CSE 4412 [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
- Understand and implement VLSM

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

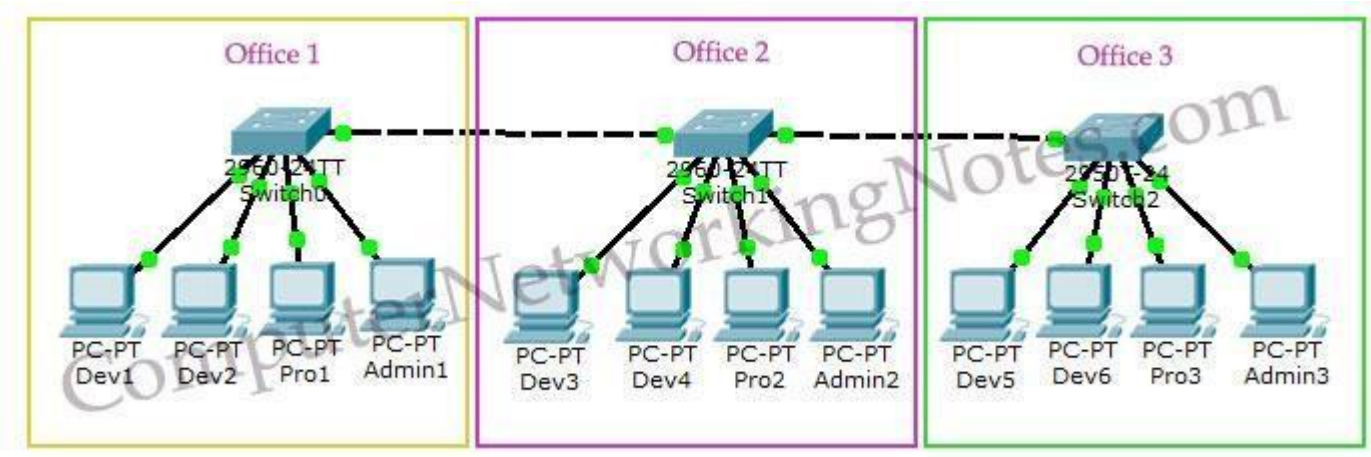
Device management is easier with VLANs. Since VLANs are a logical approach, a device can be located anywhere in the switched network and still belong to the same broadcast domain. We can move a user from one switch to another switch in same network while keeping his original VLAN. For example, a company 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.

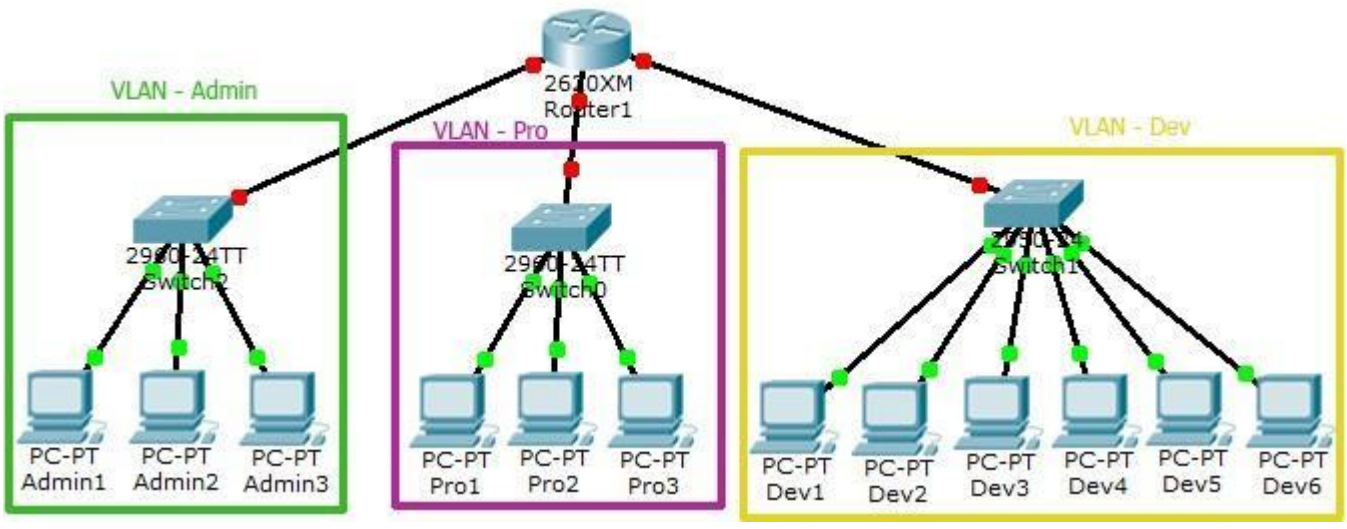
- Development department has six computers.
- Production department has three computers.
- Administration department also has three computers.
- Each office has two PCs from development department and one from both production and administration department.
- Administration and production department have 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

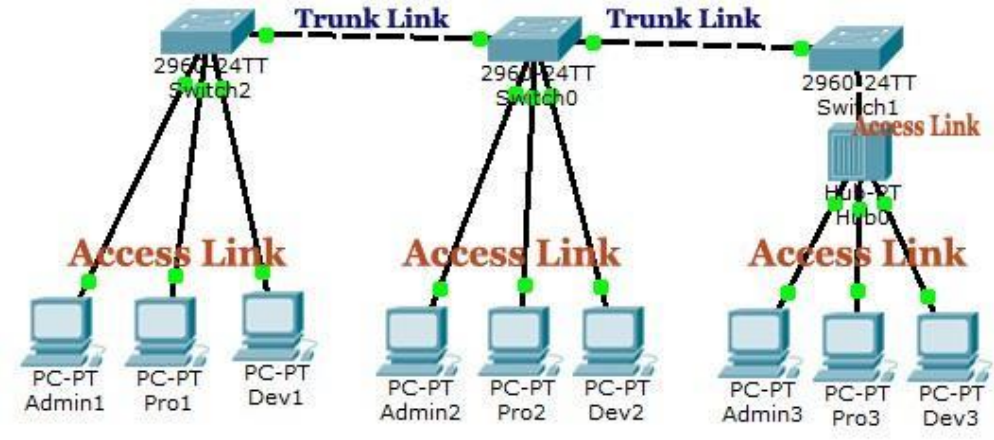
Access link

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.



Lab Demo (with Inter-VLAN routing)

I. At first, configure 2 VLANs with VLAN ID 10, 20 inside the switch and assign appropriate names.

```
S1(config)# vlan 10

S1(config)# name [VLAN_name]

S1(config-vlan)# exit

S1(config)# vlan 20

S1(config)# name [VLAN_name]

S1(config-vlan)# exit
```

```
S1(config)# exit

S1# show vlan
```

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

```
S1(config)# interface Fast-Ethernet 0/1
S1(config-if)# switchport mode access
```

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

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

This command assigns VLAN 10 access ports.

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

Do this for all the ports!

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 whats a trunk link).

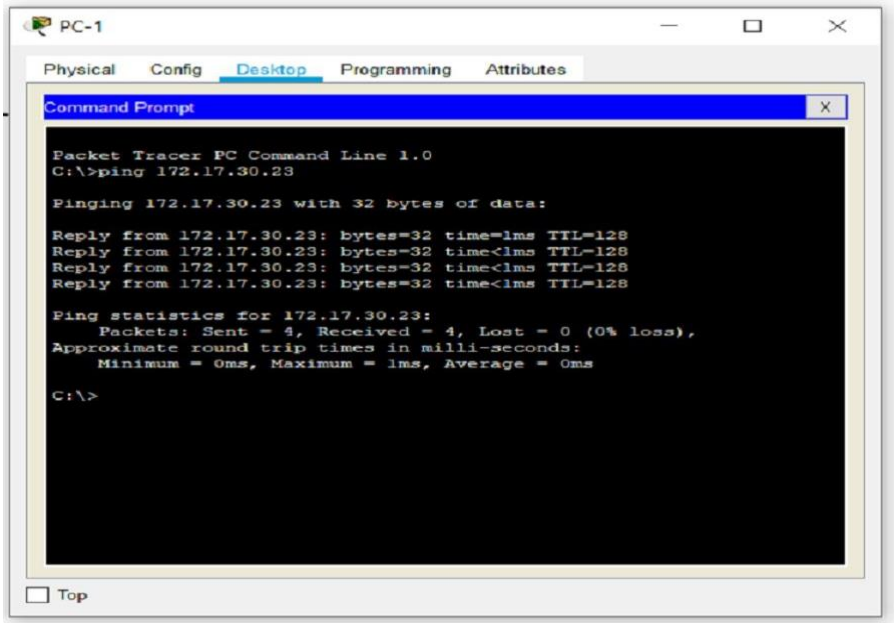
```
S1(config-if)# switchport trunk allowed vlan all
```

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. Setup the PCs with appropriate IP and subnet masks:

IV. Verify the routing is working properly by pinging *from different PCs*.



V. Now, we can reach the PCs of the VLAN but not the other VLANs. So, we need Inter-VLAN routing.

First we need to keep the router running:

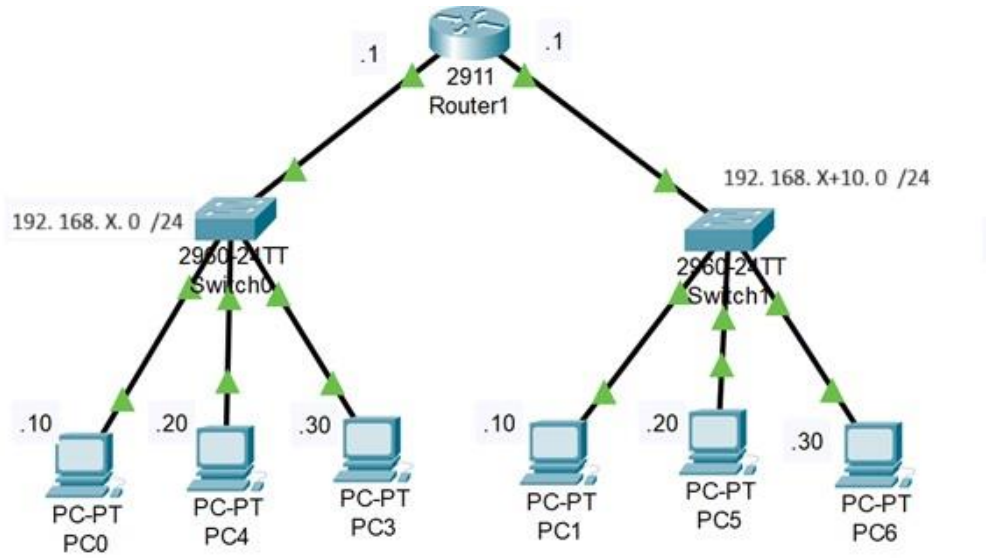
```
Router(config)#int g0/0

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

Now, we need to assign virtual VLAN to the router interface:

```
Router(config)#int g0/0.10

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip address 192.168.10.1 255.255.255.128

Router(config-subif)#int g0/0.20

Router(config-subif)#encapsulation dot1q 20

Router(config-subif)#ip address 192.168.10.129 255.255.255.128

Router(config-subif)#exit
```

VI. After all these are done, we can now ping from one PC to another.

3. Tasks:



Here, X = 10 + last 2 digits of your Student ID

I. Now, you are quickly running out because of immense network expansion. You need to change your approach of how you assign new networks. You find the idea of subnets. From now on, you decide to allow **Y hosts per network.** Using this, add another network to the existing topology (with

appropriate subnet mask) to ensure maximum utilization. Connect atleast 1 PC to that network and ping to other PCs.

Y = Max(17, Last 2 digits of your student ID)

II. You will implement VLAN routing using the network **192.167.[last 2 digits of your ID]+10.0** . VLAN 10, 20 and 30 are Students, Teachers and Admin respectively. Establish the VLAN so that none from one profession can communicate with another. Use labels to show the IPs of different PCs. (See figure for reference)