NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE
Computer Network Lab (CL3001)
Lab Session 12

Objective:

- Introduction to Virtual Area Networks - VLANS
- Types of Connections in VLAN
- Introduction to InterVLAN routing
- Configuration of VLAN
- Configuration of InterVLAN routing
- Lab Exercise

Virtual Area Networks [VLANS]

1. Introduction to Virtual Area Networks [VLANS]

A traditional LAN comprising of workstations connected to each other by means of a hub or a repeater form a single collision and broadcast domains. Due to this, these devices propagate any incoming data throughout the network. To prevent collisions from traveling through all the workstations in the network, a bridge or a switch can be used. These devices will not forward collisions, but still will allow broadcasts and multicasts to pass through. A router, therefore, may be used to prevent broadcasts and multicasts from traveling through different networks. To stop broadcasts in a same LAN segment, VLAN's allow a network manager to logically segment a LAN into different broadcast domains so that packets are only switched between ports that are designated for the same VLAN.

A Virtual Local Area Network can be defined as a group of networking devices in the same broadcast domain, logically. Since this is a logical segmentation and not a physical one, it means that the devices in the same VLAN may be widely separated in the network; both by geography and location, workstations do not have to be physically located together.

VLAN helps you group users together according to their function rather than their physical location. This means Users on different floors of the same building, or even in different buildings can now belong to the same LAN. This makes the management much simpler.

Some of the benefits of VLANs are:

1. They improve network performance by reducing the size of broadcast domains. In a broadcast domain, every device can send packets to every other device, and every packet must be received and processed. When a broadcast domain becomes very large, this can degrade the performance ofswitches on the network due to the high volumes of broadcast data

2. VLANs allow for the adding of additional layers of security. For example, a specific VLAN can becreated for users with specific security clearances.

3. VLANs make device management easier. If a user moves to a new physical location, the physical workstation of that user does not need to be reconfigured. Also, if a user stays in the same locationbut

changes jobs, only the VLAN membership of the workstation needs to be changed.

For multiple VLANs to communicate with each other, a router is required. Routers between VLANs filter broadcast traffic, enhance network security, perform address summarization, and mitigate network congestion**.**

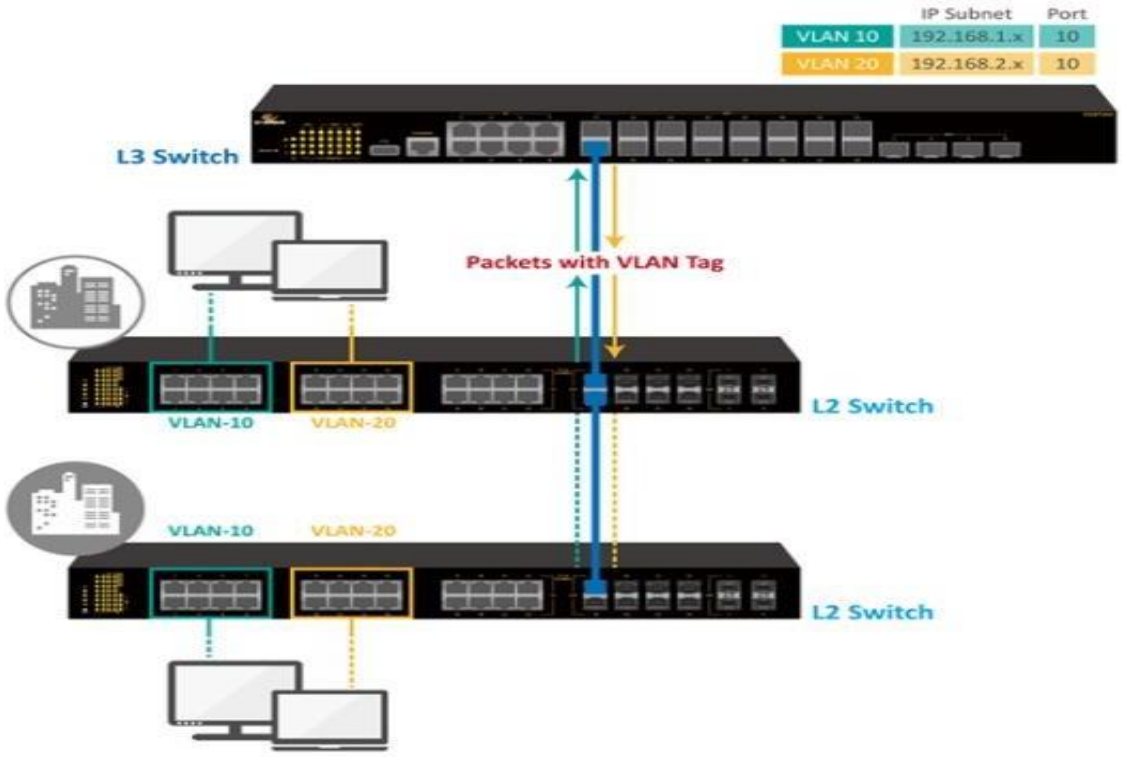

Fig-1: Multiple VLANS connections

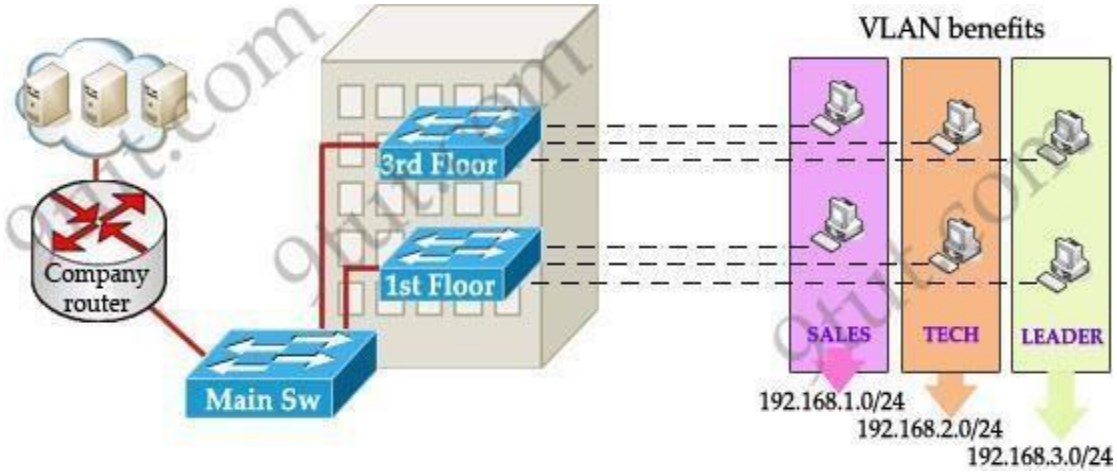

Fig-2: Real life scenario [Departmental wise VLAN example]

Take a real-world example as shown in figure 2. As VLANs break up broadcast domains, so now if a computer in Sales broadcasts, only computers in Sales will receive that frame.

It is important to point out that you don't have to configure a VLAN until your network gets so large and has so much traffic that you need one. Many times, people are simply using VLAN's because the network they are working on was already using them

You need to consider using VLAN's in any of the following situations:

- You have more than 200 devices on your LAN You have a lot of broadcast traffic on your LAN
- Groups of users need more security or are being slowed down by too many broadcasts? Groups of users need to be on the same broadcast domain because they are running the same applications.
- An example would be a company that has VoIP phones. The users using the phone could be on a different VLAN, not with the regular users. Or, just to make a single switch into multiple virtual switches.

Another important fact is that, on a Cisco switch, VLAN's are enabled by default and ALL devices are already in a VLAN. The VLAN that all devices are already in is VLAN 1. So, by default, you can just use all the ports on a switch and all devices will be able to talk to one another.

2. Types of Connection in VLAN:

Devices on a VLAN can be connected in three ways based on whether the connected devices are VLAN-aware or VLAN-unaware. Recall that a VLAN-aware device is one which understands VLAN memberships (i.e., which users belong to a VLAN) and VLAN formats. Below are the types of connection in VLAN.

(A) Trunk Link

All the devices connected to a trunk link, including workstations, must be VLAN-aware. All frames on a trunk link must have a special header attached. These special frames are called tagged frames as shown in figure 3.

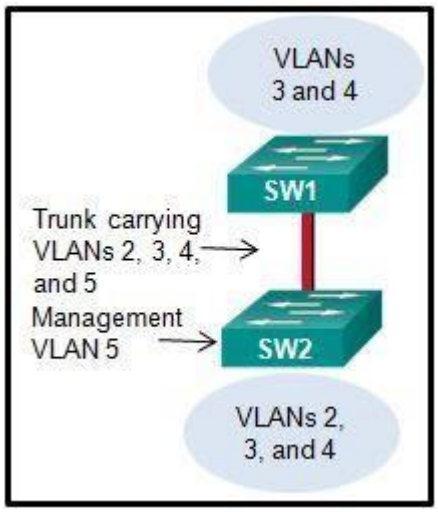

Fig-3: Trunk Link Connection

(B) Access Link

An access link connects a VLAN-unaware device to the port of a VLAN-aware bridge. All frames on access links must be implicitly tagged (untagged). The VLAN-unaware device can be a LAN segment with VLAN-unaware workstations or it can be a number of LAN segments containing VLAN-unaware devices (legacy LAN).

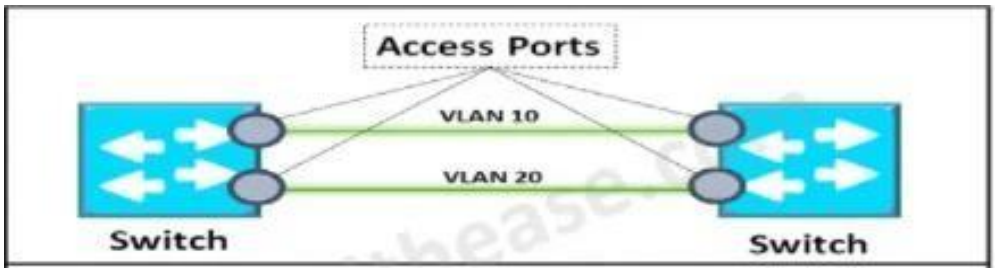

Fig-4: Access Link Connection

The combine pictural view of Access and Trunk link is given in figure 5

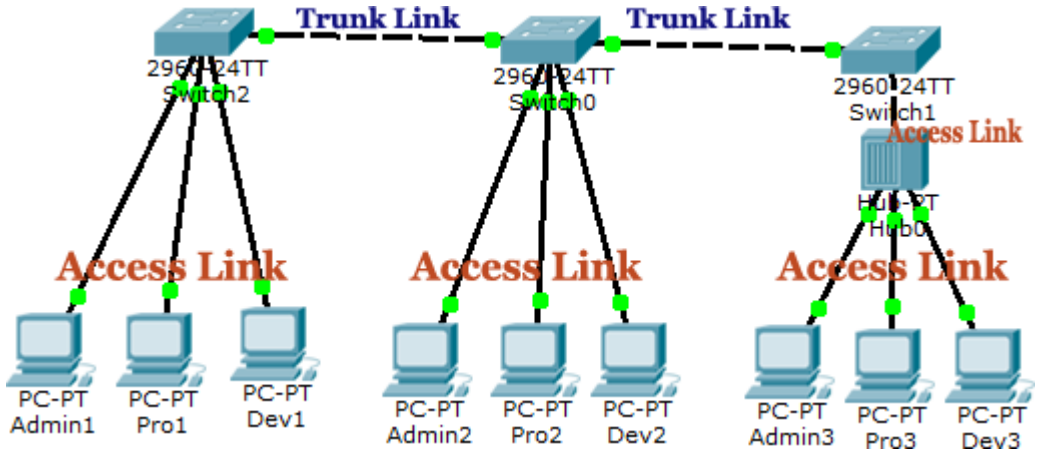

Fig-5: Combine Access & Trunk Link

Communication in VLAN

Hosts in the same VLAN can communicate normally even they are connecting to 2 or more different switches. When using multiple VLANs in networks that have multiple interconnected switches, we need to use VLAN Trunking between the switches. With VLAN trunking, the switches tag each frame sent between switches so that the receiving switch knows which VLAN the frame belongs to. This tag is known as a VLAN ID. A VLAN ID is a number which is used to identify a VLAN.

3. Introduction to InterVLAN Routing:

To enable different VLANs to communicate with each other need a router. Without a router, the computers within each VLAN can communicate with each other but not with any other computers in another VLAN. For example, we need a router to transfer file from LEADER to TECH. This is called “inter-VLAN routing”.

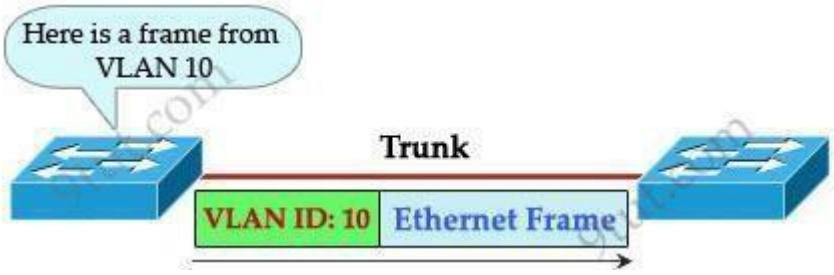

Fig-6: Trunk connection & their frame

The tag is only added and removed by the switches when frames are sent out on the trunk links. Hosts don't know about this tag because it is added on the first switch and removed on the last switch. The picture below describes the process of a frame sent from PC A to PC B.

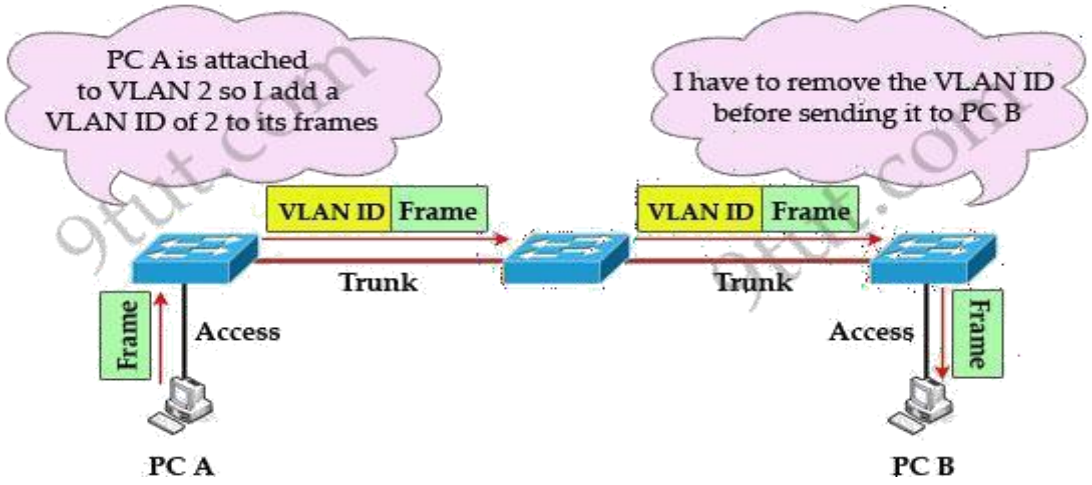

Fig-7: Connection of VLAN ID

Note: Trunk link does not belong to a specific VLAN; rather it is a conduit for VLANs between switches and routers.

To allow inter-VLAN routing you need to configure trunking on the link between router and switch. Therefore, in our example we need to configure 3 links as "trunk".

Cisco switches support two different trunking protocols, Inter-Switch Link (ISL) and IEEE 802.1q. Cisco created ISL before the IEEE standardized trunking protocol. Because ISL is Cisco proprietary, it can be used only between two Cisco switches. 802.1q is usually used in practical.

In 802.1q encapsulation, there is a concept called native VLAN that was created for backward compatibility with old devices that don't support VLANs. Native VLAN works as follows:

1. Frame belonging to the native VLAN is not tagged when sent out on the trunk links.
2. Frame received untagged on the trunk link is set to the native VLAN.

So, if an old switch doesn't support VLAN it can still "understand" that frame and continue sending it (without dropping it).

Every port belongs to at least one VLAN. If a switch receives untagged frames on a trunkport, they are assumed to be part of the native VLAN. By default, VLAN 1 is the default and native VLAN but this can

be changed on a per port basis by configuration.

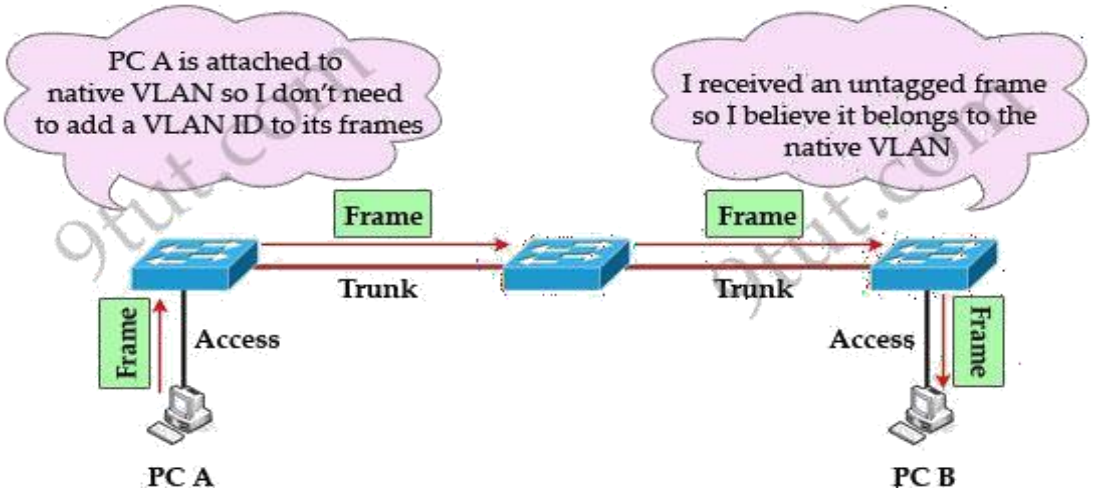

Fig-8: Understanding of the VLAN frame

4. Configuration of VLAN:

Creating Vlan

Step 1: Enter privileged EXEC mode
Switch>enable

Step 2: Enter global configuration mode.
Switch#config terminal

Step 3: Create VLAN
Switch(config)#vlan X (X can be any natural number)

Step 4: Give name to VLAN
Switch(config-vlan)#name XYZ (Name of VLAN)
Notice that we don't need to exit out of "vlan mode" to create another VLAN.

Set VLAN Membership
Assign VLAN to each port:

Step 5: Enter interface configuration mode.
Switch(config)#interface type port(int fa0/1)

Step 6: Set the mode of port as trunk or access
Switch(config-if) #switchport mode access/trunk (access when pc-switch else trunk)

Step 7: If port is in access mode, assign a VLAN to the port.
Switch(config-if) #switchport access vlan-number
Notice that for port connecting to host we must configure it as access port

5. Configuration of InterVLAN Routing:

Step 8: Enter interface configuration mode.
Router(config)#interface *type port*

Step 9: Enter sub-interface configuration mode.
Router(config-if)#interface *type port.subport*

Step 10. Set the ip address of the subinterface.
Router(config-subif)#ip address X.X.X.X Y.Y.Y.Y

Step 11. Set the encapsulation type and vlan allowed on sub-interface.
Router(config-subif)# encapsulation dot1q*vlan number*

6. Lab Exercise:

Task 1

Implement the given topology of figure A on cisco packet tracer. Perform the following task:

1. Create different vlan members on the given switches
2. Create Trunk and Access link connection
3. Create the intervlan routing on the given router

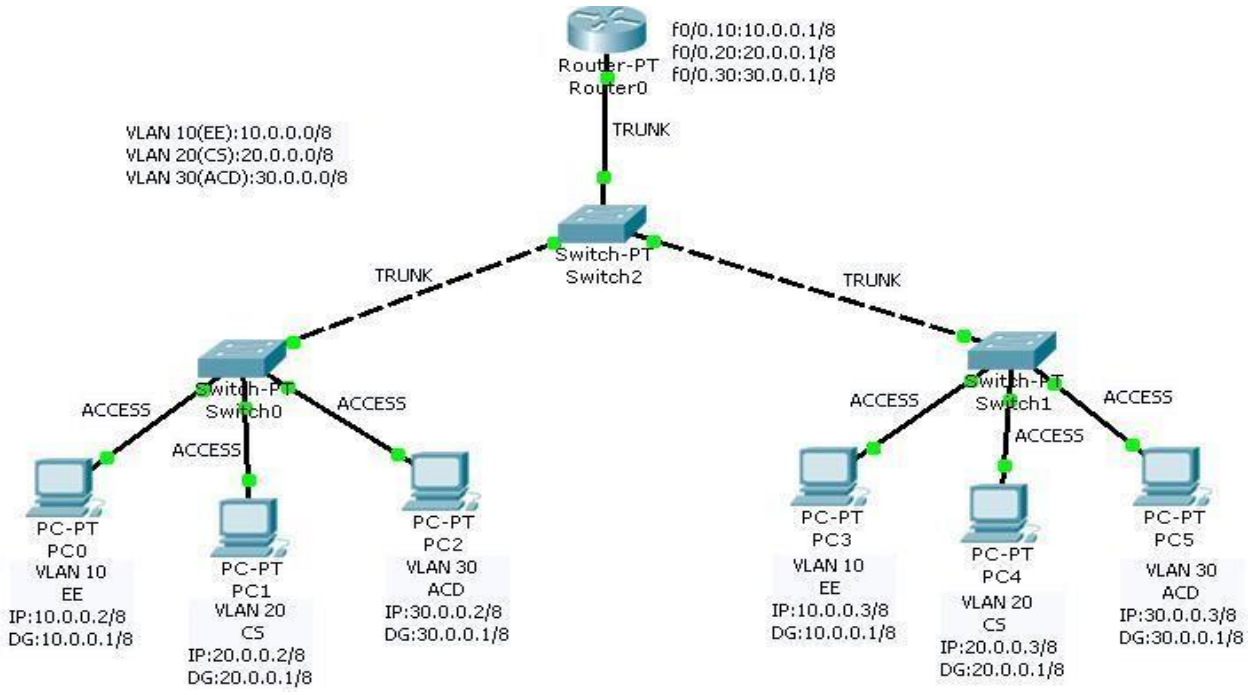

Fig-9: Topology for Task 1

Task 2

Implement the given topology of figure B on cisco packet tracer. Perform the following task:

1. Do perform Vlans and InterVlan Routing.
2. Dynamic Ips should be assign to all the end devices.
3. The default gateways should be like XX.XX.1.1, XX.XX.2.1 and so on where XX.XX will be your roll number like 3879 and it will be 38.79.1.1,38.79.2.1 and so on.

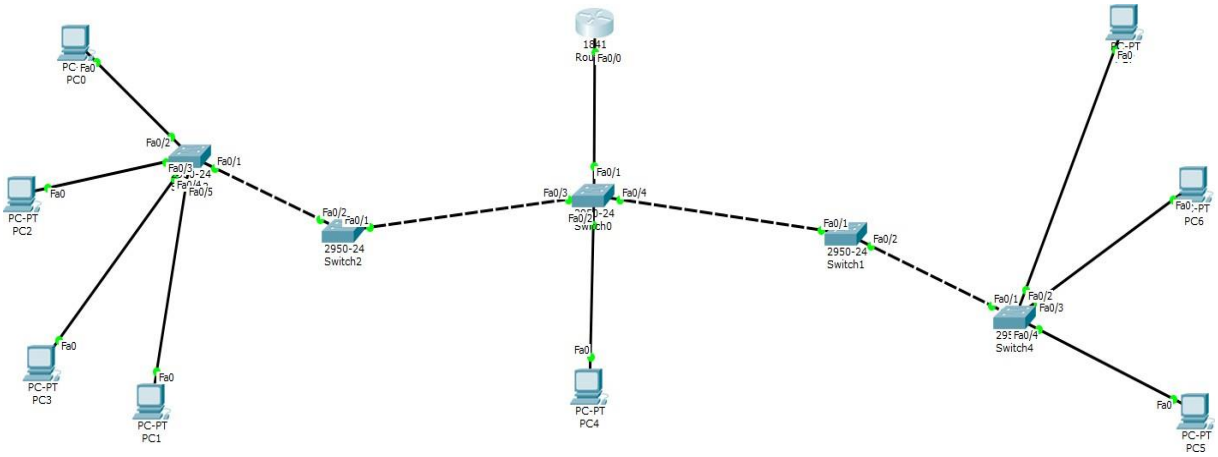

Fig-10: Topology for Task 2