Lab 05: VLAN Configuration and Inter-VLAN Routing

Duration: 1 hours 30 minutes | In-Lab Assessment
Tools: Cisco Packet Tracer

Objectives:

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

Lab Description:

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.

Part A: 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.

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

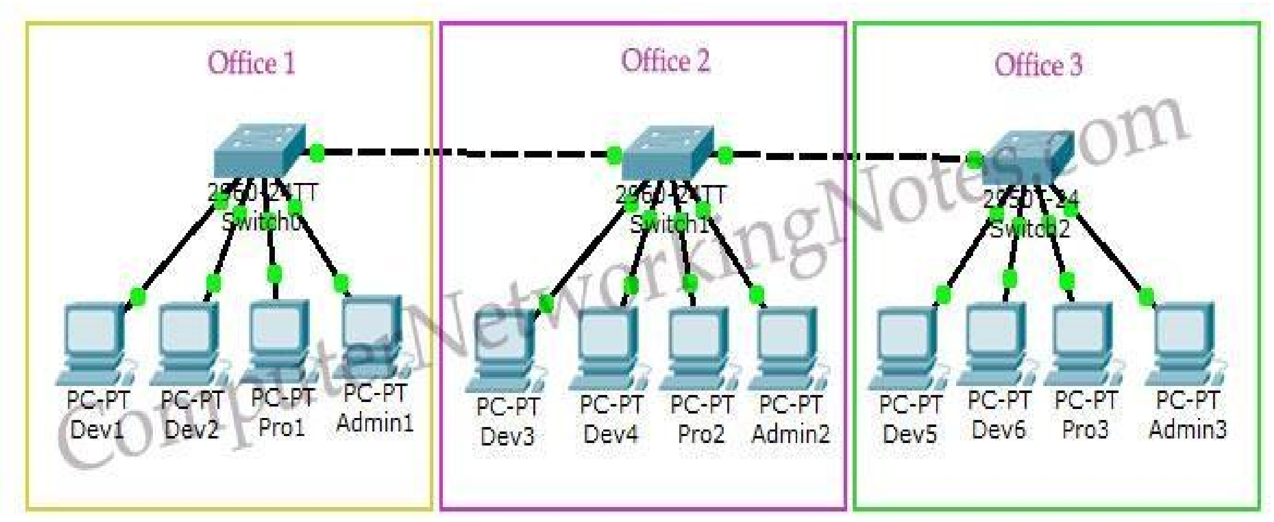

Figure 8: A Sample Network with VLANs

- 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 9.

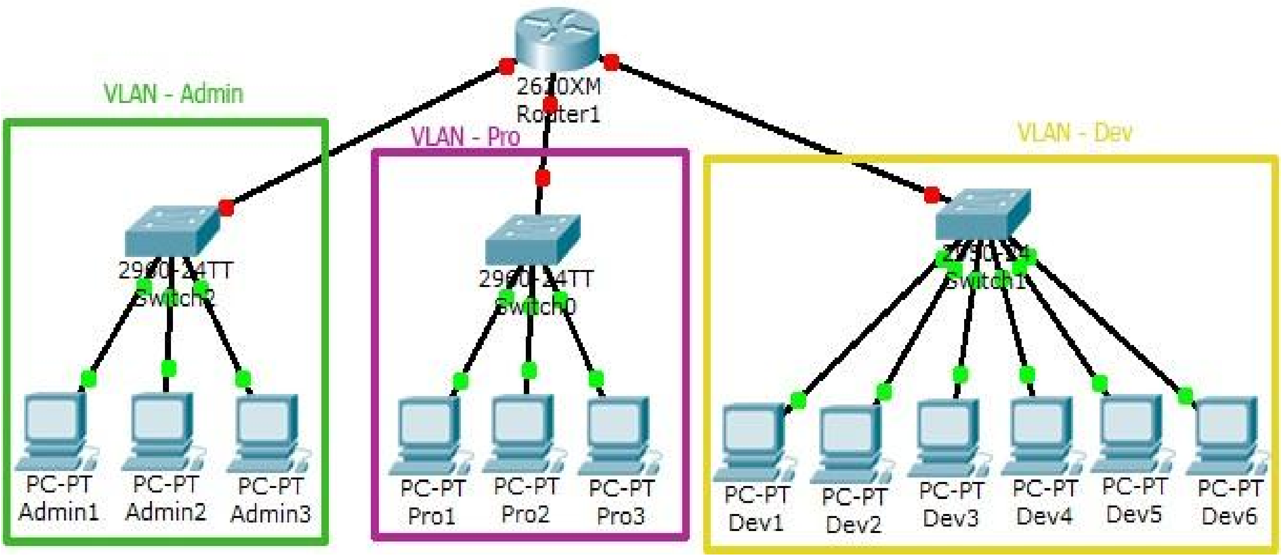

Figure 9: A logical representation of VLANs.

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.

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 10 demonstrates access links and trunk links in a VLAN.

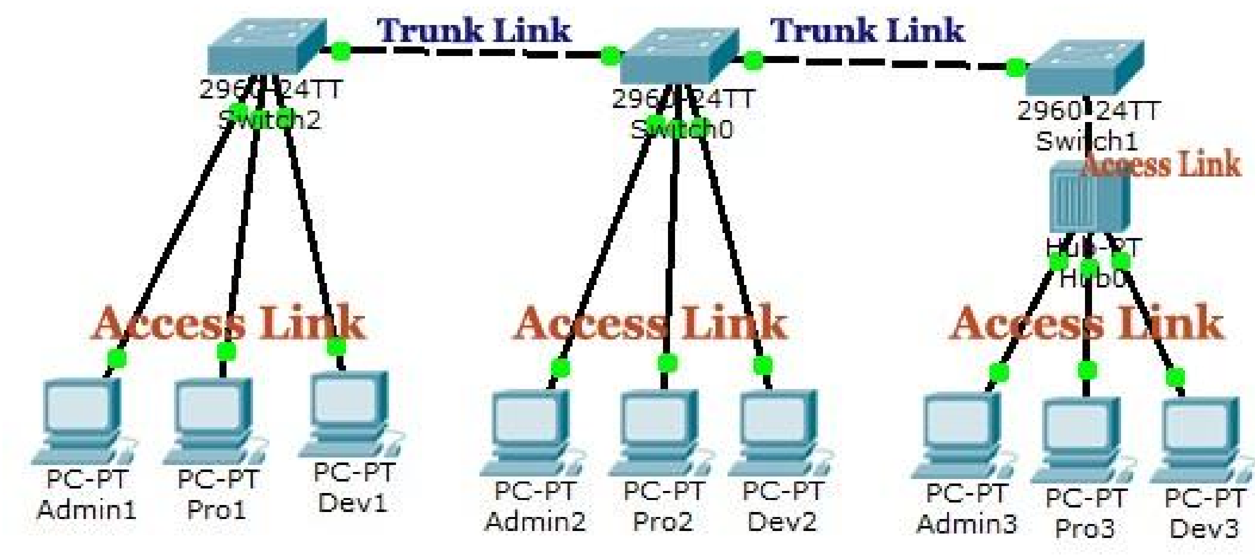

Figure 10: Access links and trunk links in a sample VLAN.

Part B: 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 11 is an example of a router-on-a-stick approach to inter-Vlan routing.

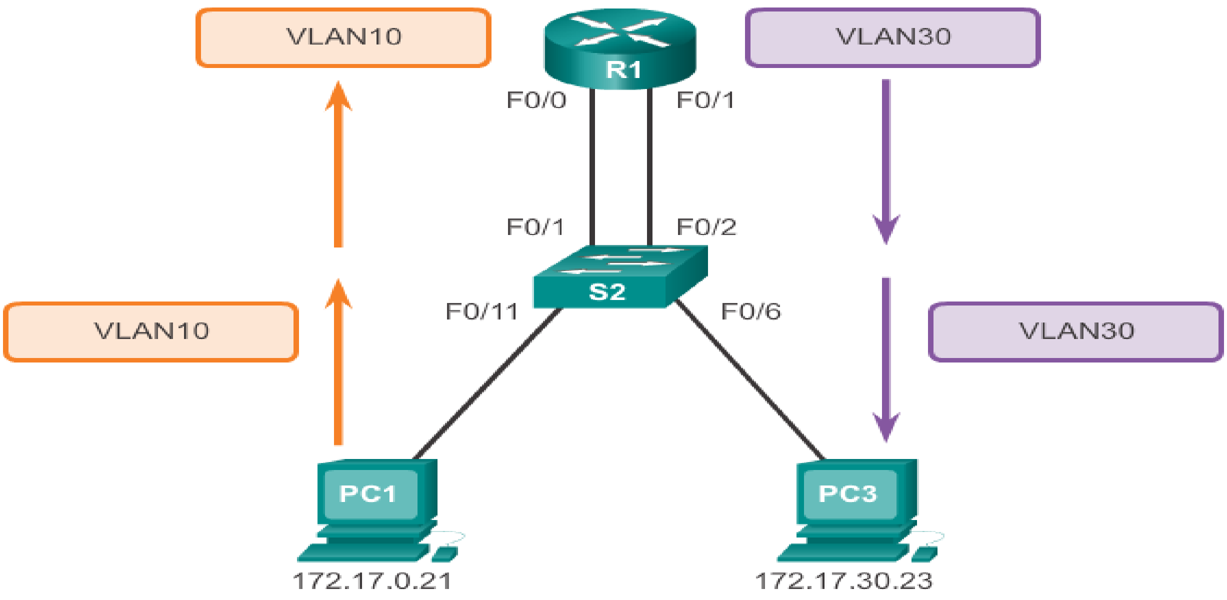

Figure 11: An example of a Router-on-a-Stick approach to inter-VLAN routing.

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 12 is an example of an MLS approach to inter-VLAN routing.

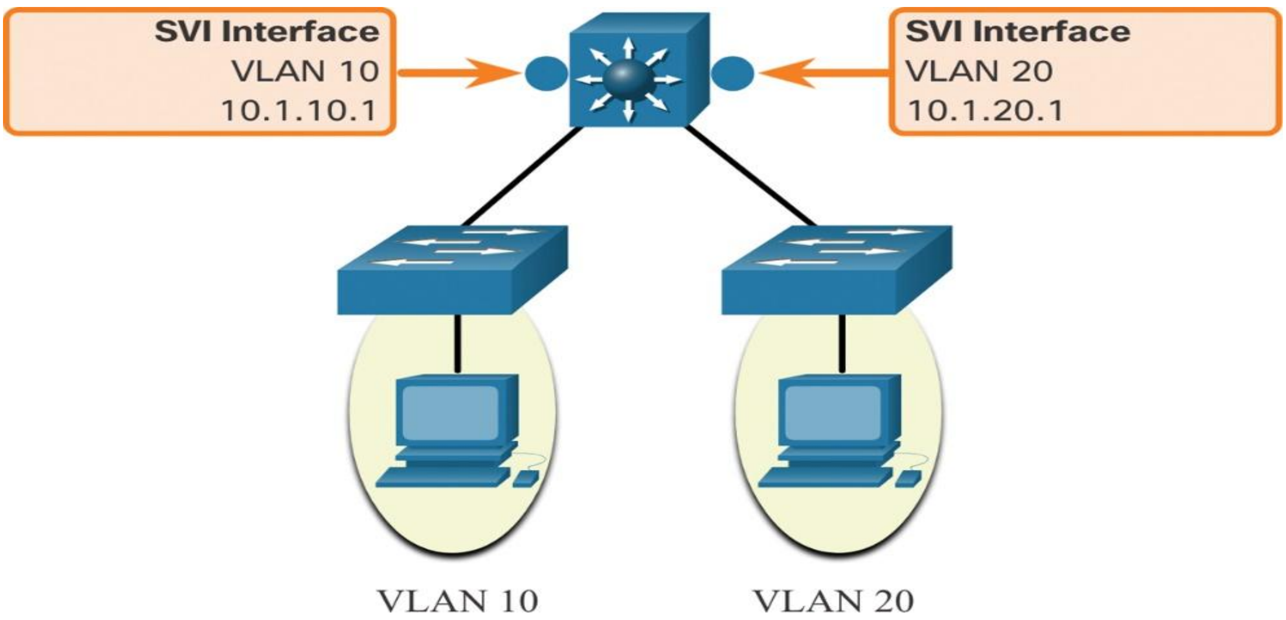

Figure 12: An example of an MLS approach to inter-VLAN routing.

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

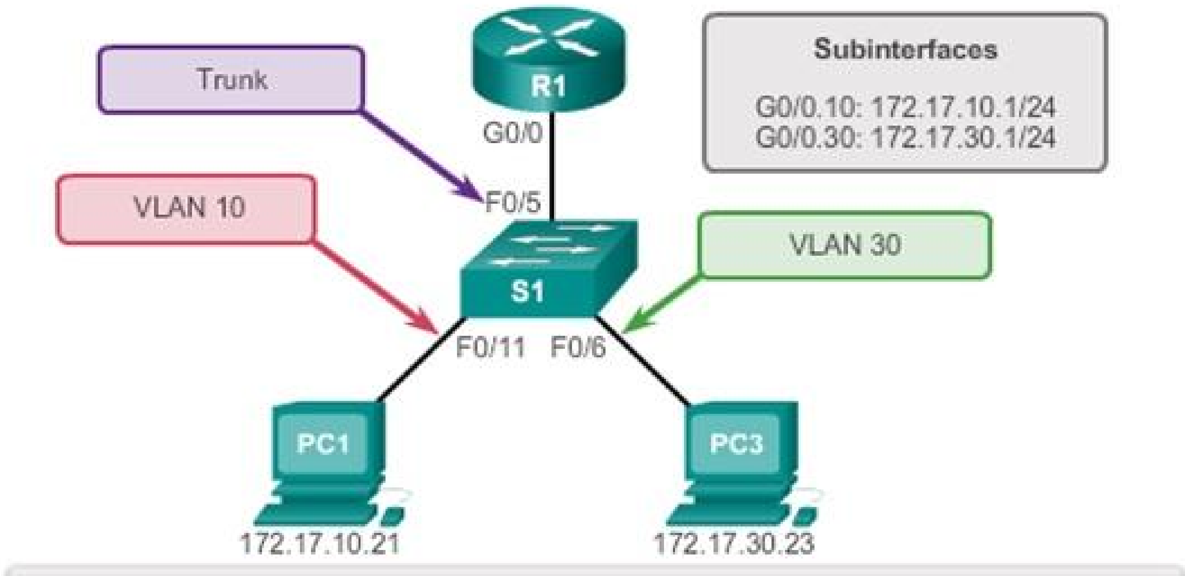

Figure 13: A sample network topology for configuring inter-Vlan routing using the router-on-a-stick approach.

In this section, we will configure the network topology in Figure 13 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
```