Domain 04 Demo 03

Implementing Network Segmentation and VLANs

Objective: To implement network segmentation and VLANs within a single physical infrastructure to enhance security and performance

Tools required: Cisco Packet Tracer and Windows Server 2022

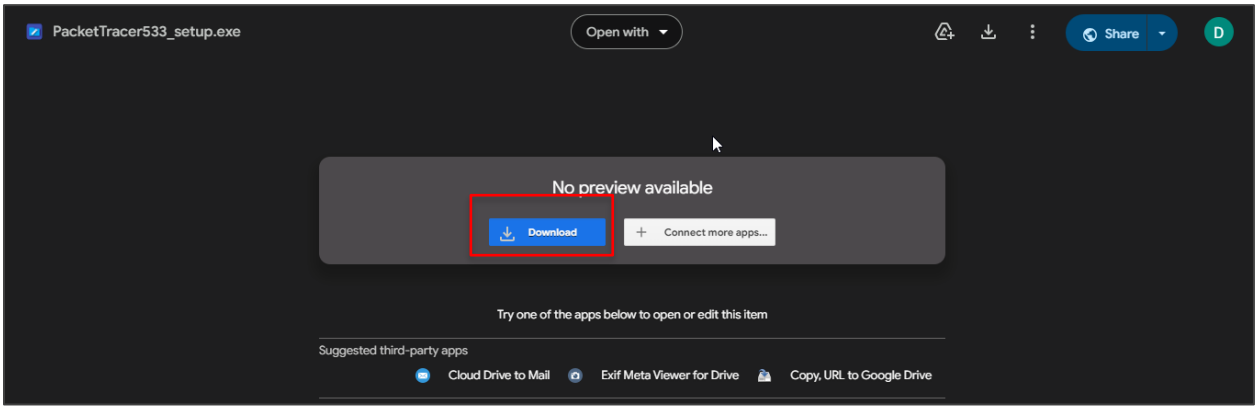
Prerequisites: None

Steps to be followed:

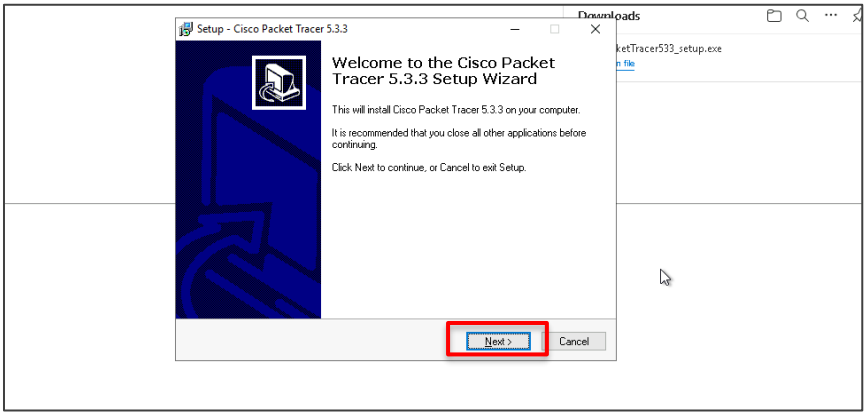
1. Install the Cisco Packet Tracer
2. Load sample network and connect devices
3. Assign IP addresses and verify initial connectivity
4. Create VLANs
5. Assign ports to VLANs and verify configuration

Step 1: Install the Cisco Packet Tracker

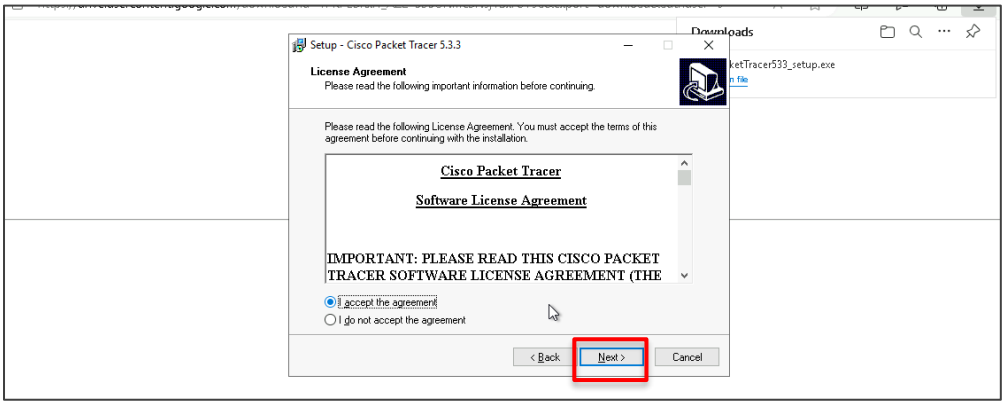
1.1 Download the Cisco Packet Tracer from the following URL:
https://drive.google.com/file/d/1PKPL5RxH_AZ2-6S6UNmc3NsjYBxrCY9a/view



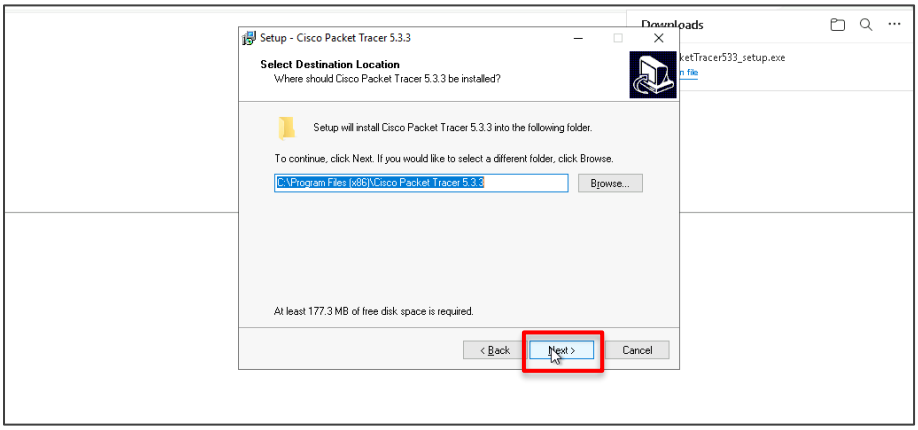
1.2 To start the installation process, run the downloaded executable file and click **Next**



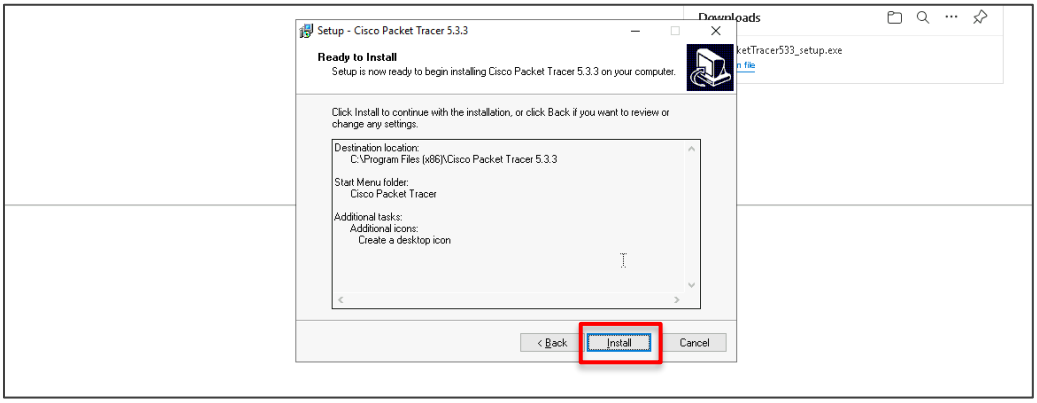
1.3 Click on **I accept the agreement** to start the installation and click on **Next**



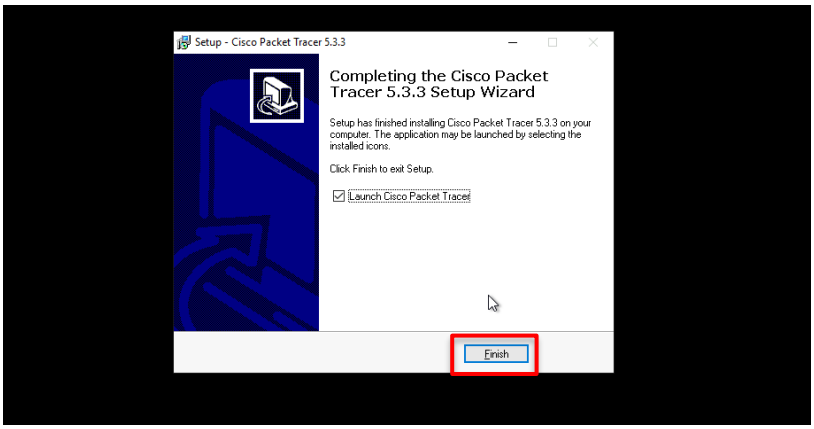
1.4 Select the destination where the Cisco Packet Tracer will be installed



1.5 Click on **Install**

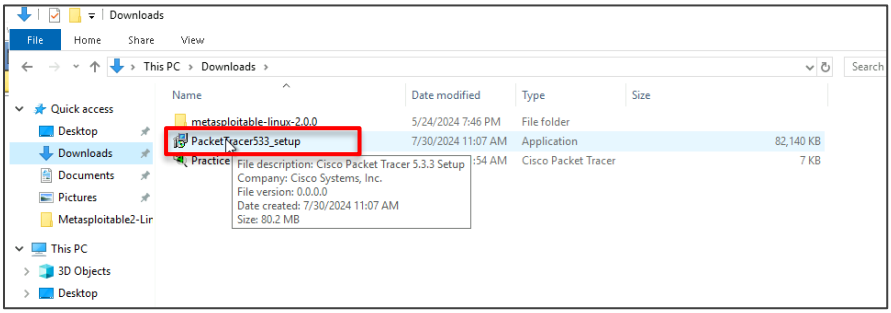


1.6 Click on the **Finish** button once the installation is complete

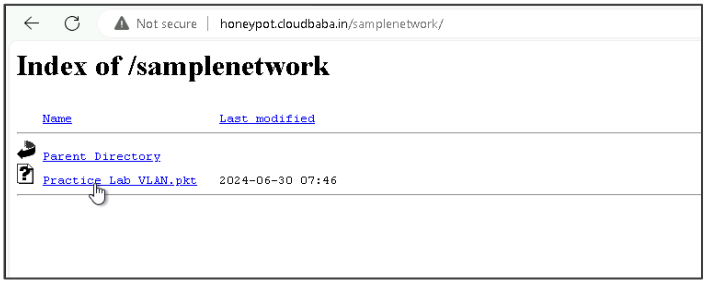


Step 2: Load sample network and connect devices

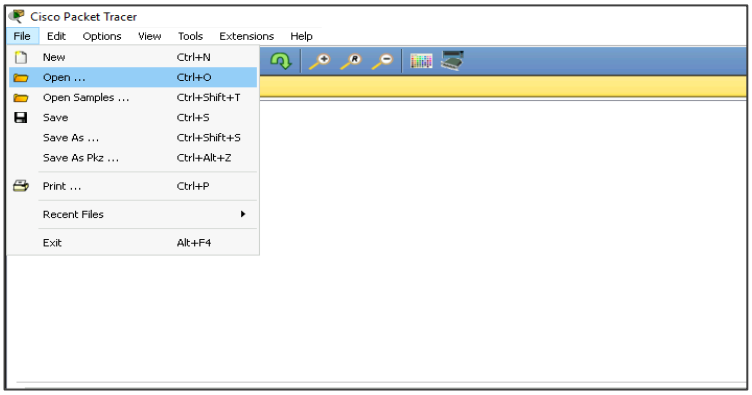
2.1 Open Cisco Packet Tracer



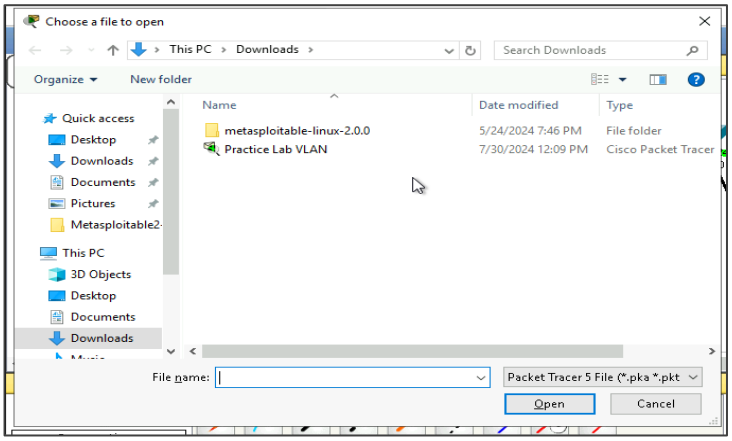
2.2 Download a sample network file from **honeypot.cloudbaba.in/samplenetwork/**



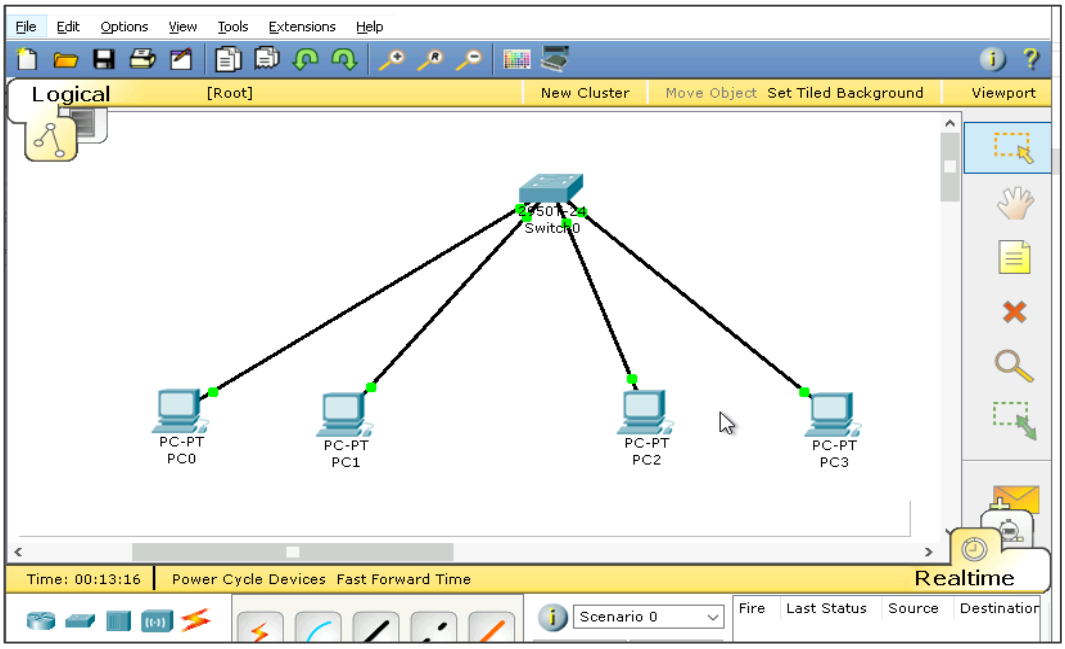
2.3 In the Cisco Packet Tracer application, go to the **File** menu and select **Open**



2.4 Locate and open the downloaded sample network file



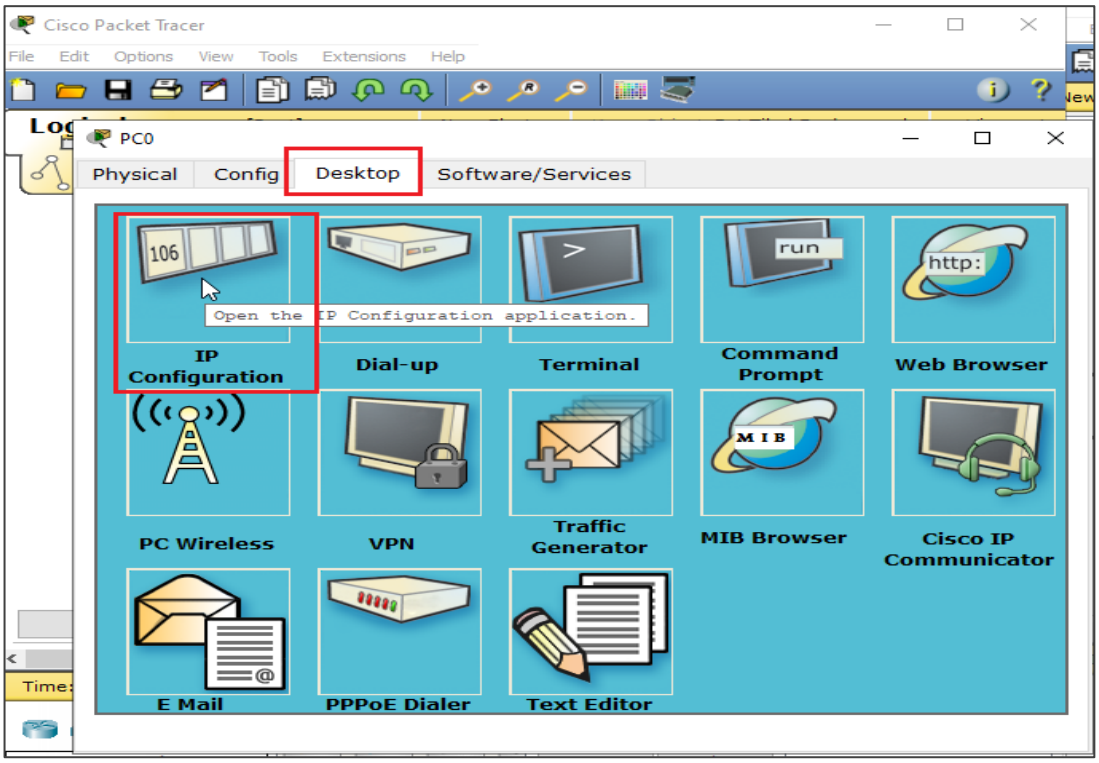
2.5 In the workspace, connect the PCs to the respective ports on the switch:
PC0 to **FastEthernet0/1,** PC1 to **FastEthernet0/2,** PC2 to **FastEthernet0/3,** PC3 to **FastEthernet0/4**



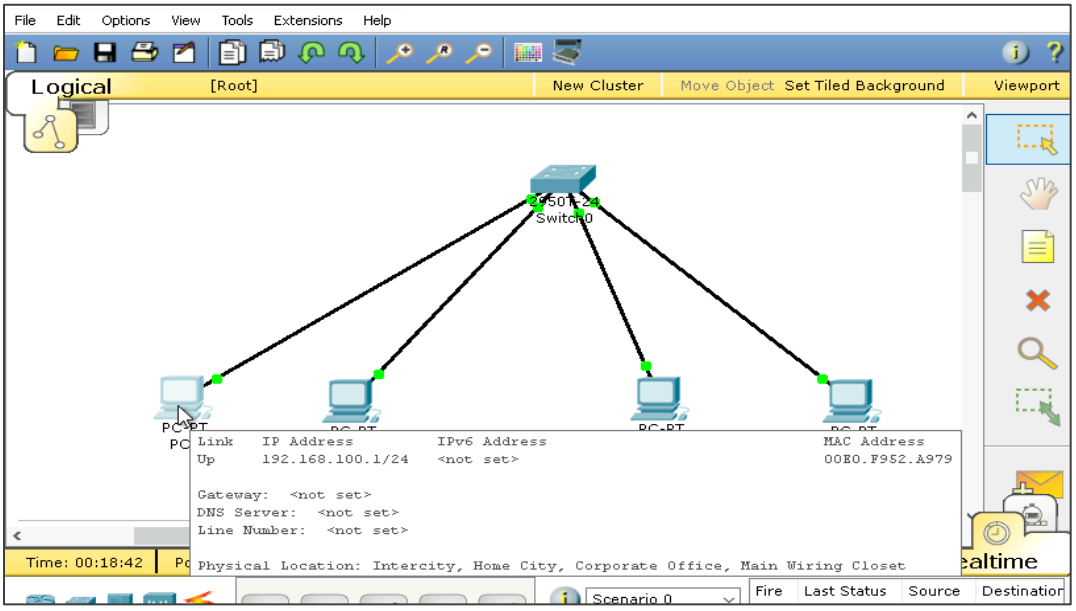
Verify that the connections are established by checking the link status indicators

Step 3: Assign IP addresses and verify initial connectivity

3.1 Click on **IP Configuration** under the **Desktop** tab



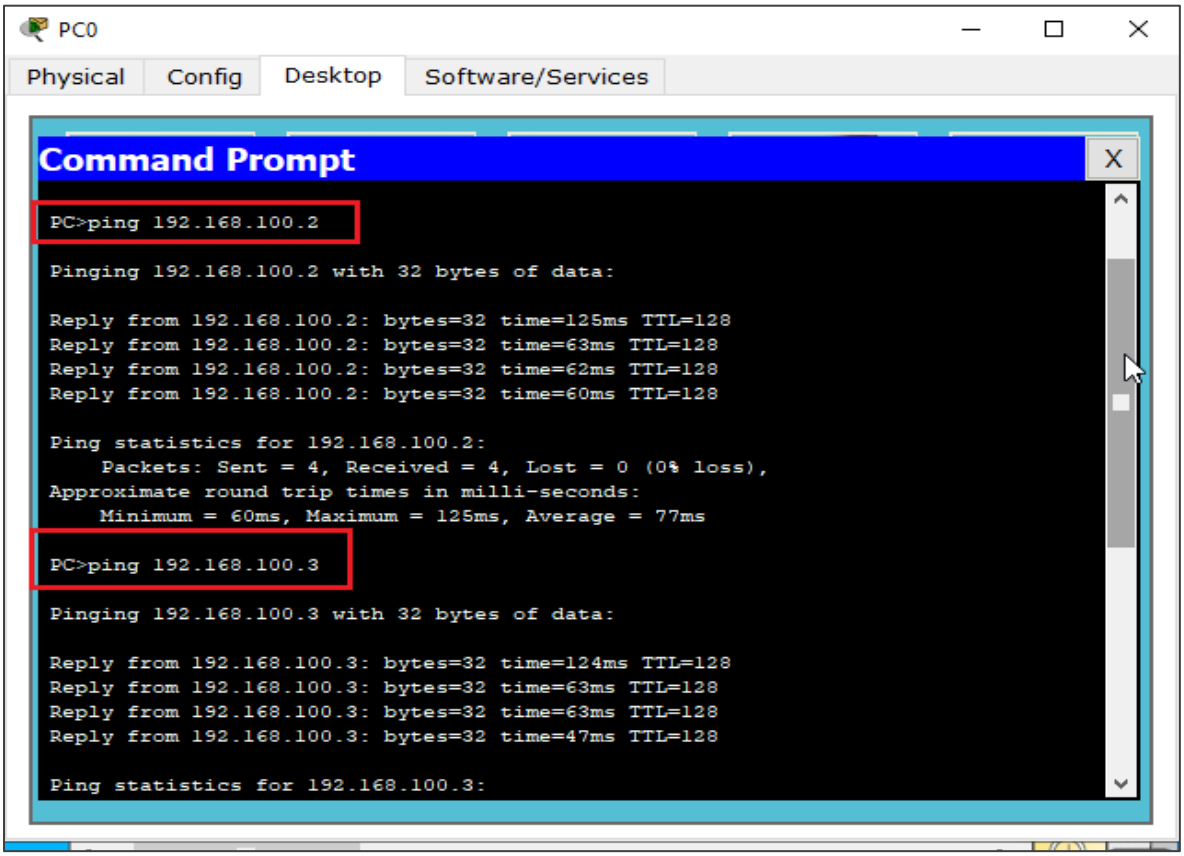
3.2 Verify connectivity details by hovering over PCs

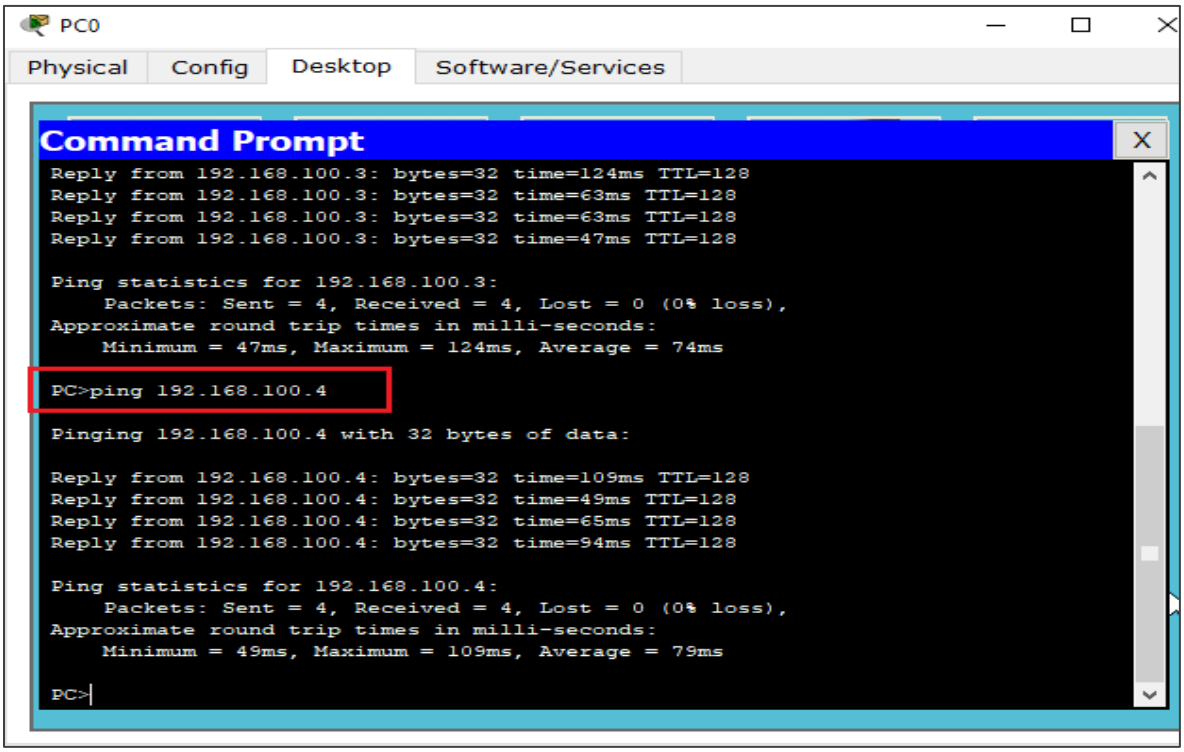


Note: Repeat the step for **PC1, PC2** and **PC3**

3.3 Open the **Command Prompt** on each PC and verify connectivity by pinging between PCs

3.4 Execute the commands **ping 192.168.100.2**, **ping 192.168.100.3**, and **ping 192.168.100.4** in PC0 to see that the networks communicate with each other

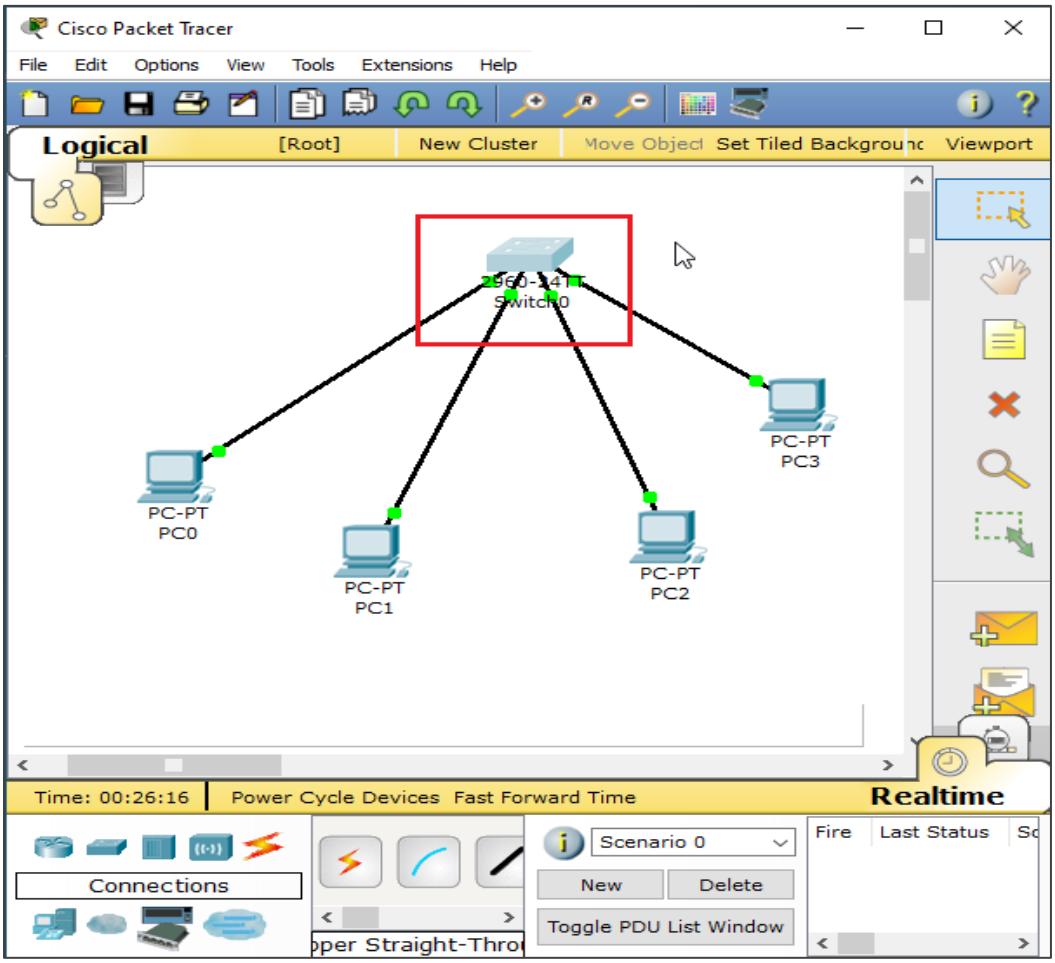




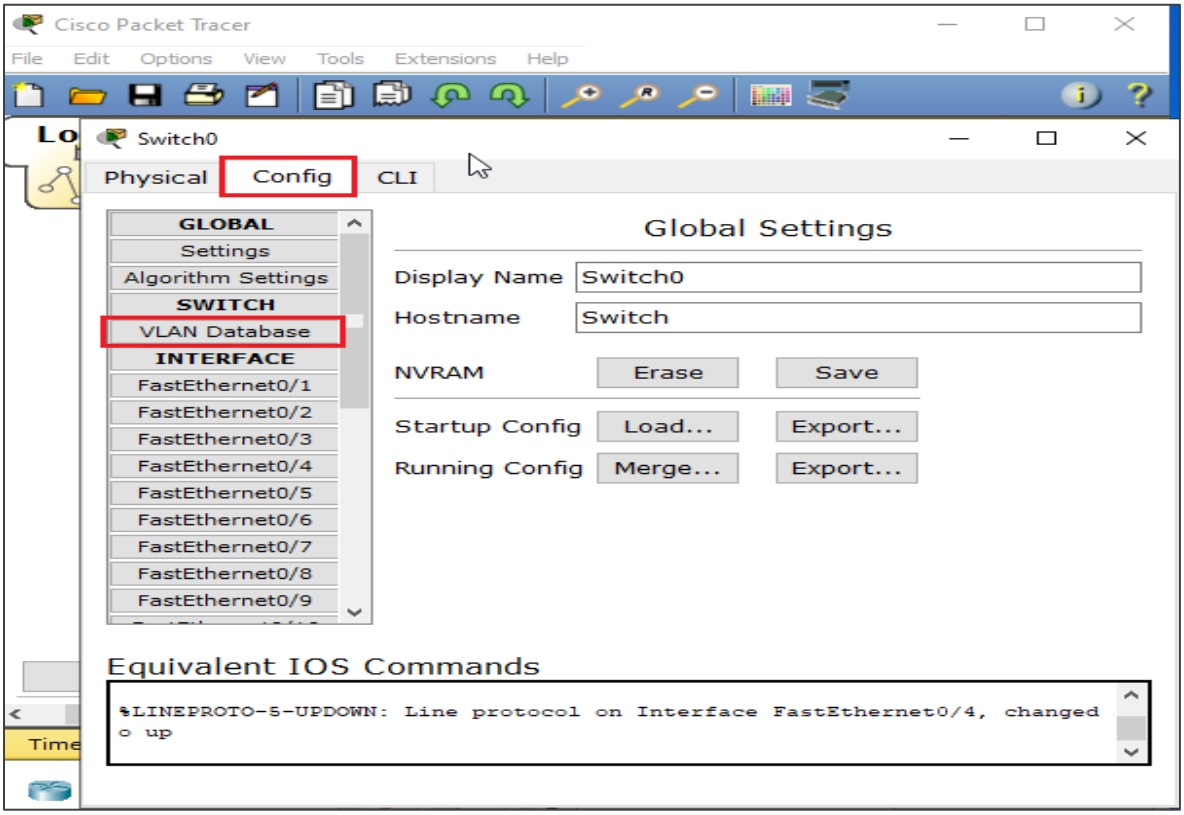
Repeat the process on **PC1, PC2,** and **PC3**

Step 4: Create VLANs

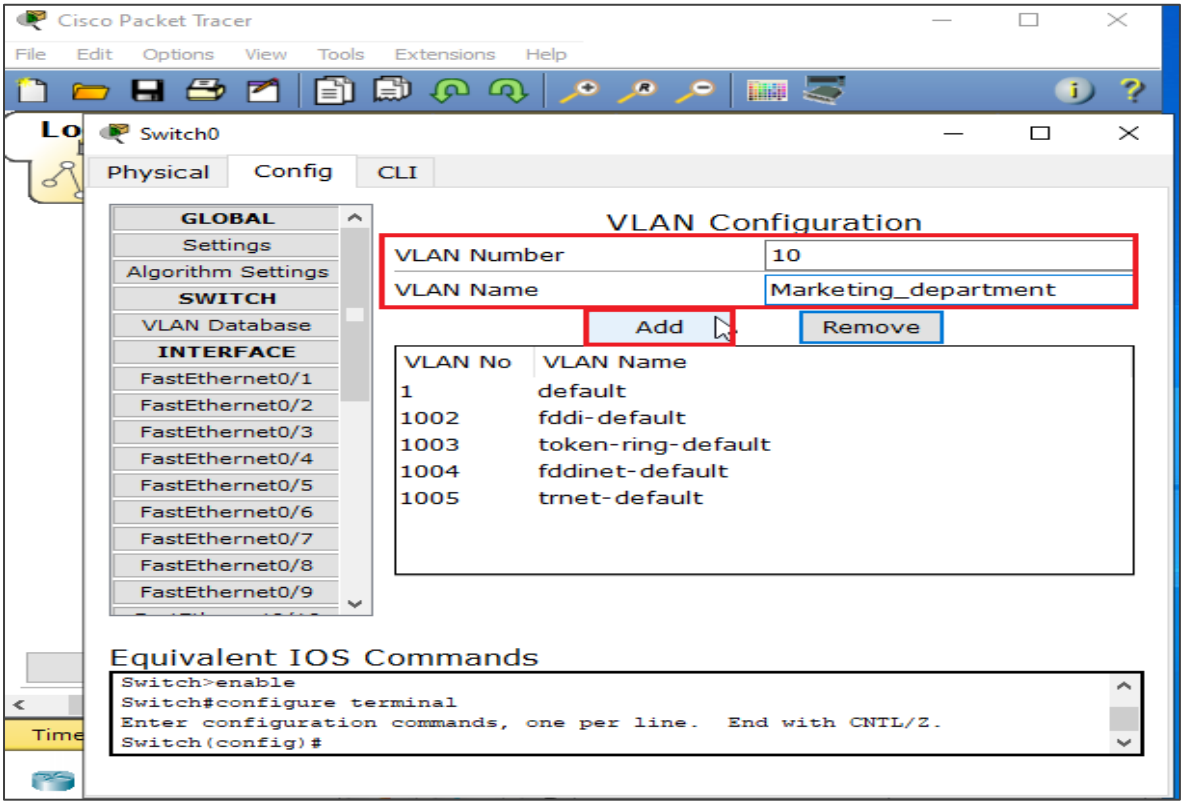
4.1 In the Cisco Packet Tracer, click the **2960 switch** in the workspace



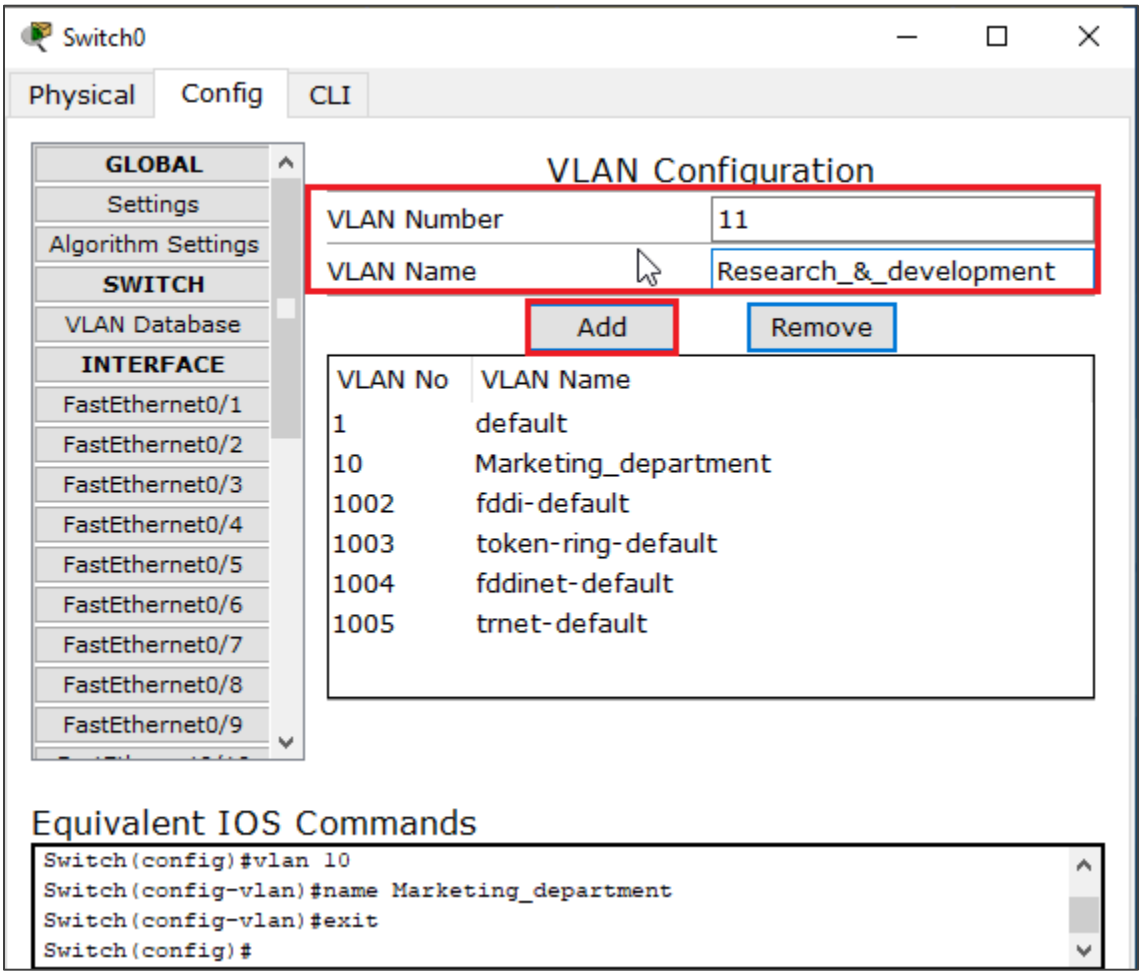
4.2 Navigate to the **Config** tab and select **VLAN Database**



4.3 Enter the value in **VLAN Number** as **10**, name it **Marketing_department**, and click **Add**

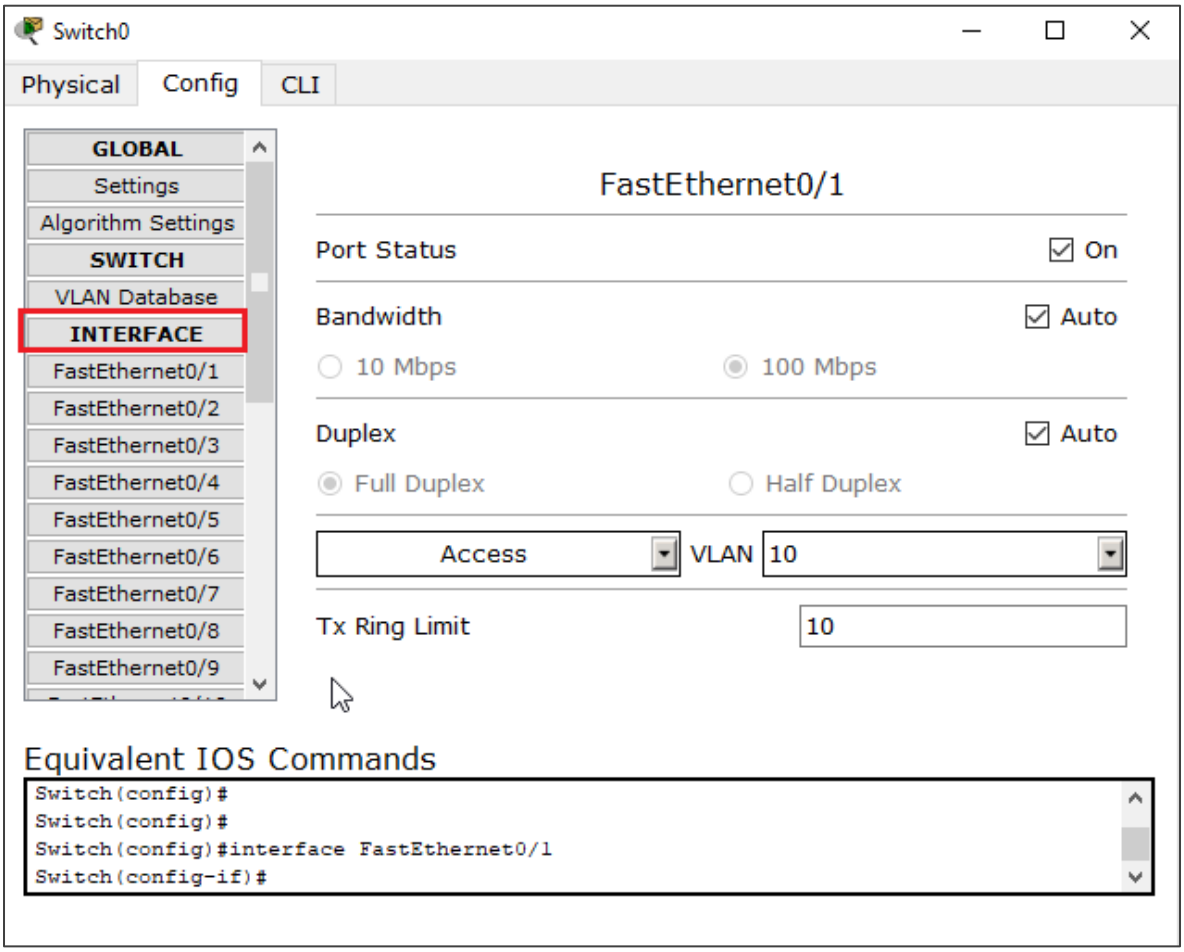


4.4 Add another VLAN configuration by setting the VLAN Number to **11**, naming it **Research_&_development**, and clicking **Add**

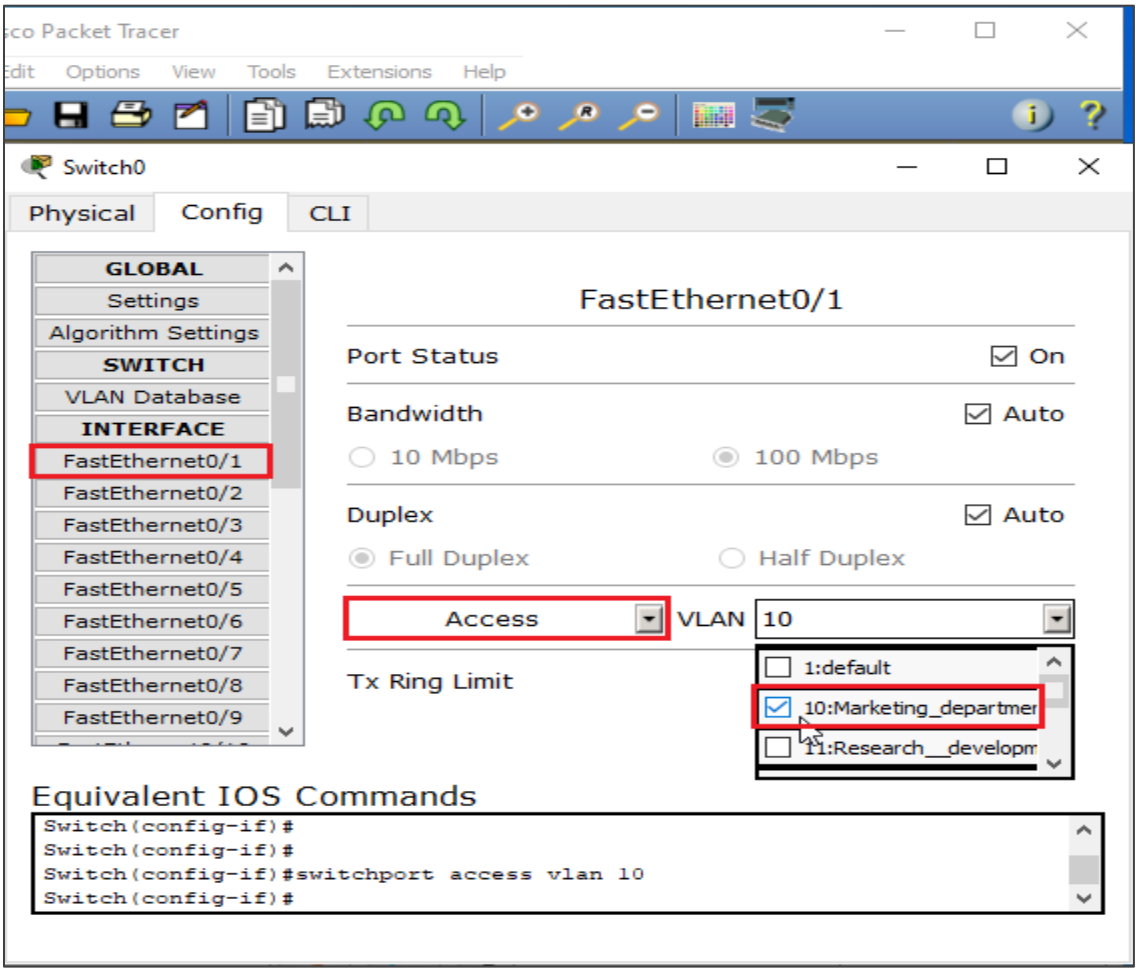


Step 5: Assign ports to VLANs and verify the configuration

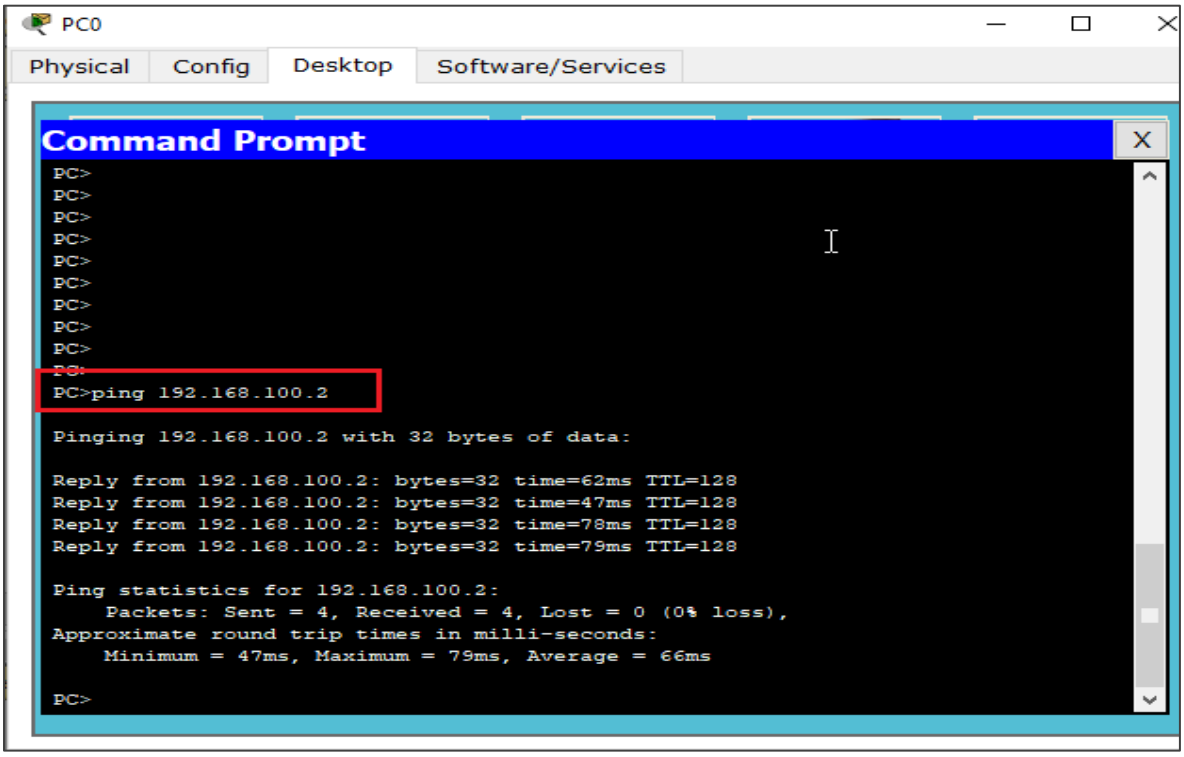
5.1 Assign FastEthernet0/1 and FastEthernet0/2 to VLAN 10 by selecting the **INTERFACE**, setting the **VLAN** field to **10** under Access, and clicking **Apply**



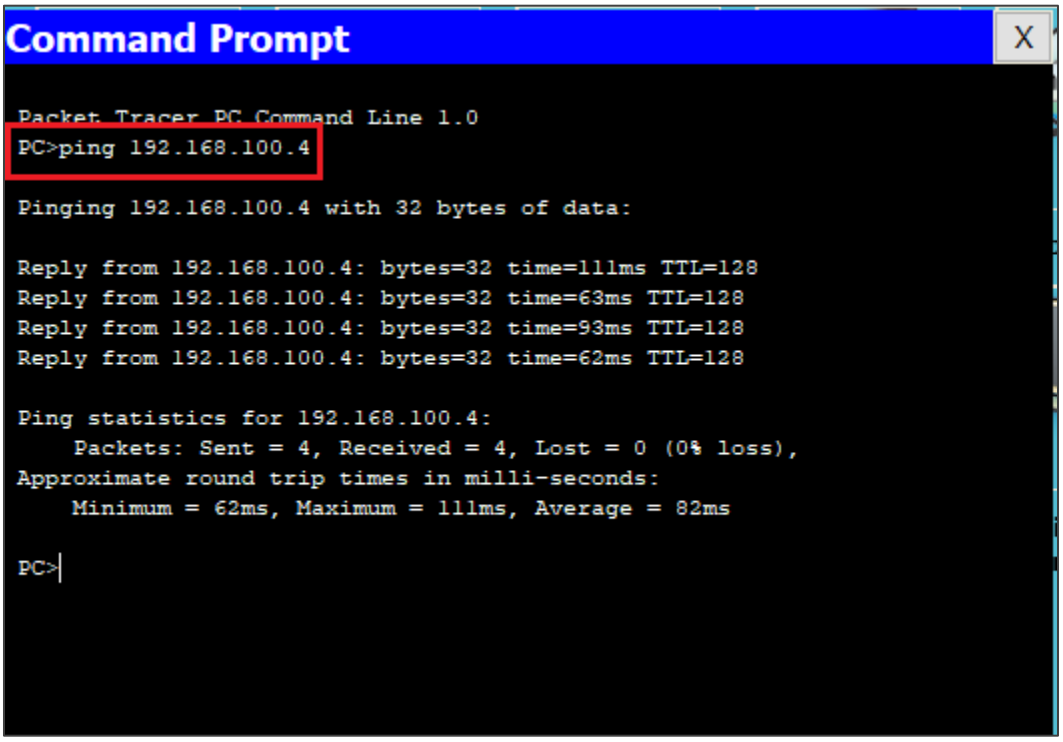
5.2 Assign FastEthernet0/3 and FastEthernet0/4 to VLAN 11 by selecting each interface, setting the VLAN field to 11 under Access, and clicking **Apply**



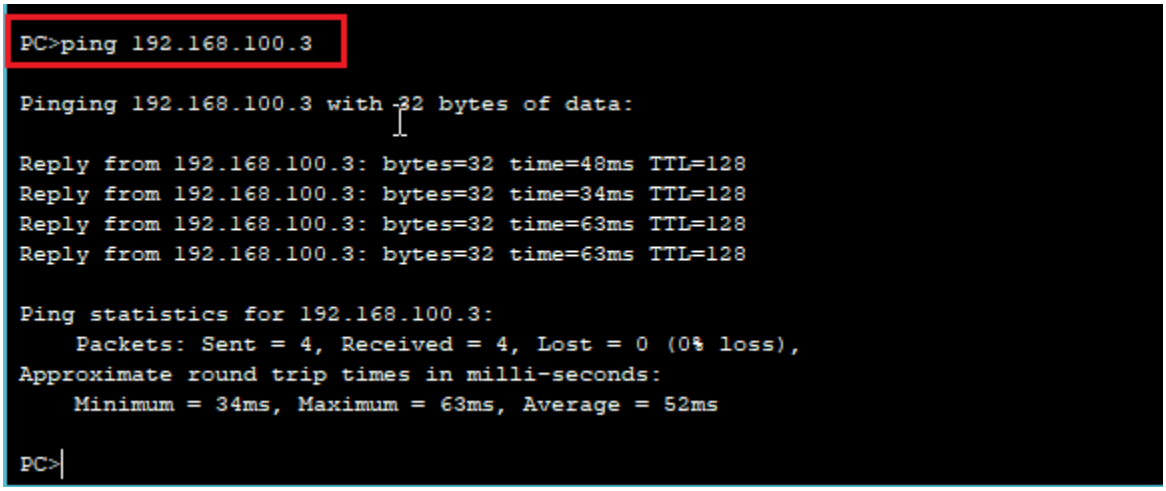
5.3 To verify communication within VLAN 10, go to the Command Prompt on PC0 and execute **ping 192.168.100.2** to check connectivity with PC1



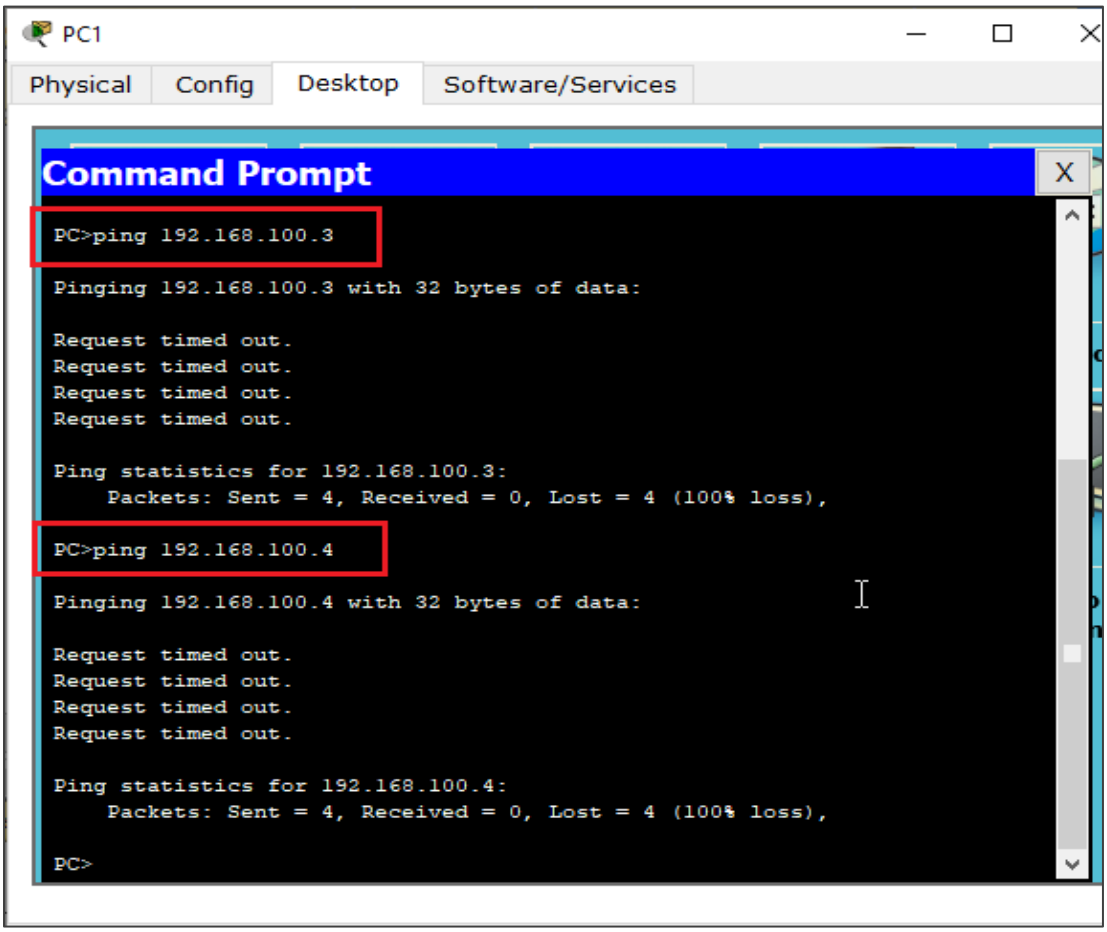
5.4 To verify communication within VLAN 11, go to the Command Prompt on PC2 and type **ping 192.168.100.4** to check connectivity with PC3



5.5 To verify isolation across different VLANs, go to the Command Prompt on PC0 VLAN 10 and type **ping 192.168.100.3** to ensure that communication with PC2 VLAN 11 does not occur



5.6 To verify isolation across different VLANs, go to the Command Prompt on PC1 (VLAN 10) and type **ping 192.168.100.4** to ensure that communication with PC3 (VLAN 11) does not occur



By following these steps, you have successfully implemented VLANs and network segmentation in a simulated environment using Cisco Packet Tracer. This implementation will allow you to logically separate network traffic, enhancing security and performance. Regular verification and testing of VLAN configurations are recommended to ensure optimal network functionality and security.