A.HARSHITHA

2320030398

EXP: 5 Configuration of Encapsulation dot 1Q using cisco packet tracer

Need for VLANs and Dot1Q Encapsulation

1. Network Segmentation:

- VLANs allow the segmentation of a larger network into smaller, isolated segments. Each segment, or VLAN, can be assigned to a different department or group within an organization, reducing broadcast traffic and improving performance.

2. Security:

- By isolating sensitive data within specific VLANs, administrators can enhance network security. Unauthorized users from one VLAN cannot access resources in another VLAN without proper routing and access control policies.

3. Flexibility and Scalability:

- VLANs provide the flexibility to add or move devices within the network without requiring physical changes to the infrastructure. As the organization grows, new VLANs can be created to accommodate additional departments or user groups.

4. Traffic Management:

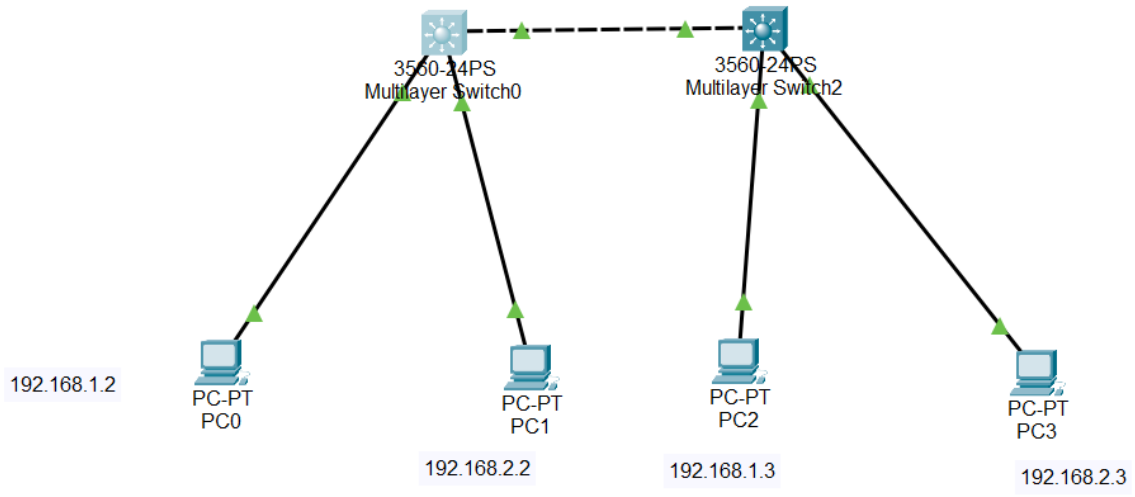
- VLANs help in managing network traffic efficiently by limiting the scope of broadcast domains. This reduces the amount of unnecessary traffic and improves the overall network performance.

5. Simplified Network Management:

- VLANs allow for easier network management and troubleshooting. Administrators can manage the network logically rather than physically, simplifying configuration and maintenance tasks.

6. Inter-VLAN Routing:

- Dot1Q encapsulation is used on trunk links to allow multiple VLANs to traverse a single physical link between switches. This enables communication between different VLANs through a router or a Layer 3 switch, ensuring network resources are accessible across the entire organization.



To configure VLANs and trunking with IEEE 802.1Q encapsulation on a Cisco Catalyst 3560-24TT switch, follow these steps:

Step-by-Step Configuration

Step 1: Set Up Your Network

1. **Open Cisco Packet Tracer** and create a new workspace.
2. **Add Devices**:
   - Drag and drop a 3560 switch and at least two PCs into the workspace.
   - Connect the PCs to the switch using copper straight-through cables.

Step 2: Configure VLANs on the Switch

1. **Access the Switch CLI**:
   - Click on the switch.
   - Go to the CLI tab.

1. **Enter Global Configuration Mode**:

```
enable
configure terminal
```

2. **Create VLANs**:

```
vlan 10
name Sales
```

```
exit
vlan 20
name Product
exit
```

3. **Assign Ports to VLANs**:
   - Assign FastEthernet 0/1 to VLAN 10:

     ```
     plaintext
     Copy code
     interface FastEthernet0/1
     switchport mode access
     switchport access vlan 10
     exit
     ```

   - Assign FastEthernet 0/2 to VLAN 20:

     ```
     interface FastEthernet0/2
     switchport mode access
     switchport access vlan 20
     exit
     ```

Step 3: Configure Trunk Port on the Switch

1. **Configure Trunk on the Switch**:

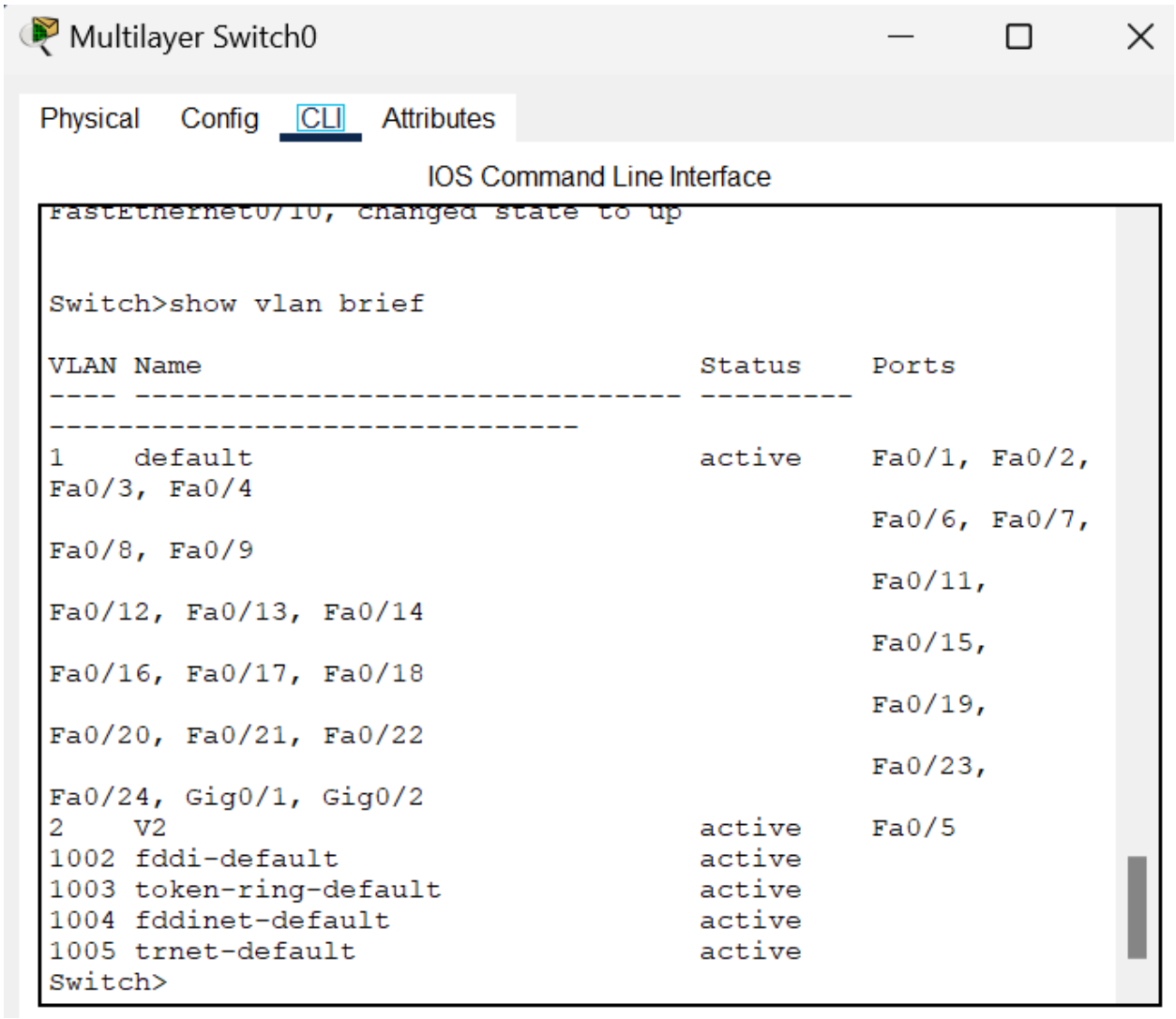
```
interface FastEthernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

Step 4: Assign IP Addresses to PCs

1. **Configure IP Address on PC1**:
   - Click on PC1.
   - Go to the Desktop tab and click on IP Configuration.
   - Assign IP Address: 192.168.10.2
   - Subnet Mask: 255.255.255.0
   - Gateway (if needed): 192.168.10.1
2. **Configure IP Address on PC2**:
   - Click on PC2.
   - Go to the Desktop tab and click on IP Configuration.
   - Assign IP Address: 192.168.20.2
   - Subnet Mask: 255.255.255.0
   - Gateway (if needed): 192.168.20.1

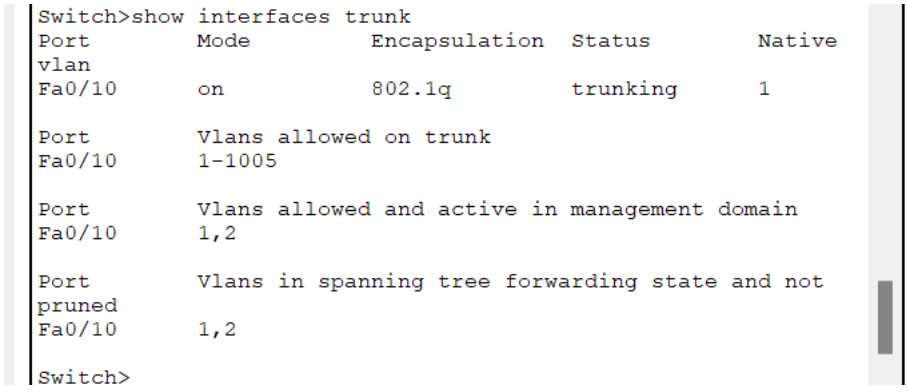
Step 5: Verify Configuration

1. **Check VLANs on the Switch**:

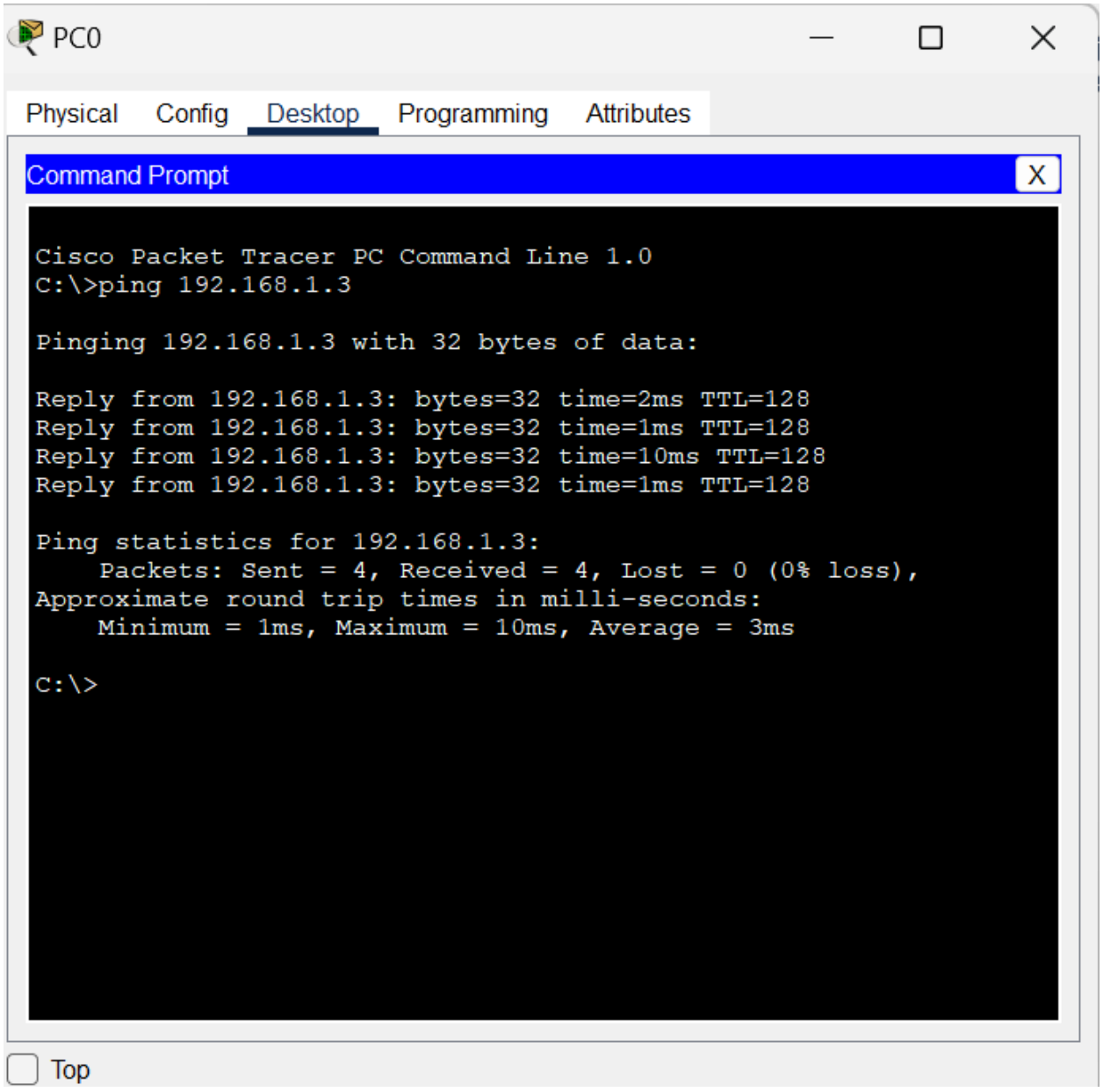


2. **Check Trunk Ports**:

`show interfaces trunk`



3. **Test Connectivity**:
    - Go to the command prompt on PC1 and ping PC2 to ensure they can communicate if routing is correctly set up.



1. Ping 192.168.1.2 to 192.168.12.2
2. Ping 192.168.1.3 to 192.168.2.3
3. Ping 192.168.2.2 to 192.168.2.3