g0/1** of S1 as a static trunk.
b. Configure the native VLAN on the trunk.

Step 5: Enable routing.

- 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 6: 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.
- f. From any device, ping this address inside **Cloud**, 209.165.200.226.

The Layer 3 switch is now routing between VLANs and providing routed connectivity to the cloud.

References:

1. (CISCO Blogs, n.d.)
2. (CCNA Blogs, n.d.)