

# 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**

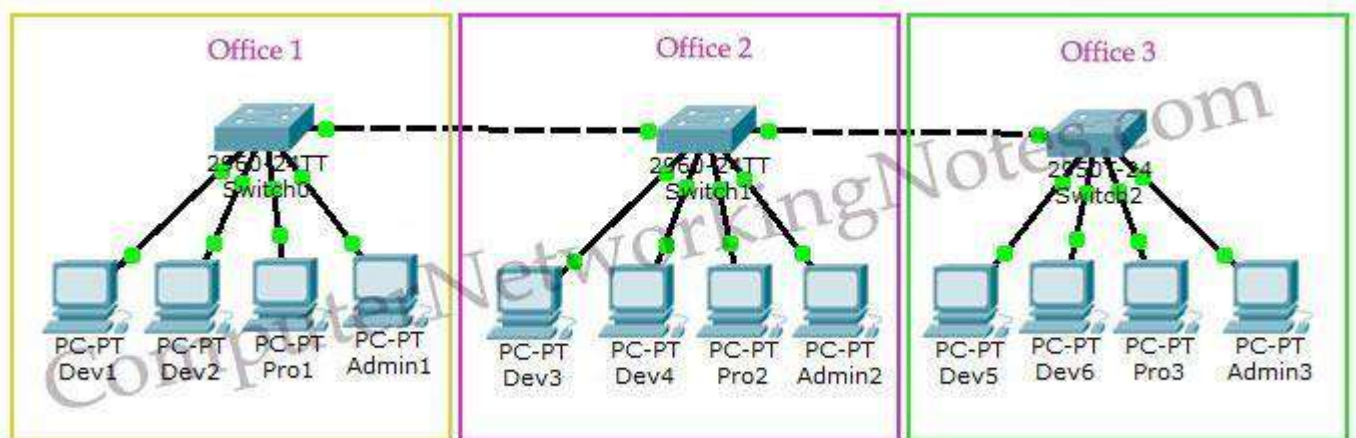
Device management is easier with VLANs. Since VLANs are a logical approach, a device can be located anywhere in the switched network and still belong to the same broadcast domain. We can move a user from one switch to another switch in same network while keeping his original VLAN. For example, a company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

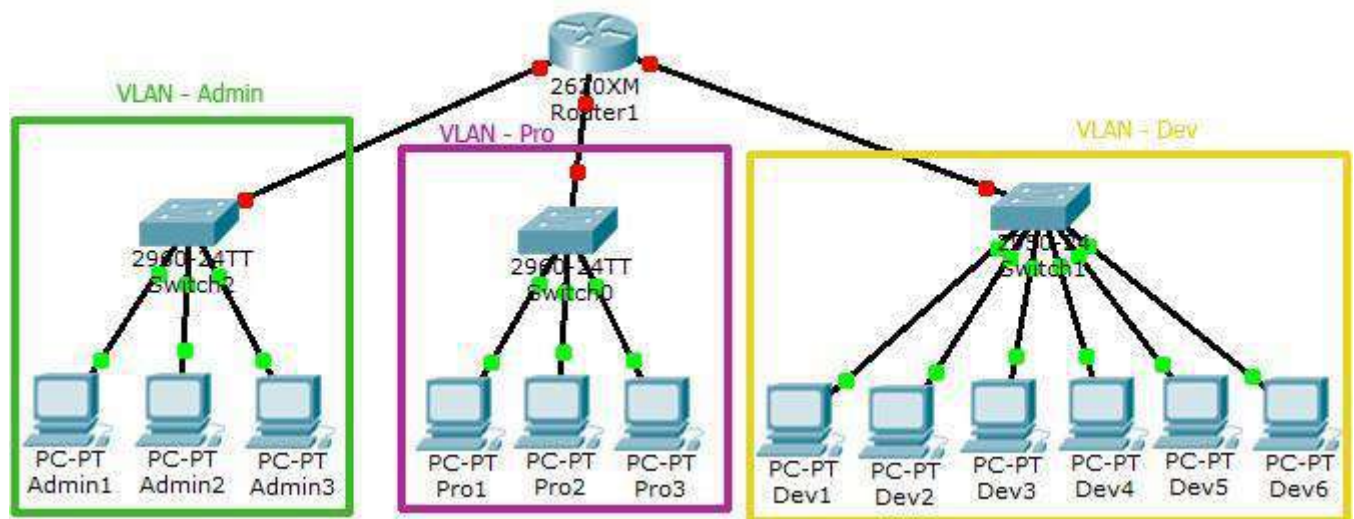
- Development department has six computers.
- Production department has three computers.
- Administration department also has three computers.
- Each office has two PCs from development department and one from both production and administration department.
- Administration and production department have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

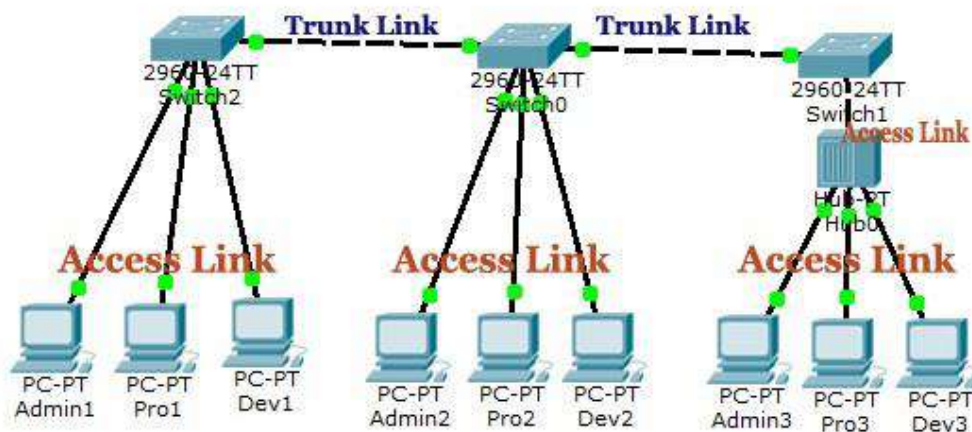
### Access link

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.

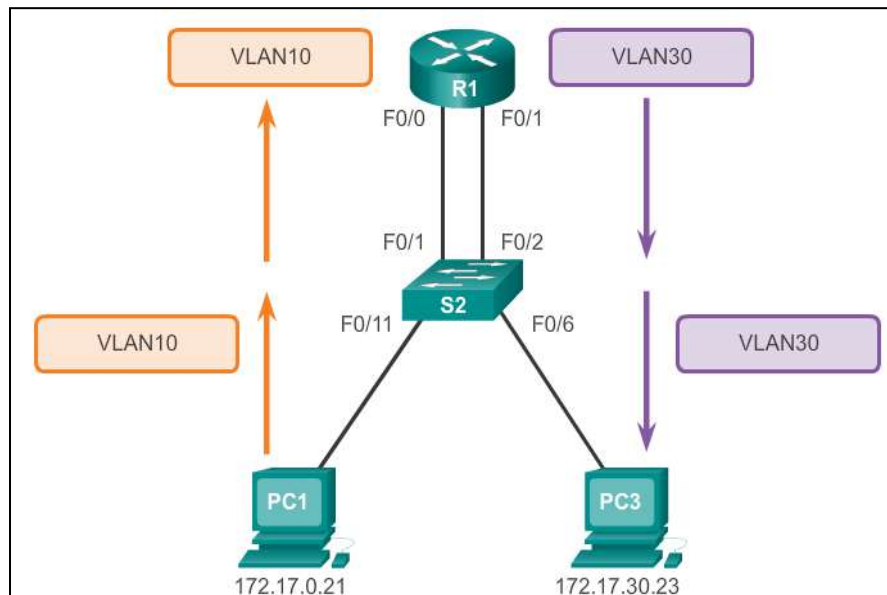


### Inter-VLAN Routing:

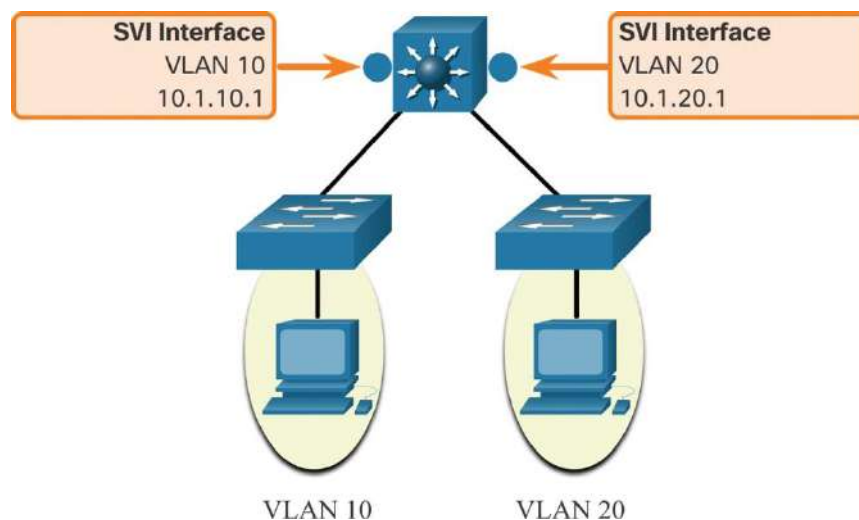
Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another, using a layer 3 device. Two common approaches to inter-VLAN routing are, router-on-a stick approach and layer 3 switch using switch virtual interfaces (SVIs).

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.



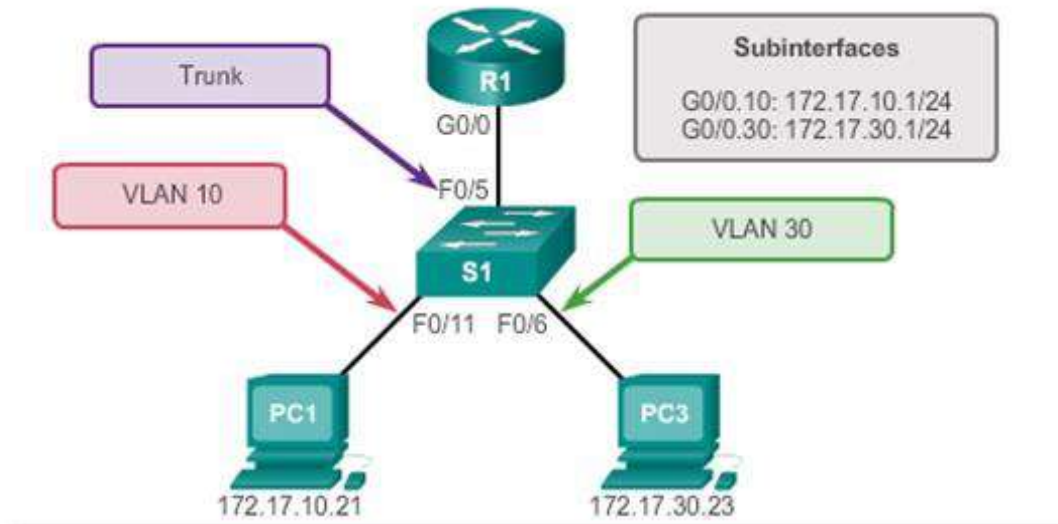
A layer 3 switch is also known as Multi Layer Switch (MLS) as it operates both in layer 2 and 3. A switch virtual interface or SVI is created for each VLAN i.e. one SVI for one VLAN. The function of a SVI is the same as the router interface in case of router-on-a-stick approach. It processes the incoming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

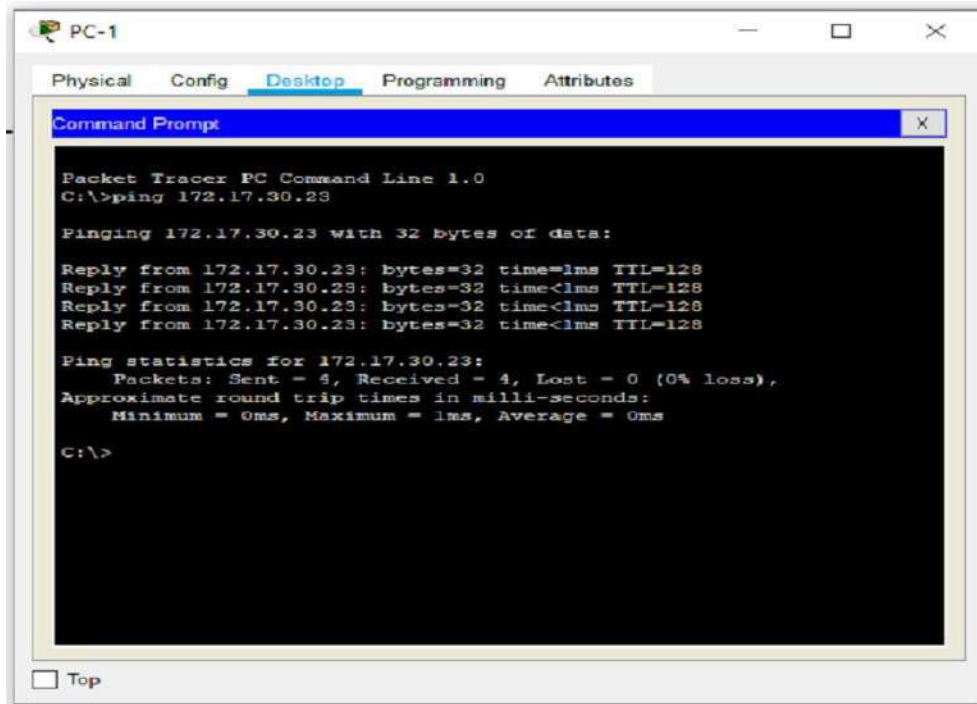
**IP Address:** 172.17.30.23

**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 PC Command Line window for PC-1. The window has tabs for Physical, Config, Desktop, Programming, and Attributes, with Desktop selected. The Command Prompt shows the following text:

```
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:\>
```

At the bottom left of the window, there is a checkbox labeled "Top" which is currently unchecked.

## 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.