Practical 7

Objective: NAT (Network Address Translation): Set up NAT on a router to translate private IP addresses to public IP addresses for outbound internet connectivity. Test the translation and examine how NAT helps conserve IPv4 address space.(Using Packet Tracer) **Procedure: Step 1: Set Up the Devices**

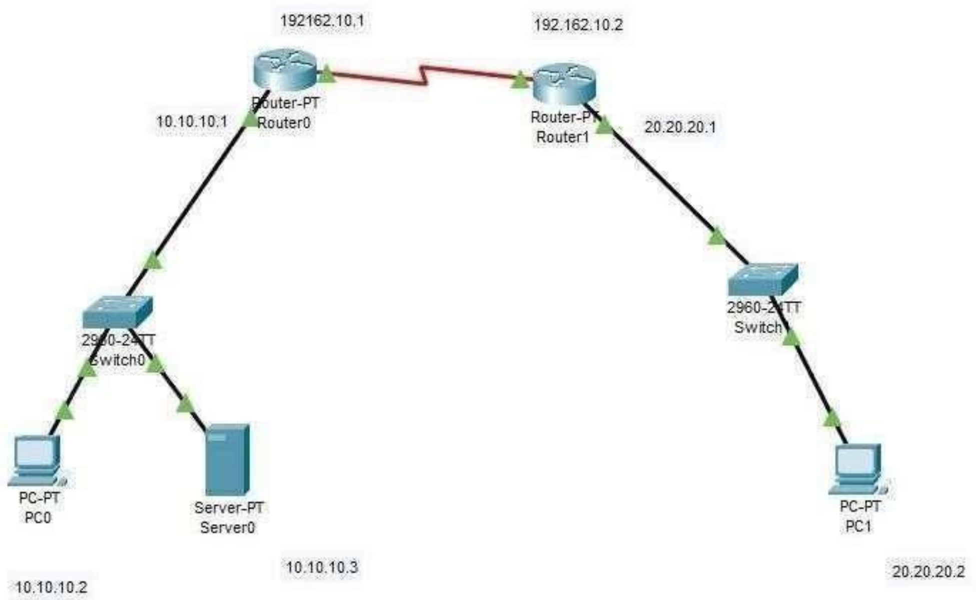
1. Open packet Tracer.

2. Add the following Devices to the workspace:

- 2 Router
- 2 PC
- 2 Switch
- 1 Server

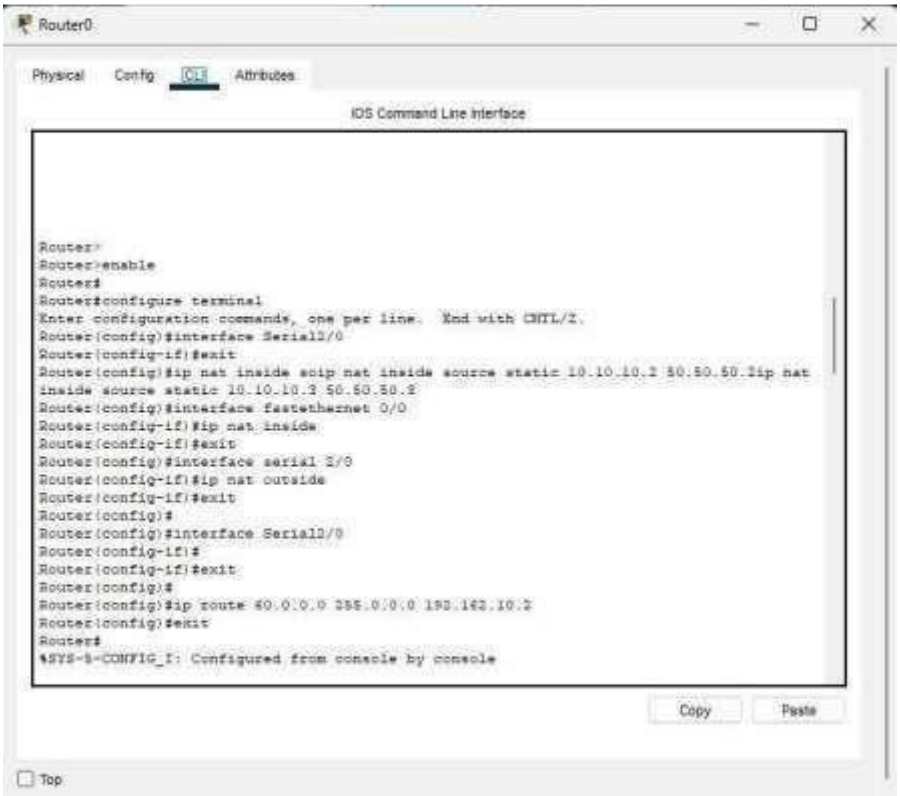
3. Connect Devices:

- Use straight-through ethernet cable to link the devices together (PCs, Switch, Server, router).
- For connection of router0-to-router1 communication, use serial DTE wire(serial2/0 to serial2/0).



Router(config)#interface fastethernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface serial 2/0

Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#ip route 60.0.0.0 255.0.0.0 192.162.10.2 Router(config)#exit

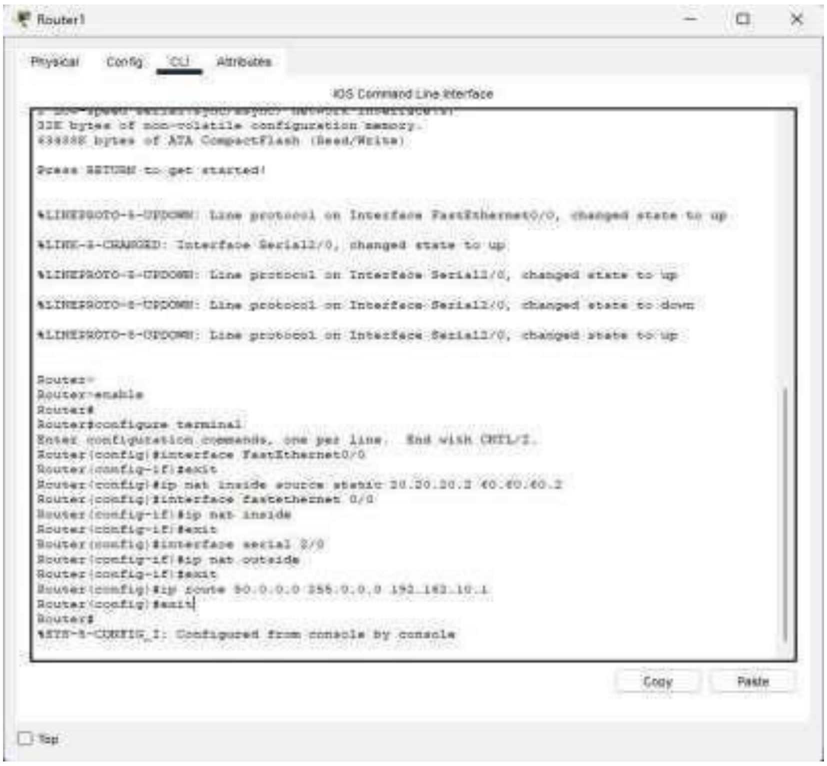


4. Assign IP address to router1 in Config.

1) Go in Config then • FastEthernet 0/0- Port Status: on IPv4
Address: 20.20.20.1
Subnet Mask: 255.0.0.0 •
Serial2/0- Port Status: on
IPv4 Address: 192.162.10.2
Subnet Mask: 255.255.255.0

2) CLI command in router type following ccommands
Router>enable
Router#

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#exit
Router(config)#ip nat inside source static 20.20.20.2 60.60.60.2
Router(config)#interface fastethernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface serial 2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip route 50.0.0.0 255.0.0.0 192.162.10.1 Router(config)#exit
```

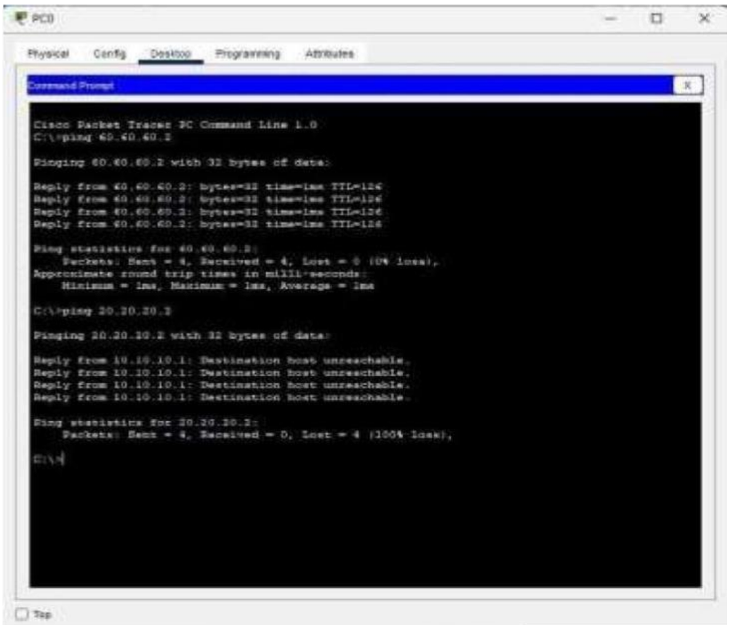


5. Configure the Server
   a) Click on Server0
   b) Go to the Services tab
   c) Click on HTTP.
   d) Ensure the HTTP services is ON.
   e) Edit text in index.html

6. Test the translation

1) Verify pass message PC0 to PC1

- Click on PC0
- Ping 60.60.60.2 (get reply)
- Ping 20.20.20.2 (unreachable hide ip private)



2) Check for server

- Go to PC1
- On desktop, open the web browser.
- Enter the url 50. 50.50.3

Practical 8

Objective: Network Troubleshooting- IP Misconfiguration: Identify and resolve network connectivity issues caused by an incorrect IP configuration. We will create a simple network in Cisco Packet Tracer (2 PCs, 2 routers, 2 switches) where one device's IP settings are intentionally wrong, then use simulation mode and CLI troubleshooting to find and fix the error.

Procedure

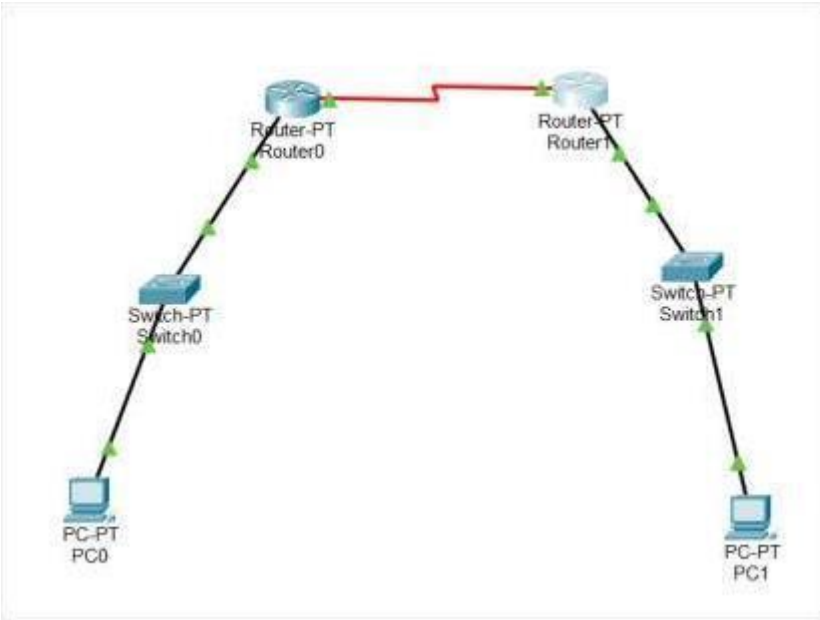
1. **Step 1: Set Up the Devices** ○ Open Cisco Packet Tracer. Add the following devices to the workspace:

- 2 Routers (e.g. Router0, Router1)
- 2 Switches (Switch0, Switch1)
- 2 PCs (PC0, PC1)

o Connect devices with straight-through cables as follows:

- PC0 → Switch0, and PC1 → Switch1.
- Router0 (FastEthernet0/0) → Switch0; Router1 (FastEthernet0/0) → Switch1.

o Connect the routers to each other: Use a serial DTE cable to link Router0's Serial2/0 port to Router1's Serial2/0 port (one end will be DCE).

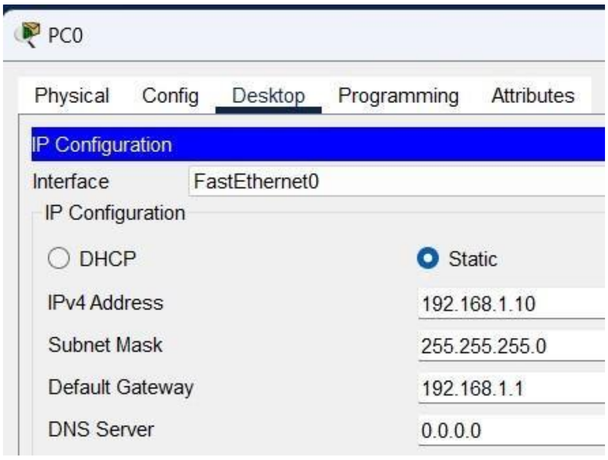


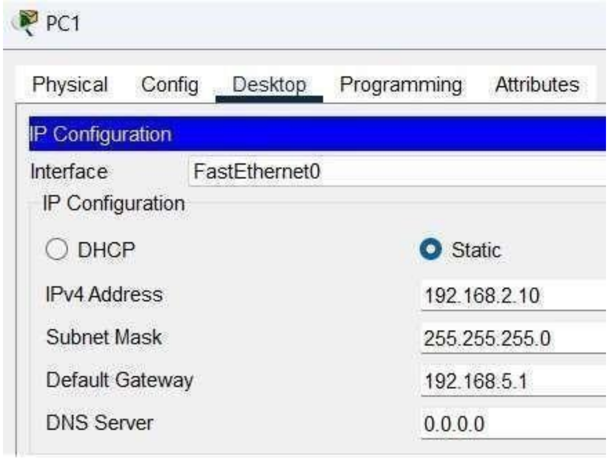
2. **Step 2: Assign IP Addresses (with an intentional error)** ○ **PC**

Configurations:

- **PC0:** Go to PC0 → **Desktop** tab → **IP Configuration**. Set:
- IPv4 Address: 192.168.1.10
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1 (Router0's Fa0/0)
- **PC1:** Go to PC1 → **Desktop** → **IP Configuration**. Set:
- IPv4 Address: 192.168.2.10
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1 (***Incorrect*** – should be 192.168.2.1)

Note: This mismatch of the gateway on PC1 is the intended misconfiguration.





- **Router0 Configuration (via CLI):**

  Click Router0 → **CLI** tab. Enter:

```
Router0> enable
Router0# configure terminal
Router0(config)# interface FastEthernet0/0
Router0(config-if)# ip address 192.168.1.1 255.255.255.0
Router0(config-if)# no shutdown
Router0(config-if)# exit
Router0(config)# interface Serial2/0
Router0(config-if)# ip address 10.0.0.1 255.255.255.252
Router0(config-if)# no shutdown
Router0(config-if)# exit
Router0(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2 Router0(config)# exit
```

- **Router1 Configuration (via CLI):**

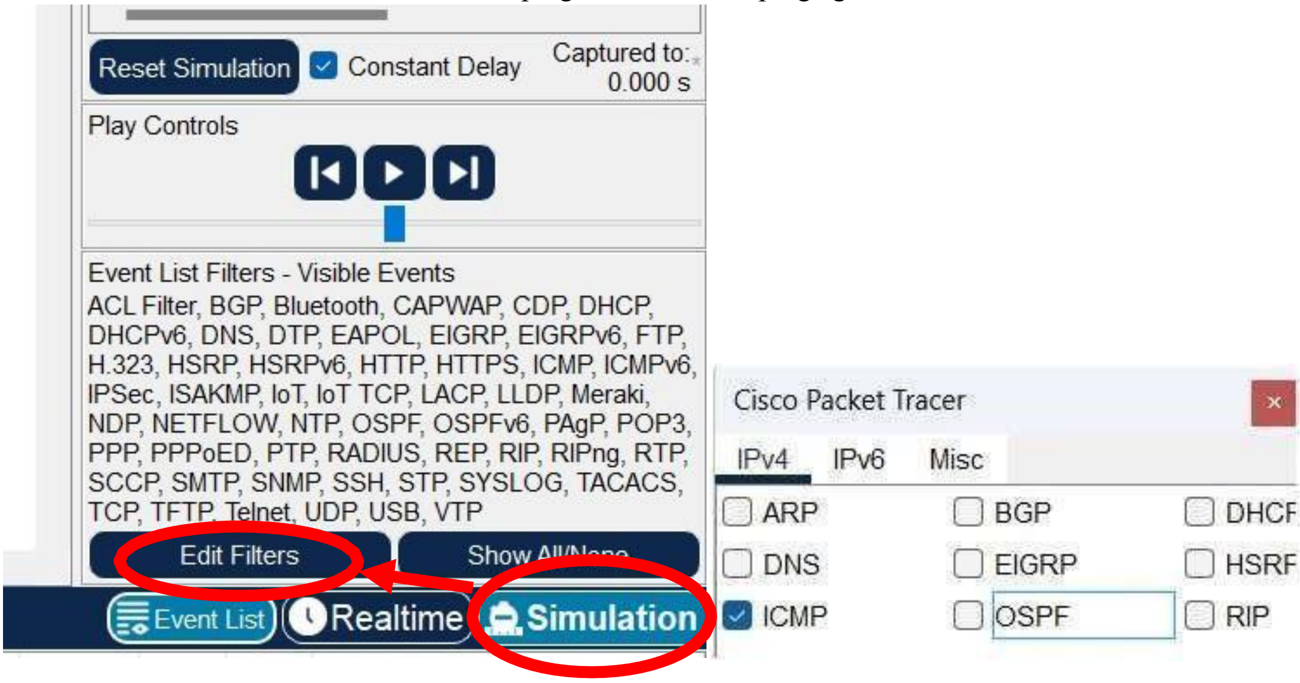
  Click Router1 → **CLI** tab. Enter:

```
Router1> enable
Router1# configure terminal
Router1(config)# interface FastEthernet0/0
Router1(config-if)# ip address 192.168.2.1 255.255.255.0
Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1(config)# interface Serial2/0
Router1(config-if)# ip address 10.0.0.2 255.255.255.252
Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1 Router1(config)# exit
```

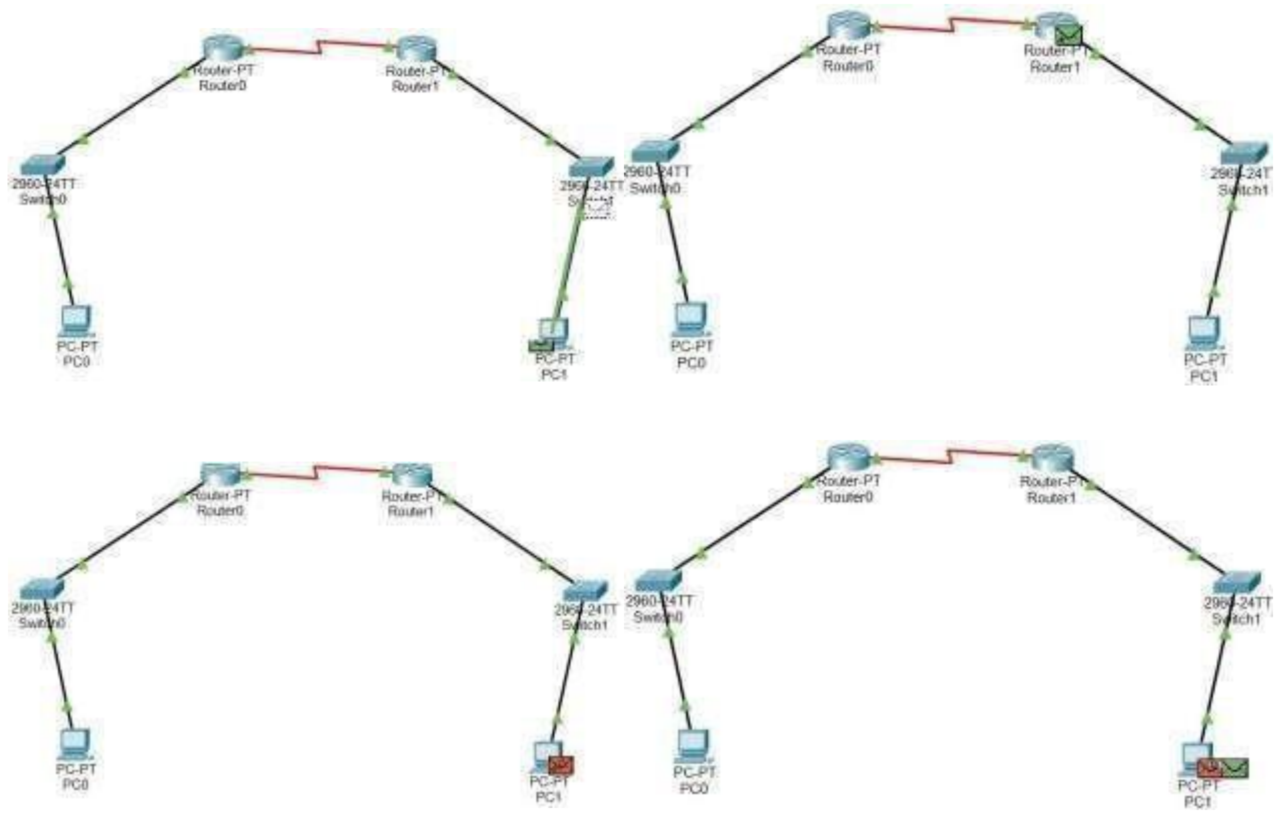
3. **Step 3: Test Connectivity (Initial Ping - Should Fail)** ○ On **PC0**, go to **Desktop** → **Command Prompt**. Issue the ping: ○ PC> ping 192.168.2.10

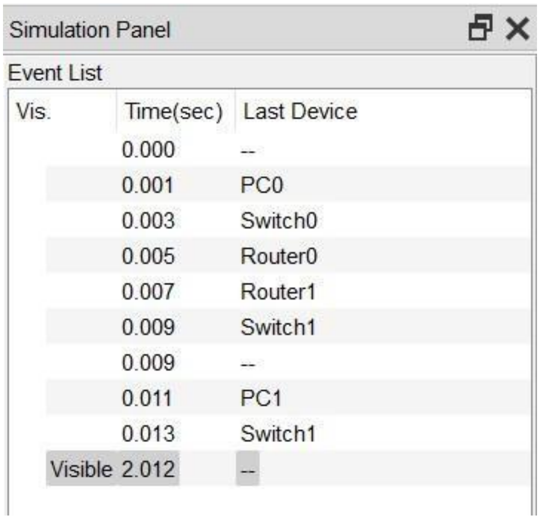
```
C:\>ping 19.168.2.10

Pinging 19.168.2.10 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 19.168.2.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

- Switch **Packet Tracer to Simulation mode** (button at bottom right). Clear filters except **ICMP** so we can trace the ping. Then send the ping again from PC0.



- In the Event List, observe the following:
    - PC0 ARPs for 192.168.1.1 (its gateway) and sends the ICMP echo to Router0.
    - Router0 forwards to Router1, and Router1 ARPs for PC1. PC1 receives the ICMP request.
    - **Critical:** PC1 then issues an ARP for 192.168.5.1 (its configured gateway) with no reply. This shows PC1 is trying to reach the wrong gateway (192.168.5.1 instead of 192.168.2.1).





Simulation Panel

Event List

Vis.	Time(sec)	Last Device
	0.000	--
	0.001	PC0
	0.003	Switch0
	0.005	Router0
	0.007	Router1
	0.009	Switch1
	0.009	--
	0.011	PC1
	0.013	Switch1
Visible	2.012	--

4. **Step 4: Troubleshoot the Misconfiguration** ○ On **PC1**, check the IP configuration. In Desktop > Command Prompt, run: ○

   PC> ipconfig

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::201:C9FF:FE9E:3D30
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.2.10
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.5.1
```

or simply look at the **IP Configuration** settings. You will see: Default Gateway = 192.168.5.1 (incorrect).

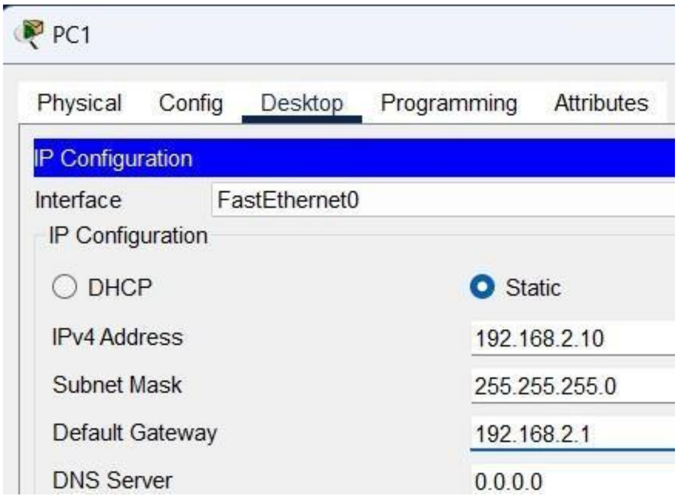
- Alternatively, on **Router1** CLI, use show ip interface brief to verify Router1's Fa0/0 address is 192.168.2.1, confirming the gateway should be that.

- Conclusion: PC1's default gateway is wrong. It should be the address of Router1's interface on that network.

5. **Step 5: Correct the Configuration**

   - Fix PC1's gateway: Click PC1 → **Desktop** → **IP Configuration**. Change **Default Gateway** to 192.168.2.1 (Router1's Fa0/0 address).

   - Ensure all other settings remain: IPv4=192.168.2.10, Mask=255.255.255.0. Save/close the settings.



6. **Step 6: Verify Connectivity (Ping - Should Succeed)** On **PC0**, in Command Prompt, run the ping again: ○ PC> ping 192.168.2.10

```
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time=12ms TTL=126
Reply from 192.168.2.10: bytes=32 time=7ms TTL=126
Reply from 192.168.2.10: bytes=32 time=8ms TTL=126
Reply from 192.168.2.10: bytes=32 time=8ms TTL=126

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 12ms, Average = 8ms
```

This confirms PC0 can reach PC1.

- (Optional) On **PC1**, try ping 192.168.1.10 to verify two-way communication.

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=9ms TTL=126
Reply from 192.168.1.10: bytes=32 time=11ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 8ms
```

- All pings should now succeed, indicating the network is fully connected after correcting the IP misconfiguration.

Practical 9

Objective: To monitor network traffic using Wire Shark.

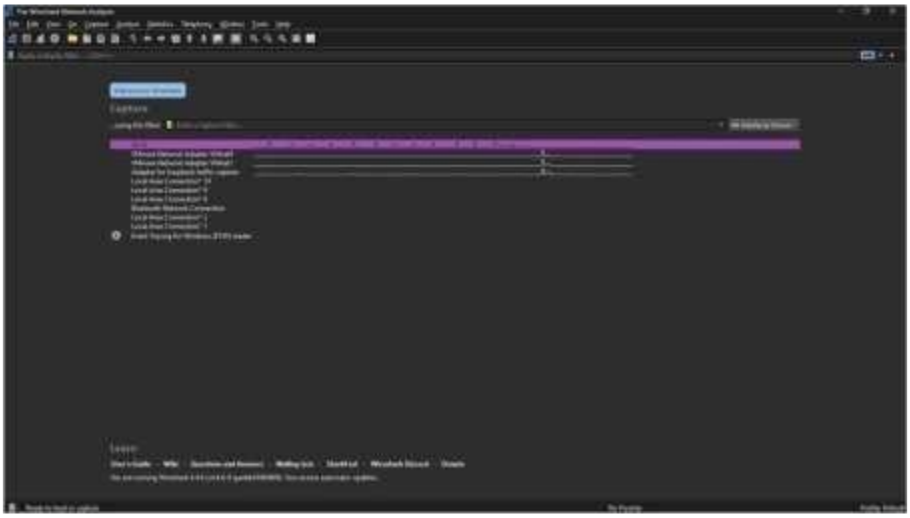
Procedure:

Step 1: Open Wireshark.

- Right-click on Wireshark icon → Run as Administrator.

Step 2: Select the appropriate network interface (such as Wi-Fi or Ethernet) from the list shown.

- Choose the one that shows active traffic (moving graph).



Step 3: Start capturing packets.

- Click the blue shark fin icon to start live capture.

Step 4: Perform some network activity.

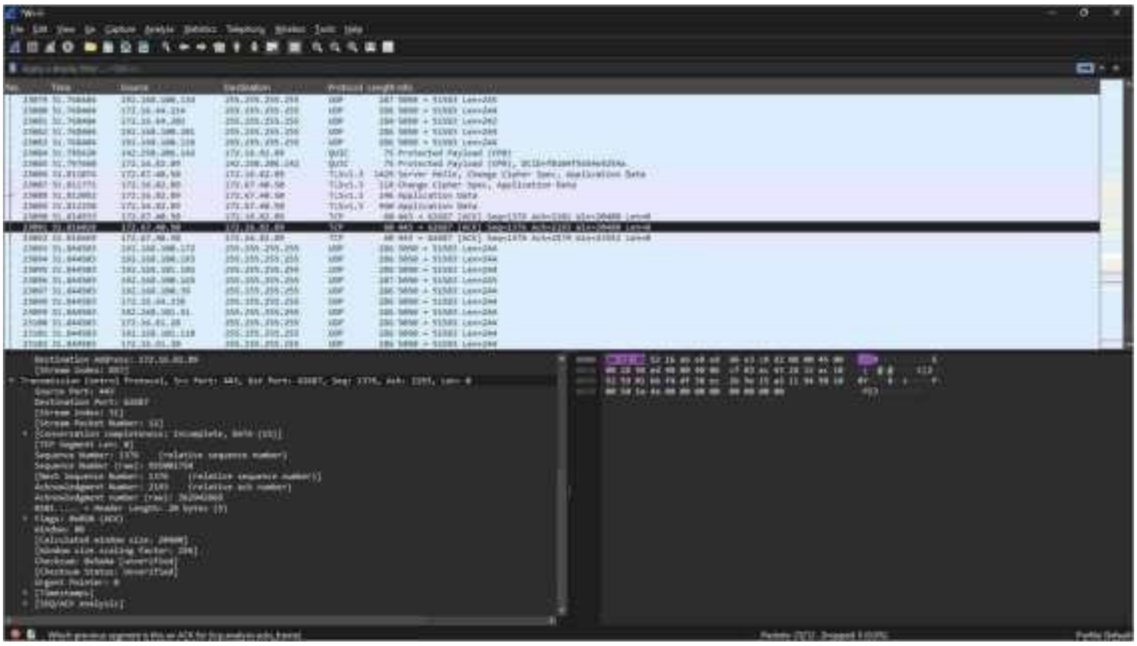
- Open a web browser and visit any website (e.g., www.google.com) to generate traffic.

Step 5: Observe live packet capture.

- Packets will appear in the capture window with details like Source, Destination, Protocol, and Info.

Step 6: Stop the capture.

- After a few seconds, click the red square (Stop) button to end capturing.



Step 7: Analyze the captured packets.

Click on any packet to expand and view detailed header information of protocols like:

- Ethernet (Data Link Layer)
- IP (Network Layer)
- TCP/UDP (Transport Layer)
- Application Layer protocols (like HTTP, DNS, etc.)

Practical 10

Objective: To analyze complete TCP/IP protocol suite layer's headers using Wire Shark.

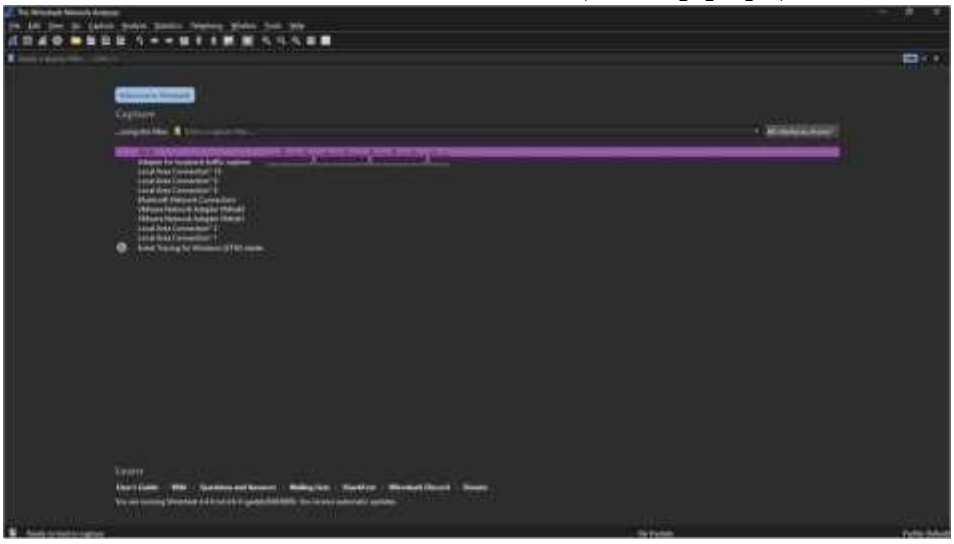
Procedure:

Step 1: Open Wireshark.

- Right-click on Wireshark icon → Run as Administrator.

Step 2: Select the appropriate network interface (such as Wi-Fi or Ethernet) from the list shown.

- Choose the one that shows active traffic (moving graph).



Step 3: Start capturing packets.

- Click the blue shark fin 영옂옂엿였 icon to start live capture.

Step 4: Run Some TCP Traffic

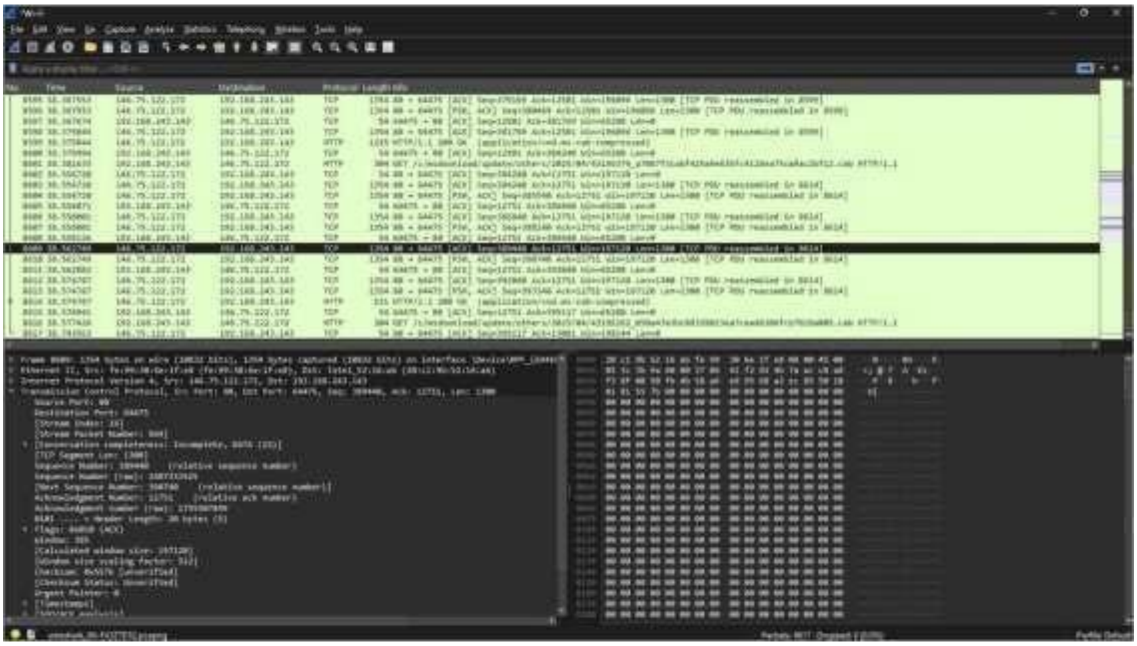
- Open a web browser (Chrome, Firefox, Edge).
- Visit a website like https://www.google.com or https://www.wikipedia.org. (Websites use TCP).

Step 5: Observe live packet capture.

- Packets will appear in the capture window with details like Source, Destination, Protocol, and Info.

Step 6: Stop the capture.

- After a few seconds, click the red square (Stop) button to end capturing.



Step 7: Select a TCP/IP packet from the captured packets list.

- Identify a packet using TCP or UDP as the transport protocol.

Step 8: Expand and examine each layer.

- Click on the packet and expand the following protocol layers:

  a) Ethernet II (Data Link Layer) → Source and Destination MAC addresses.

  b) Internet Protocol (IP) (Network Layer) → Source IP, Destination IP, TTL, Protocol, etc.

  c) Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) (Transport Layer) → Ports, Sequence numbers, Flags.

  d) Application Layer (e.g., HTTP, DNS) → Application data and methods.

Step 9: Note down the header fields.

- Observe how each layer adds its own header information during packet transmission