

## Experiment 5

**Aim:** To design and configure a Virtual Private Network (VPN) using Cisco Packet Tracer for secure communication.

**Theory:** A Virtual Private Network (VPN) is a secure communication method that allows data to travel between remote networks as if they were on the same private network. This experiment aims to design and configure a VPN using Cisco Packet Tracer to connect two networks securely. By establishing a tunnel between two routers, data packets can traverse the public network safely, with the tunnel acting as a virtual private link.

To achieve this, a network topology consisting of two PCs and three routers is created. PC0 and PC1 are connected to Router1 and Router2 respectively, while Router1 and Router2 are linked through a third router (Router0). The communication between the networks is secured using a tunnel interface configured on both Router1 and Router2. Below are the steps to configure and verify the VPN:

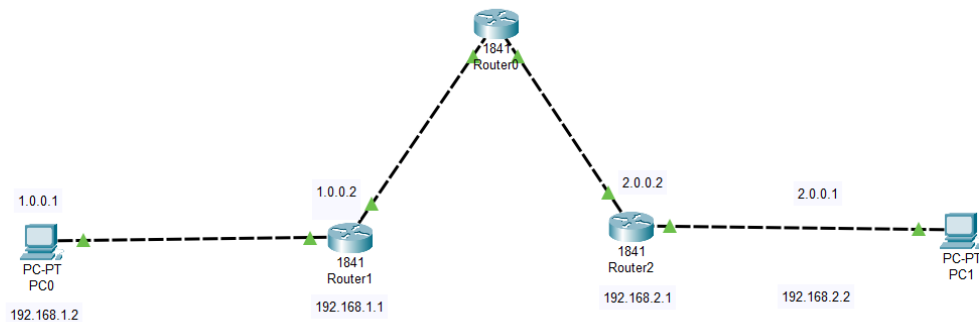
1. Network Design and Setup:
  - Create a network topology with two PCs (PC0 and PC1) connected to Router1 and Router2 via FastEthernet interfaces.
  - Use Router0 to establish a serial link connection between Router1 and Router2 for WAN communication.
2. Assign IP Addresses:
  - Configure IP addresses for PCs, routers, and their respective interfaces. Assign LAN IPs for PC0 and PC1 and gateway IPs on Router1 and Router2. Use a different subnet for the tunnel network (e.g., 172.16.1.0/30).
3. Configure Tunnel Interfaces:
  - On Router1, create a tunnel interface, assign it an IP (172.16.1.1/30), and set the tunnel source as the FastEthernet interface and the destination as Router2's public IP.
  - Repeat this configuration on Router2, assigning the tunnel IP as 172.16.1.2/30 and specifying Router1's public IP as the destination.
4. Static Routing:
  - Configure static routes to enable communication between the two networks:
    - On Router1, route traffic destined for 192.168.2.0/24 through the tunnel IP 172.16.1.2.
    - On Router2, route traffic destined for 192.168.1.0/24 through the tunnel IP 172.16.1.1.
5. Verify Connectivity:
  - Test the VPN tunnel by pinging from PC0 to PC1.

- Use show ip interface brief and traceroute commands to confirm the tunnel is operational and that data is routed correctly.

#### 6. Validate Security:

- Confirm that traffic between the two networks travels exclusively through the VPN tunnel, ensuring a secure connection.

#### Observations:



```

Router1
Physical Config CLI Attributes
IOS Command Line Interface
Router#ping 2.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.0.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms

Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface tunnel 1

Router(config-if)#
%LINK-5-CHANGED: Interface Tunnell, changed state to up

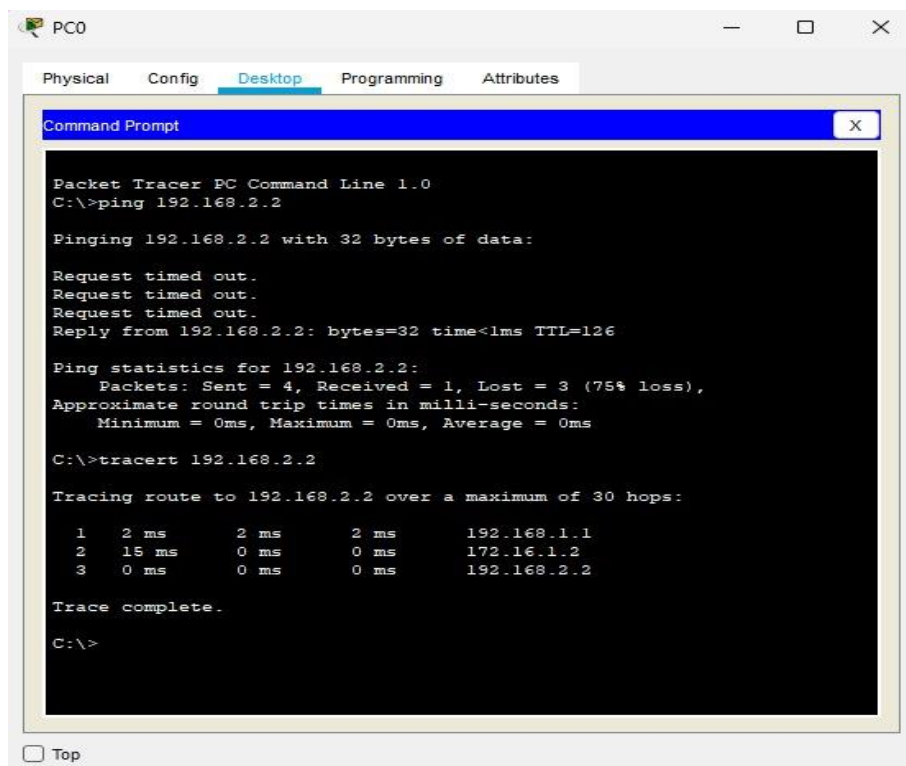
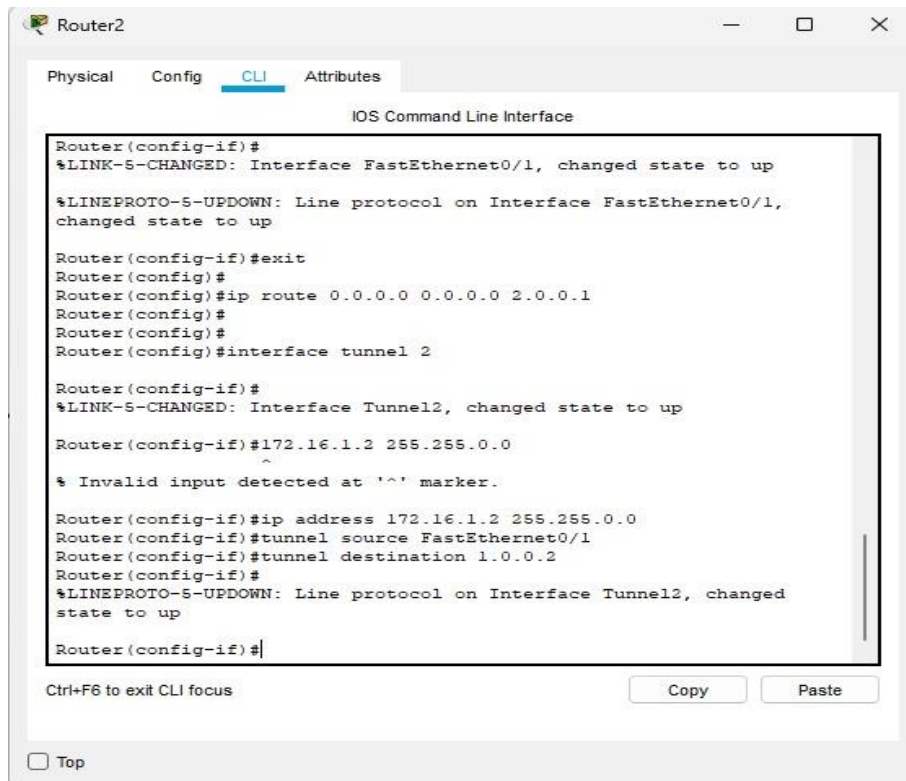
Router(config-if)#ip address 172.16.1.1
% Invalid input detected at '^' marker.

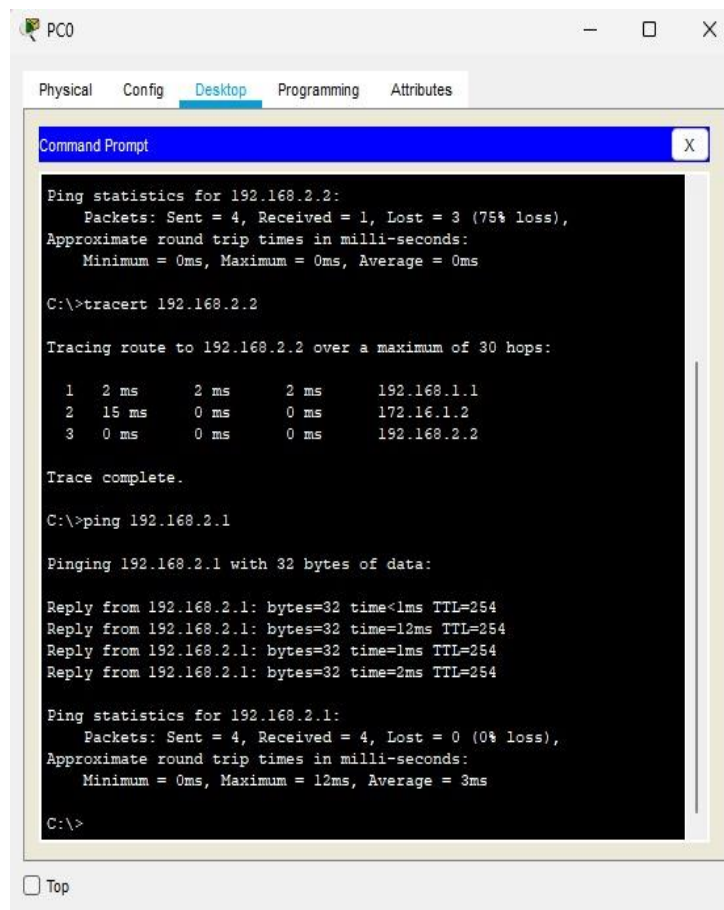
Router(config-if)#ip address 172.16.1.1
% Incomplete command.
Router(config-if)#ip address 172.16.1.1 255.255.0.0
Router(config-if)#tunnel source FastEthernet 0/1
Router(config-if)#tunnel destination 2.0.0.2
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnell, changed
state to up
Router(config-if)#
  
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top





The screenshot shows a Cisco Packet Tracer interface with a PC0 icon in the top left. The 'Desktop' tab is selected, displaying a Command Prompt window. The window contains the following text:

```
Command Prompt

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  0  2 ms    2 ms    2 ms    192.168.1.1
  1  15 ms   0 ms    0 ms    172.16.1.2
  2   0 ms   0 ms    0 ms    192.168.2.2

Trace complete.

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=12ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=2ms TTL=254

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>
```

At the bottom left of the Command Prompt window, there is a 'Top' button.

**Result:** Successfully implemented a Virtual Private Network (VPN) using Cisco Packet Tracer for secure communication.