Graphic Era
HILL UNIVERSITY
Established by an Act of the State Legislature of Uttarakhand (Adhiniyam Sankhya 12 of 2011)
University under section 2(f) of UGC Act, 1956

DEHRADUN CAMPUS

# PRACTICAL FILE/TERM WORK COMPUTER NETWORK

“LAB MANUAL”

PCS-604

B.Tech CSE VI

2025-26

## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

## GRAPHIC ERA HILL UNIVERSITY,DEHRADUN

| SUBMITTED TO | SUBMITTED BY |
|---|---|
| DR. Ashook Sahoo | NAME:-Aman Uniyal |
| | UNIV. ROLL :-2218318 |

DEPARTMENT OF COMPUTER SCIENCE

COURSE/SEM:- B.TECH & ENGG. CSE

Name-Aman uniyal Student-Id-220211206 Semester-6 Section-K1

Graphic Era
HILL UNIVERSITY
Established by an Act of the State Legislature of Uttarakhand (Adhiniyam Sankhya 12 of 2011)
University under section 2(f) of UGC Act, 1956

Graphic Era
HILL UNIVERSITY
Established by an Act of the State Legislature of Uttarakhand (Adhiniyam Sankhya 12 of 2011)
University under section 2(f) of UGC Act, 1956

DEPARTMENT OF B.Tech(CSE) STUDENT LAB REPORT SHEET

Photograph
PassportSize

Name of Student…………………………………………..…….
Mob.No…………………………………..…………..

Address Permanent
……………………………………………………………………………………….………..

Father's Name…………………………Occupation……………………………Mo No……..……..…..………

Mother's Name …………………….. Occupation…………………………… Mo No…………….…………..

Section ………… Branch…………………… Semester……………. Class Roll No ................. Grade A B
C

Local Address……………………………………………Email…………….…………………….Marks 5
3 1

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

# Experiment No.1

**Objective:** Familiarization of Network Environment, Understanding and using network utilities: ipconfig, netstat, ping, telnet, ftp, traceroute etc.

## Theory:

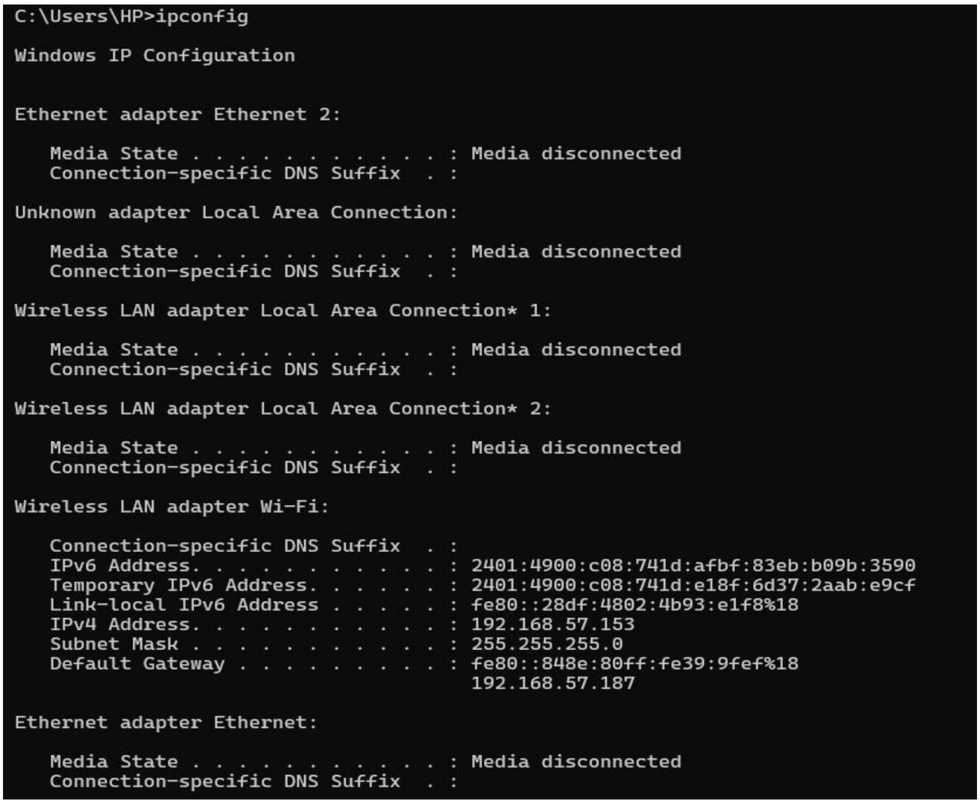
1) **ipconfig -** The ipconfig command is used in Windows to display and manage the network configuration of a computer. It provides details about the IP addresses, subnet masks, and default gateways for all network adapters.

### Common uses of ipconfig:

1) View IP configuration (ipconfig) - Displays the IP addresses, subnet masks, and gateway information for all network interfaces.
2) Detailed IP Configuration (ipconfig /all) - Shows additional details like MAC address, DHCP status, and DNS servers.
3) Release IP Address (ipconfig /release) - Releases the current IP address assigned by DHCP.

This command is useful for troubleshooting network issues like connectivity problems, incorrect IP configurations, and DNS resolution failures.

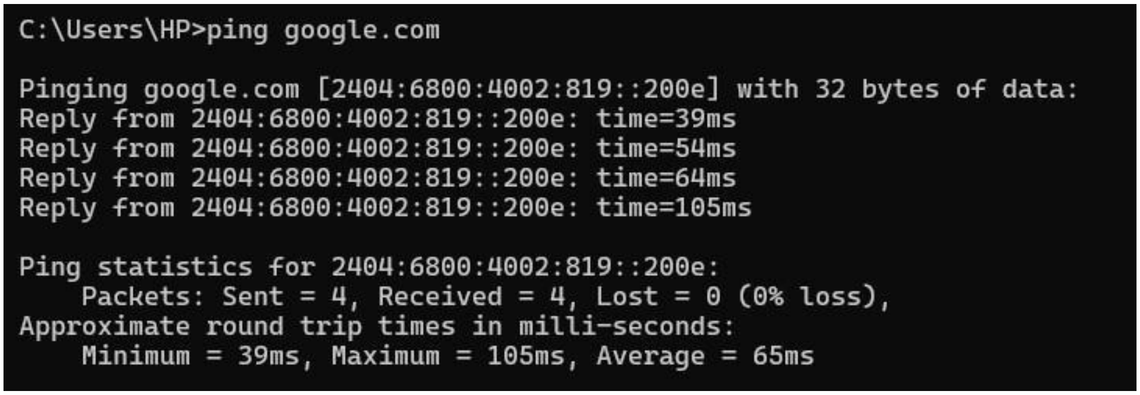
**ipconfig**



```
C:\Users\HP>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:c08:741d:afbf:83eb:b09b:3590
   Temporary IPv6 Address. . . . . . : 2401:4900:c08:741d:e18f:6d37:2aab:e9cf
   Link-local IPv6 Address . . . . . : fe80::28df:4802:4b93:e1f8%18
   IPv4 Address. . . . . . . . . . . : 192.168.57.153
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::848e:80ff:fe39:9fef%18
                                       192.168.57.187

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

2) **ping -** The ping command is used to test the connectivity between your computer and another device (like a server or website) over a network. It sends small packets of data (ICMP Echo Requests) to the target and waits for a response.

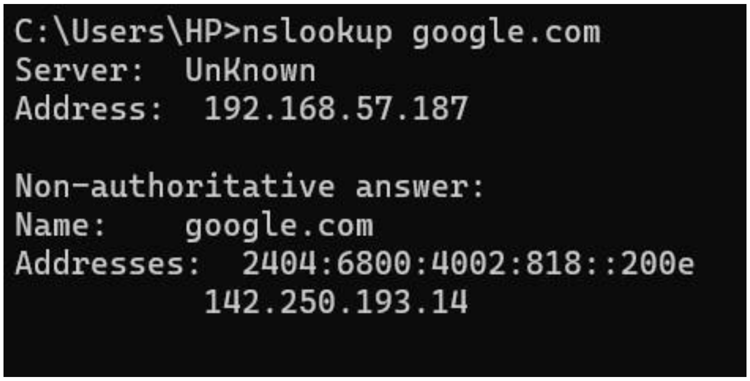
**ping**



```
C:\Users\HP>ping google.com

Pinging google.com [2404:6800:4002:819::200e] with 32 bytes of data:
Reply from 2404:6800:4002:819::200e: time=39ms
Reply from 2404:6800:4002:819::200e: time=54ms
Reply from 2404:6800:4002:819::200e: time=64ms
Reply from 2404:6800:4002:819::200e: time=105ms

Ping statistics for 2404:6800:4002:819::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 39ms, Maximum = 105ms, Average = 65ms
```

3) **nslookup -** The ping command is used to test the connectivity between your computer and another device (like a server or website) over a network. It sends small packets of data (ICMP Echo Requests) to the target and waits for a response.

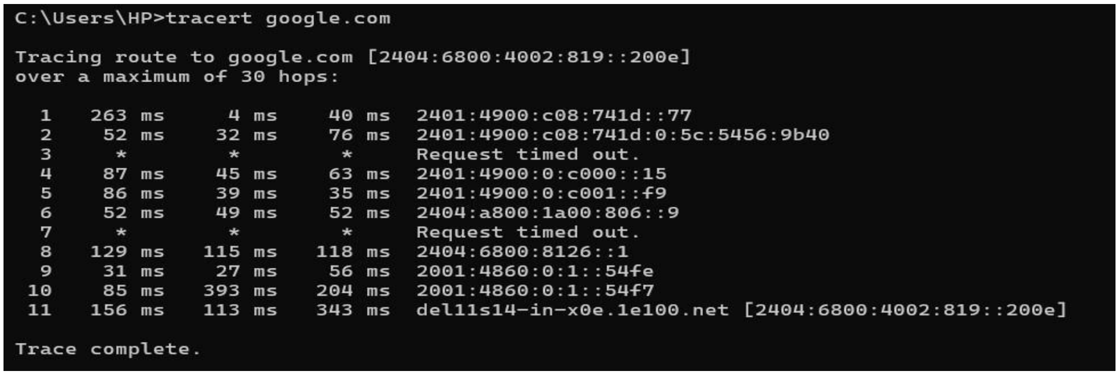
**nslookup**



```
C:\Users\HP>nslookup google.com
Server:  UnKnown
Address:  192.168.57.187

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4002:818::200e
          142.250.193.14
```

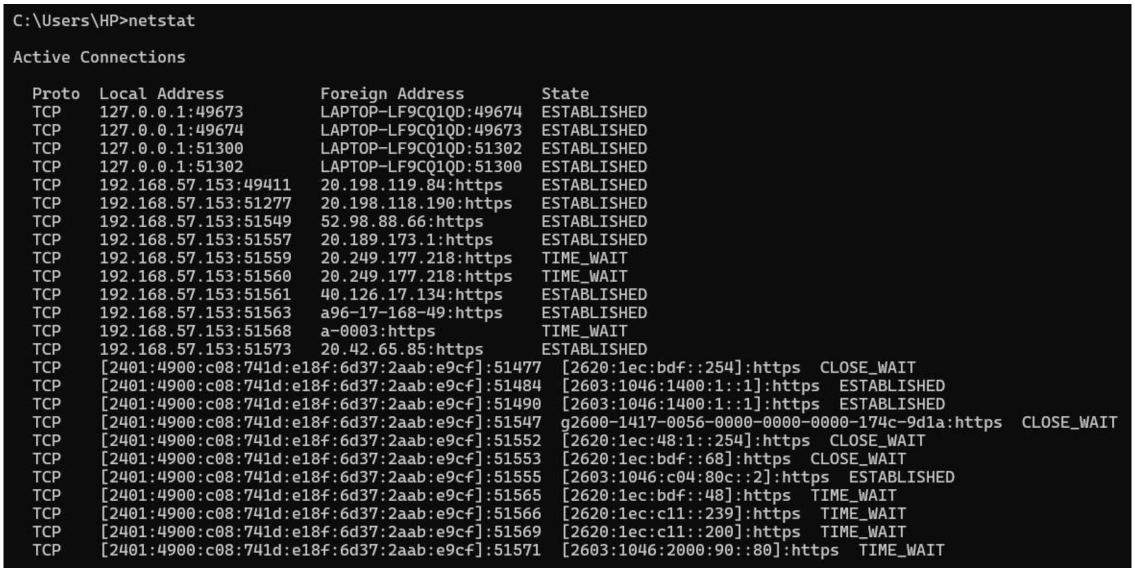
4) **tracert -** The tracert (Trace Route) command is used to track the path that packets take from your computer to a destination (such as a website or server). It helps identify network latency, routing issues, and the number of hops a packet takes to reach its destination.

**tracert**



```
C:\Users\HP>tracert google.com

Tracing route to google.com [2404:6800:4002:819::200e]
over a maximum of 30 hops:

  1   263 ms     4 ms    40 ms  2401:4900:c08:741d::77
  2    52 ms    32 ms    76 ms  2401:4900:c08:741d:0:5c:5456:9b40
  3     *        *        *     Request timed out.
  4    87 ms    45 ms    63 ms  2401:4900:0:c000::15
  5    86 ms    39 ms    35 ms  2401:4900:0:c001::f9
  6    52 ms    49 ms    52 ms  2404:a800:1a00:806::9
  7     *        *        *     Request timed out.
  8   129 ms   115 ms   118 ms  2404:6800:8126::1
  9    31 ms    27 ms    56 ms  2001:4860:0:1::54fe
 10    85 ms   393 ms   204 ms  2001:4860:0:1::54f7
 11   156 ms   113 ms   343 ms  del11s14-in-x0e.1e100.net [2404:6800:4002:819::200e]

Trace complete.
```

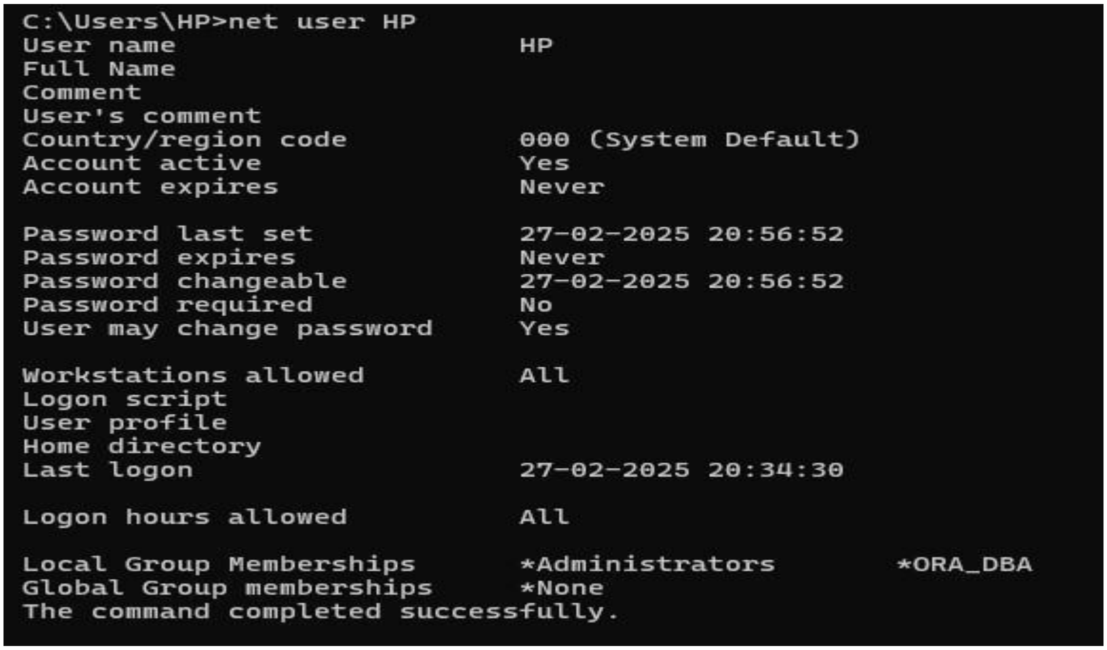
5) **netstat -** The netstat (Network Statistics) command is used to display active network connections, routing tables, and various network statistics. It helps in monitoring network activity and troubleshooting connectivity issues. – **netstat**



```
C:\Users\HP>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49673        LAPTOP-LF9CQ1QD:49674  ESTABLISHED
  TCP    127.0.0.1:49674        LAPTOP-LF9CQ1QD:49673  ESTABLISHED
  TCP    127.0.0.1:51300        LAPTOP-LF9CQ1QD:51302  ESTABLISHED
  TCP    127.0.0.1:51302        LAPTOP-LF9CQ1QD:51300  ESTABLISHED
  TCP    192.168.57.153:49411   20.198.119.84:https    ESTABLISHED
  TCP    192.168.57.153:51277   20.198.118.190:https   ESTABLISHED
  TCP    192.168.57.153:51549   52.98.88.66:https      ESTABLISHED
  TCP    192.168.57.153:51557   20.189.173.1:https     ESTABLISHED
  TCP    192.168.57.153:51559   20.249.177.218:https   TIME_WAIT
  TCP    192.168.57.153:51560   20.249.177.218:https   TIME_WAIT
  TCP    192.168.57.153:51561   40.126.17.134:https    ESTABLISHED
  TCP    192.168.57.153:51563   a96-17-168-49:https    ESTABLISHED
  TCP    192.168.57.153:51568   a-0003:https           TIME_WAIT
  TCP    192.168.57.153:51573   20.42.65.85:https      ESTABLISHED
  TCP    [2401:4900:c08:741d:e18f:6d37:2aab:e9cf]:51477  [2620:1ec:bdf::254]:https  CLOSE_WAIT
  TCP    [2401:4900:c08:741d:e18f:6d37:2aab:e9cf]:51484  [2603:1046:1400:1::1]:https  ESTABLISHED
  TCP    [2401:4900:c08:741d:e18f:6d37:2aab:e9cf]:51490  [2603:1046:1400:1::1]:https  ESTABLISHED
  TCP    [2401:4900:c08:741d:e18f:6d37:2aab:e9cf]:51547  g2600-1417-0056-0000-0000-0000-174c-9d1a:https  CLOSE_WAIT
  TCP    [2401:4900:c08:741d:e18f:6d37:2aab:e9cf]:51552  [2620:1ec:48:1::254]:https  CLOSE_WAIT
  TCP    [2401:4900:c08:741d:e18f:6d37:2aab:e9cf]:51553  [2620:1ec:bdf::68]:https  CLOSE_WAIT
  TCP    [2401:4900:c08:741d:e18f:6d37:2aab:e9cf]:51555  [2603:1046:c04:80c::2]:https  ESTABLISHED
  TCP    [2401:4900:c08:741d:e18f:6d37:2aab:e9cf]:51565  [2620:1ec:bdf::48]:https  TIME_WAIT
  TCP    [2401:4900:c08:741d:e18f:6d37:2aab:e9cf]:51566  [2620:1ec:c11::239]:https  TIME_WAIT
  TCP    [2401:4900:c08:741d:e18f:6d37:2aab:e9cf]:51569  [2620:1ec:c11::200]:https  TIME_WAIT
  TCP    [2401:4900:c08:741d:e18f:6d37:2aab:e9cf]:51571  [2603:1046:2000:90::80]:https  TIME_WAIT
```

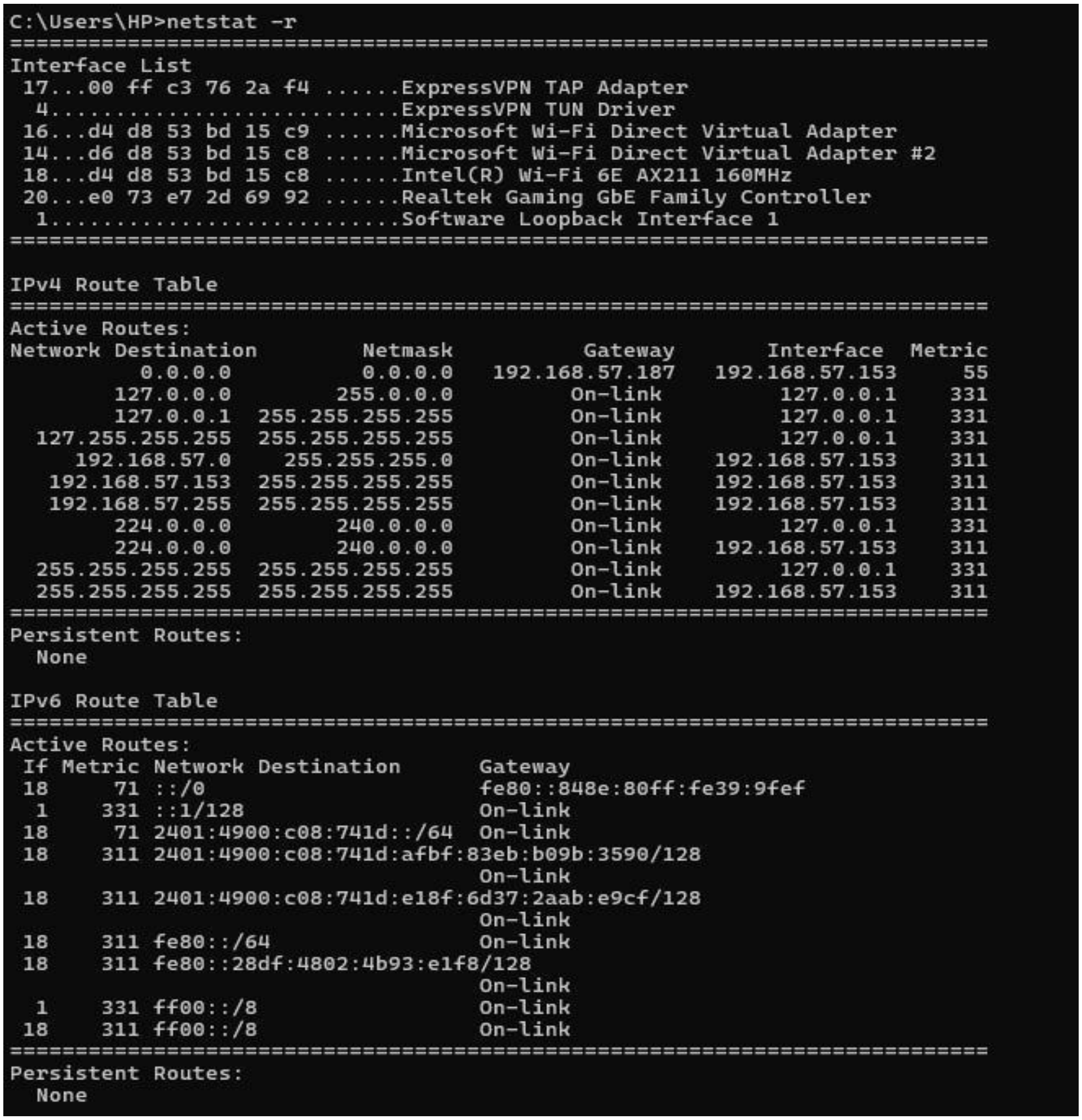
6) **net user <username> -** The net user <username> command is used in Windows to manage user accounts on a computer or a domain. It allows you to view, modify, create, or delete user accounts.

**Net user<username>**



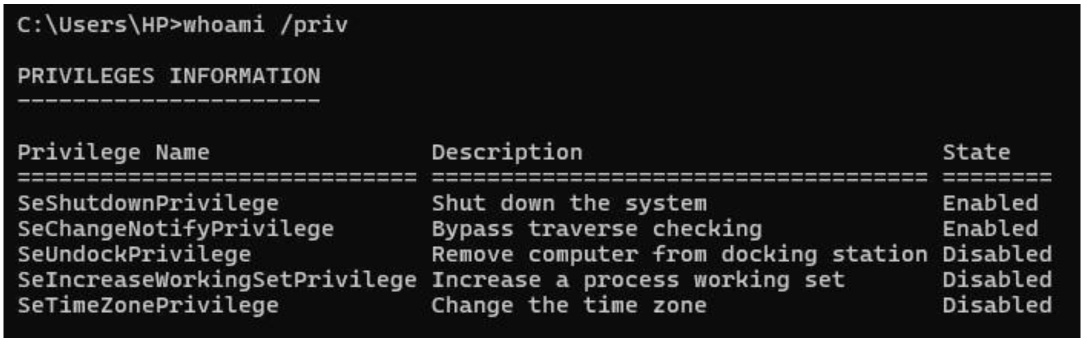
```
C:\Users\HP>net user HP
User name                    HP
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            27-02-2025 20:56:52
Password expires             Never
Password changeable          27-02-2025 20:56:52
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   27-02-2025 20:34:30

Logon hours allowed          All

Local Group Memberships      *Administrators       *ORA_DBA
Global Group memberships     *None
The command completed successfully.
```

8) **netstat -r :** Displays the system’s current routing table. **netstat -r**



```
C:\Users\HP>netstat -r
===========================================================================
Interface List
 17...00 ff c3 76 2a f4 ......ExpressVPN TAP Adapter
  4...........................ExpressVPN TUN Driver
 16...d4 d8 53 bd 15 c9 ......Microsoft Wi-Fi Direct Virtual Adapter
 14...d6 d8 53 bd 15 c8 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 18...d4 d8 53 bd 15 c8 ......Intel(R) Wi-Fi 6E AX211 160MHz
 20...e0 73 e7 2d 69 92 ......Realtek Gaming GbE Family Controller
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   192.168.57.187  192.168.57.153     55
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.57.0    255.255.255.0         On-link    192.168.57.153    311
   192.168.57.153  255.255.255.255         On-link    192.168.57.153    311
   192.168.57.255  255.255.255.255         On-link    192.168.57.153    311
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link    192.168.57.153    311
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link    192.168.57.153    311
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 18     71 ::/0                     fe80::848e:80ff:fe39:9fef
  1    331 ::1/128                  On-link
 18     71 2401:4900:c08:741d::/64  On-link
 18    311 2401:4900:c08:741d:afbf:83eb:b09b:3590/128
                                    On-link
 18    311 2401:4900:c08:741d:e18f:6d37:2aab:e9cf/128
                                    On-link
 18    311 fe80::/64                On-link
 18    311 fe80::28df:4802:4b93:e1f8/128
                                    On-link
  1    331 ff00::/8                 On-link
 18    311 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

9) **whoami /priv** - The whoami /priv command in Windows is used to display the privileges assigned to the currently logged-in user and their status (enabled or disabled). Example: - **whoami /priv**



```
C:\Users\HP>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

## Experiment No.2

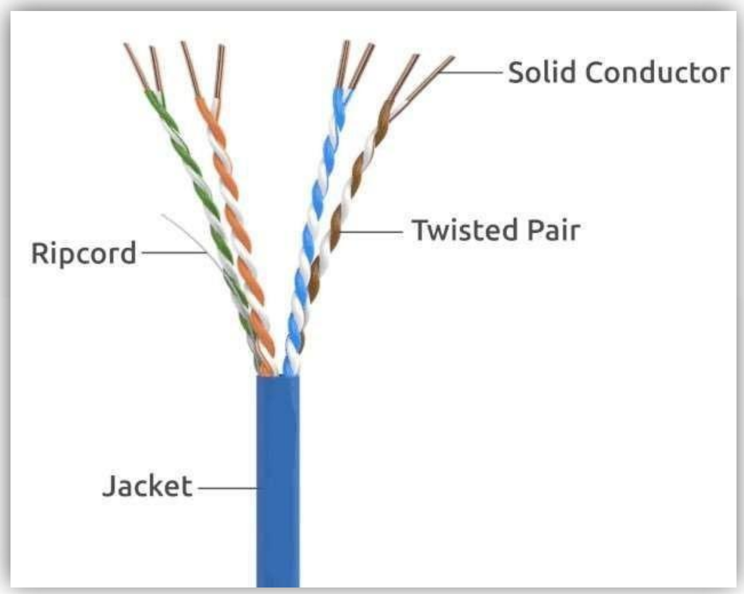
**Objective:** Familiarization with Transmission media and tools: Co-axial cable, UTP cable, Crimping tool, Connectors etc. Preparing the UTP cable for cross and direct connection using crimping tool.

**Theory:**

**1) UTP Cable -** UTP (Unshielded Twisted Pair) cable is a type of network cable used for transmitting data in computer networks, telecommunications, and various electronic applications. It consists of multiple pairs of twisted copper wires enclosed in an insulating sheath without any additional shielding, making it cost-effective and widely used for Ethernet connections.

## Structure of UTP Cable

- **Copper Conductors** – Carries electrical signals.
- **Twisted Pairs** – Wires are twisted in pairs to reduce electromagnetic interference (EMI) and crosstalk.
- **Outer Jacket** – Protects the internal wires.
- **No Shielding** – Unlike STP (Shielded Twisted Pair), UTP cables do not have extra metallic shielding.



## Advantages of UTP Cables

1) Cost-effective – Cheaper than shielded cables.

2) Flexible & Lightweight – Easy to install and manage.

## Disadvantages of UTP Cables

1) More prone to EMI & Crosstalk – No shielding to block interference.

2) Shorter Distance for High Speeds – Performance degrades over long distances.

**Common Uses of UTP Cables**

- Ethernet Networking (LANs, WANs, Internet connections) • CCTV and Security Systems

**2) Coaxial Cable -** A coaxial cable (coax) is a type of electrical cable used for transmitting radio frequency (RF) signals, internet data, cable television, and other forms of communication. It consists of a central conductor surrounded by multiple layers for insulation and shielding, which helps minimize signal interference and loss.

## Structure of a Coaxial Cable

A coaxial cable has multiple layers arranged concentrically:

1. **Inner Conductor** – A copper or aluminum wire that carries the electrical signal.
2. **Dielectric Insulator** – A non-conductive material that separates the core from the shielding.
3. **Metal Shield (Braided or Foil Shielding)** – Prevents external electromagnetic interference (EMI).
4. **Outer Jacket** – A plastic or rubber coating that protects the internal components.

## Advantages of Coaxial Cables

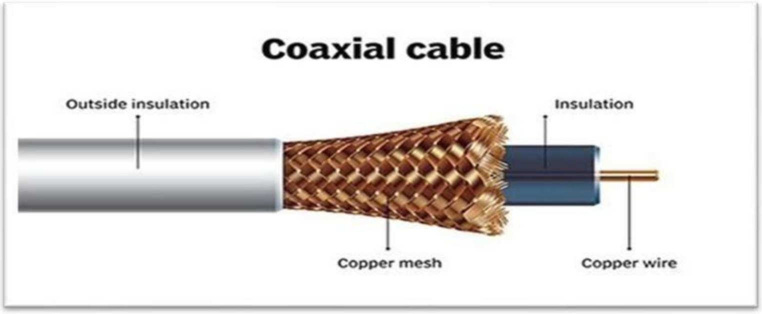
- High Signal Quality – Better resistance to interference than twisted pair cables.
- Durable and Shielded – Protects against electromagnetic and radio frequency interference.

## Disadvantages of Coaxial Cables

- Thicker and Less Flexible – Harder to install and manage compared to UTP cables.
- More Expensive than Twisted Pair – Due to additional shielding and materials.
- Limited Data Transmission Speed – Slower than fiber optics.

**Common Uses of Coaxial Cables**

- Cable TV & Satellite TV Connections



**3) Fiber Optic Cable** - A fiber optic cable is a high-speed data transmission cable that uses light signals to transfer data instead of electrical signals. It is made of ultra-thin glass or plastic fibers that allow data to travel at near the speed of light, making it much faster and more efficient than traditional copper cables.

## Structure of a Fiber Optic Cable

A fiber optic cable consists of multiple layers for efficient and protected signal transmission:

1. **Core** – The central glass or plastic fiber where light signals travel.

2. **Cladding** – A layer around the core that reflects light inward, preventing signal loss.

3. **Buffer Coating** – A protective layer to prevent damage.

4. **Outer Jacket** – A strong outer sheath that protects the cable from environmental damage.

## Advantages of Fiber Optic Cables

- High Speed – Supports speeds up to 100 Gbps or more.
- Long Distance – Can transmit data over hundreds of kilometers with minimal signal loss.
- Less Interference – Immune to electromagnetic interference (EMI) from electrical devices.

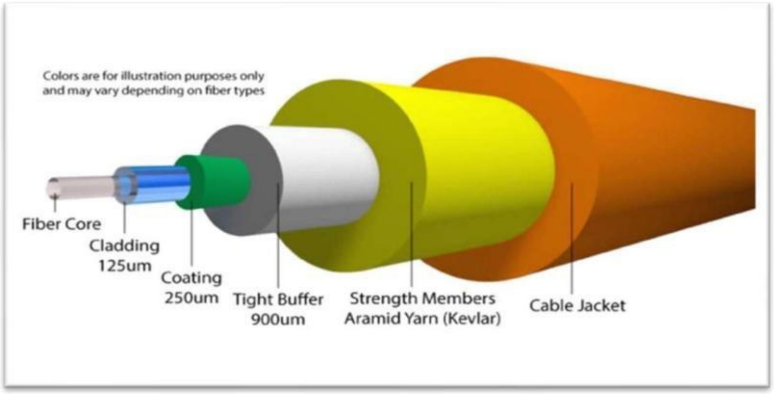
## Disadvantages of Fiber Optic Cables

- Expensive – Higher installation cost compared to copper cables.

- Fragile – Glass fibers are more delicate and need careful handling.

## Common Uses of Fiber Optic Cables

- Military & Space Applications (Secure and high-speed communication)
- Medical Equipment (Endoscopy, laser surgeries)


Colors are for illustration purposes only and may vary depending on fiber types
Fiber Core
Cladding 125um
Coating 250um
Tight Buffer 900um
Strength Members Aramid Yarn (Kevlar)
Cable Jacket

**4) RJ45 Connector -** An RJ45 (Registered Jack 45) connector is an 8-pin connector used for networking cables, primarily in Ethernet (LAN) connections. It connects devices like computers, routers, and switches using twisted pair cables (Cat5, Cat6, etc.).

**Key Features:**

- **8 Pins** – Supports 4 twisted pairs of wires.
- **Standard for Ethernet** – Used in wired LAN networks.
- **Plastic Clip** – Locks into the Ethernet port securely.
- **Compatible with UTP & STP cables** – Works with both **shielded** and **unshielded** cables.

5) **Crimping tool -** A crimping tool is a hand-held device used to attach RJ45 connectors to Ethernet cables by pressing and securing the metal pins into the wire conductors.

**Key Features:**

- **Wire Cutting & Stripping** – Cuts and removes cable insulation.
- **Handheld & Easy to Use** – Essential for network cable installations.

**Steps for Crimping an RJ45 Connector:**

1. **Strip the Cable** – Remove the outer sheath using the stripping blade.
2. **Arrange the Wires** – Follow **T568A or T568B** color coding.
3. **Insert into RJ45 Connector** – Ensure proper alignment.
4. **Crimp the Connector** – Squeeze the crimping tool to secure the pins.

**Common Uses of a Crimping Tool:**

- Networking (Ethernet Cable Installation & Repair)
- Telephone Line Crimping
- Custom LAN Cable Making

## Experiment No.3

**Objective:** Installation and introduction of simulation tool. (Packet Tracer)

**Theory:** Cisco Packet Tracer is a powerful network simulation tool by Cisco, allowing users to design, configure, and test virtual networks. It supports various Cisco devices and features a graphical interface for building complex topologies. With real-time simulation, protocol testing, and troubleshooting capabilities, it's ideal for networking education, CCNA exam preparation, and professional training—eliminating the need for physical hardware.

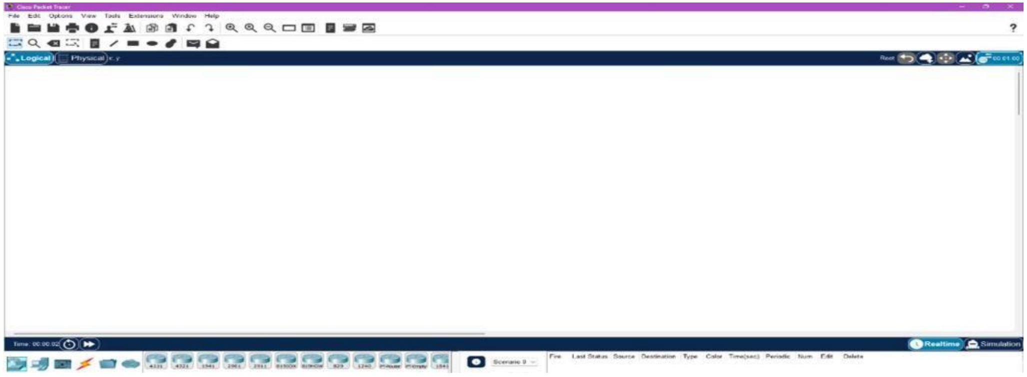
**Installation Steps**:

- Step 1: Visit the official Cisco Networking Academy website at Cisco Packet Tracer.
- Step 2: Create a free account or log in if you already have one.
- Step 3: Navigate to the Resources section and download the appropriate version for your operating system (Windows, macOS, or Linux).
- Step 4: Once the download is complete, run the installer and follow the on-screen instructions to install the tool.
- Step 5: After installation, log in with your NetAcad credentials to start using Packet Tracer. Now you are good to go with your packet tracer.

**Key Features of Cisco Packet Tracer:**

- **Network Simulation**: It allows you to design and simulate complex networks with routers, switches, computers, and other networking devices.
- **Virtual Devices**: You can configure routers, switches, and computers as if you were working on real hardware.
- **Multiuser Capability**: Enables collaborative work by allowing multiple users to interact within the same network.
- **Learning and Training**: It provides a platform to experiment with configurations, explore scenarios, and understand network behaviors.
- **Packet Tracing**: You can analyze packet-level information, see how traffic moves through your network, and view packet contents as they traverse the network.

**Practice for Cisco Certifications**: Cisco Packet Tracer is a great way to prepare for Cisco's CCNA or CCNP exams, as it allows for hands-on practice with Cisco commands and configurations.



## Experiment No.4

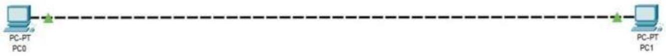
**Objective**: Build a simple network topology with routers, switches, and end devices such as PCs or laptops. Configure IP addresses and confirm connectivity between the devices using Packet Tracer.

**Procedure:**

**Direct Connection Between End Devices:**

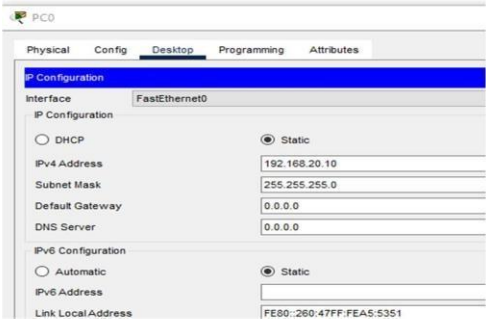
**Step 1**: Setting Up Network Devices

- In Cisco Packet Tracer, place the PCs and connect it.



**Step 2**: Configuring IP Addresses on the End Devices

- For each PC, navigate to **Desktop > IP Configuration**.
- Assign the following IP addresses:
  - PC0: 192.168.20.10 ○
  PC1: 192.168.20.11



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.20.10

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

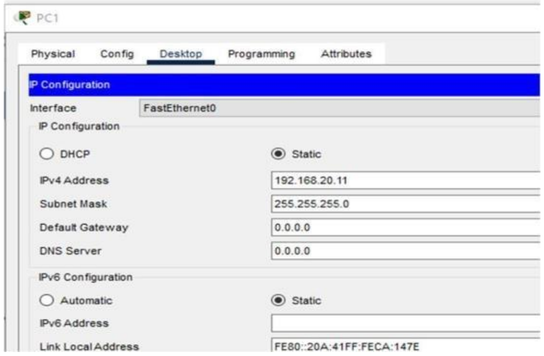
DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address:

Link Local Address: FE80::260:47FF:FEA5:5351



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.20.11

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

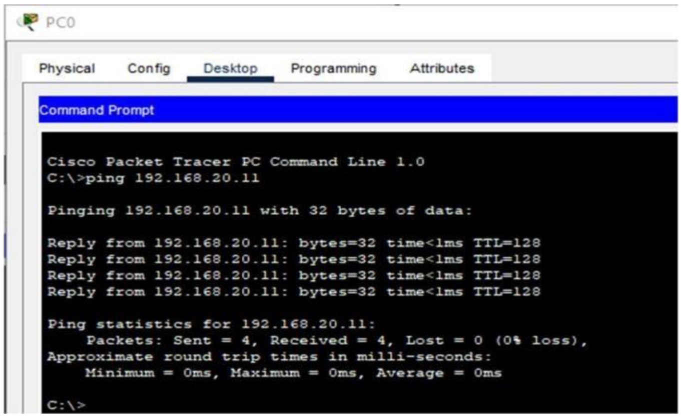
○ Automatic ● Static

IPv6 Address:

Link Local Address: FE80::20A:41FF:FECA:147E

**Step 3**: Testing Connectivity

- Open the **Command Prompt** on each PC and use ping command.

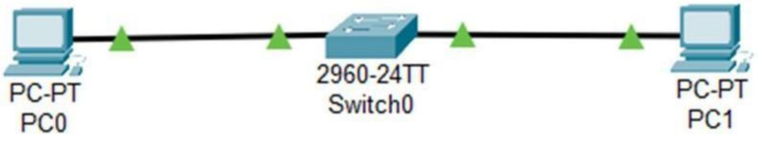


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.11

Pinging 192.168.20.11 with 32 bytes of data:

Reply from 192.168.20.11: bytes=32 time<1ms TTL=128
Reply from 192.168.20.11: bytes=32 time<1ms TTL=128
Reply from 192.168.20.11: bytes=32 time<1ms TTL=128
Reply from 192.168.20.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

**Direct Connection Between End Devices Using a Switch**

**Step 1: Setting Up Network Devices**

1. Open Cisco Packet Tracer and create a new workspace.
2. Drag and drop a switch from the Network Devices section.
3. Drag and drop two PCs from the End Devices section.
4. Connect each PC to the switch using straight-through Ethernet cables.



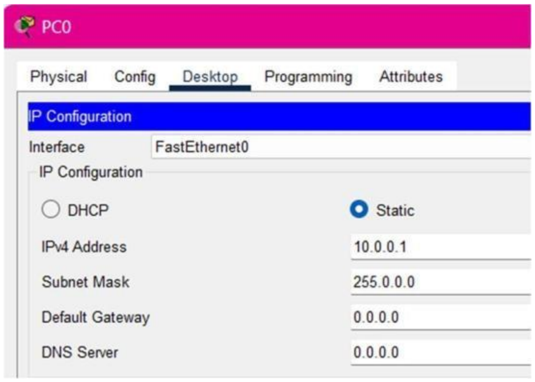
### Step 2: Configuring IP Addresses on End Devices

1. Click on PC0, go to Desktop > IP Configuration.

2Assign the following IP address:

PC0: 10.0.0.1(Subnet Mask: 255.0.0.0):

PC1: 10.0.0.2 (Subnet Mask: 255.0.0.0)



IP Configuration

Interface FastEthernet0

IP Configuration

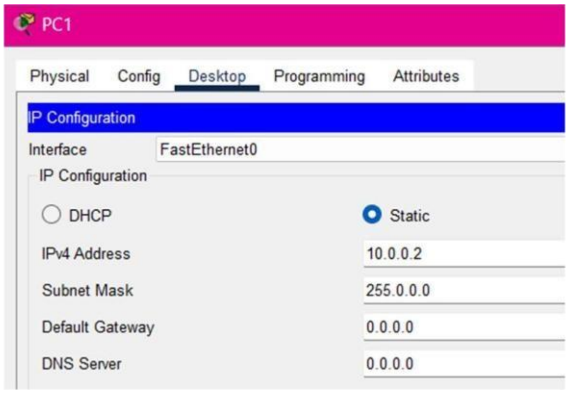
○ DHCP ● Static

IPv4 Address 10.0.0.1

Subnet Mask 255.0.0.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0



IP Configuration

Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address 10.0.0.2

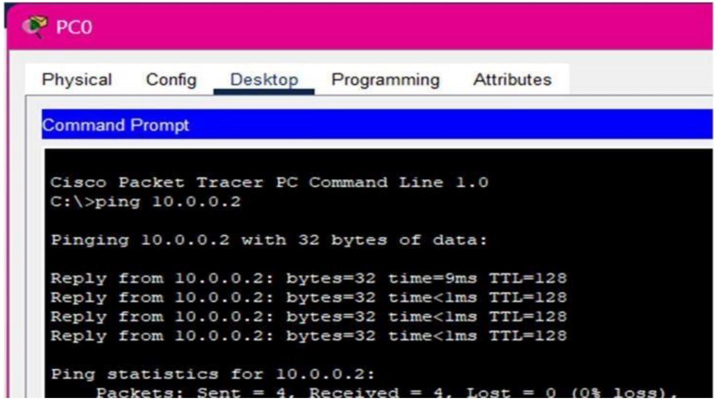
Subnet Mask 255.0.0.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

### Step 3: Testing Connectivity

Open command prompt on PC0 and enter command ping 10.0.0.2



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=9ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

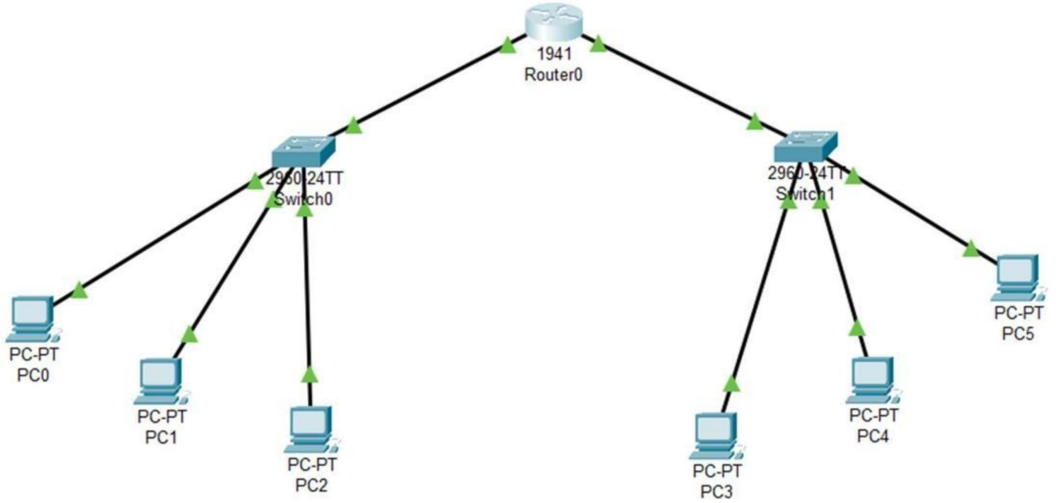
### Direct Connection Between End Devices Using a Switch and Router:

### Step 1: Setting Up Network Devices

1. Open Cisco Packet Tracer and create a new workspace.
2. Drag and drop a router (e.g., 1941) from the Network Devices section.

3. Drag and drop a switch (e.g., 2960) from the Network Devices section.

4. Drag and drop PCs from the End Devices section and connect it.



**Step 2: Configuring IP Addresses on End Devices**

1. Click on each device, go to Desktop > IP Configuration.

   ○ PC0: 10.0.0.1(Subnet Mask: 255.0.0.0) ○ PC1: 10.0.0.2(Subnet Mask: 255.0.0.0) ○ PC2: 10.0.0.3(Subnet Mask: 255.0.0.0) ○ PC3: 20.0.0.1(Subnet Mask: 255.0.0.0)

   ○ PC4: 20.0.0.2(Subnet Mask: 255.0.0.0)

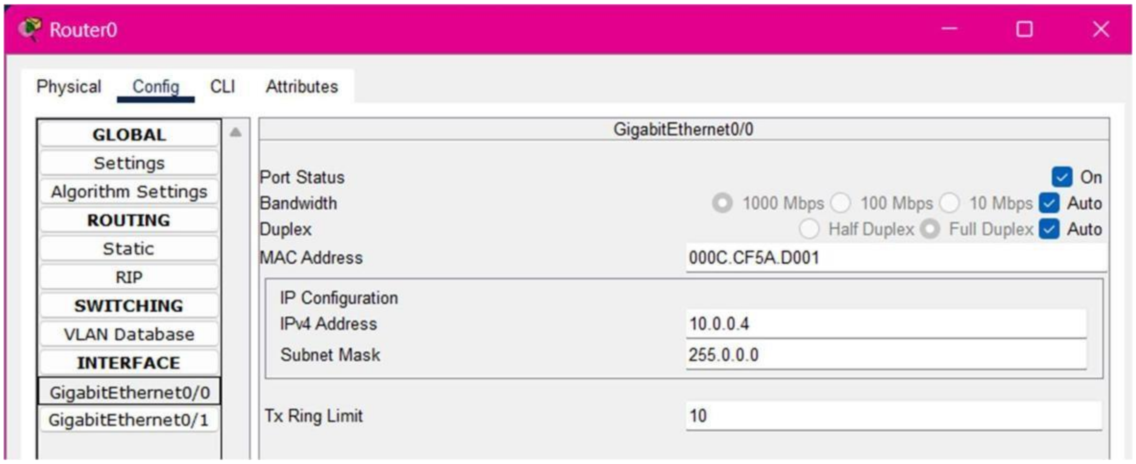
   ○ PC5: 20.0.0.3(Subnet Mask: 255.0.0.0)

**Step 3: Configuring the Router**

1. Click on the Router and go to the GUI Configuration tab.

2. Navigate to Interfaces and select GigabitEthernet0/0 and assign ip address as 10.0.0.4 then turn it ON.

3. Similarly, select GigabitEthernet0/1 and assign ip address as 20.0.0.4 then turn it ON.



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

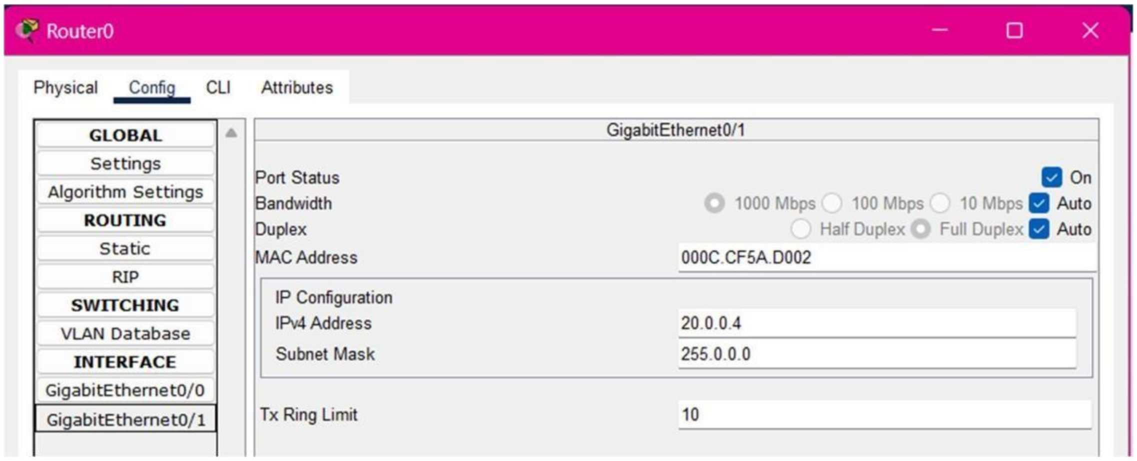
MAC Address 000C.CF5A.D001

IP Configuration

IPv4 Address 10.0.0.4

Subnet Mask 255.0.0.0

Tx Ring Limit 10



GigabitEthernet0/1

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 000C.CF5A.D002

IP Configuration

IPv4 Address 20.0.0.4

Subnet Mask 255.0.0.0

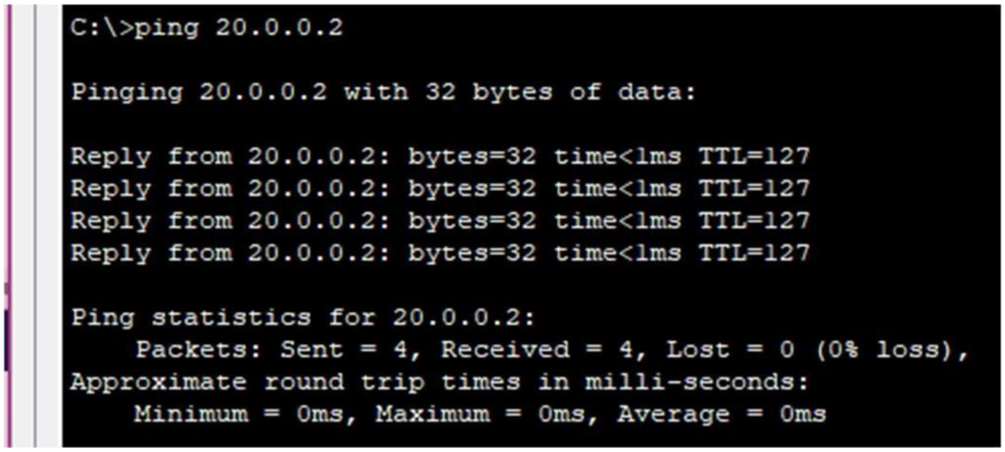
Tx Ring Limit 10

### Step 4: Set gateway

For devices connected to switch0, set Default Gateway: 10.0.0.4 and devices connected to switch1, set Default Gateway: 20.0.0.4

### Step 5: Testing Connectivity

1. Open the Command Prompt on each PC.
2. Use the ping command to test connectivity:



```
C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time<1ms TTL=127
Reply from 20.0.0.2: bytes=32 time<1ms TTL=127
Reply from 20.0.0.2: bytes=32 time<1ms TTL=127
Reply from 20.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

## COMPUTER NETWORKS LAB FILE

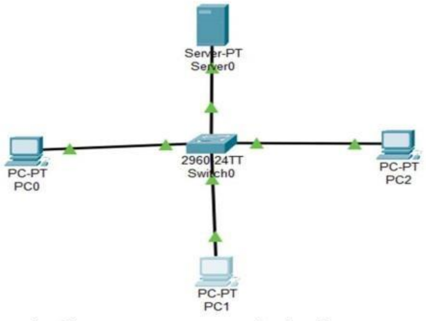
## Experiment No.5

**Objective**: To configure a DHCP server on a router device. Assign IP addresses dynamically to devices on the network and verify successful address assignment. (Using packet Tracer)

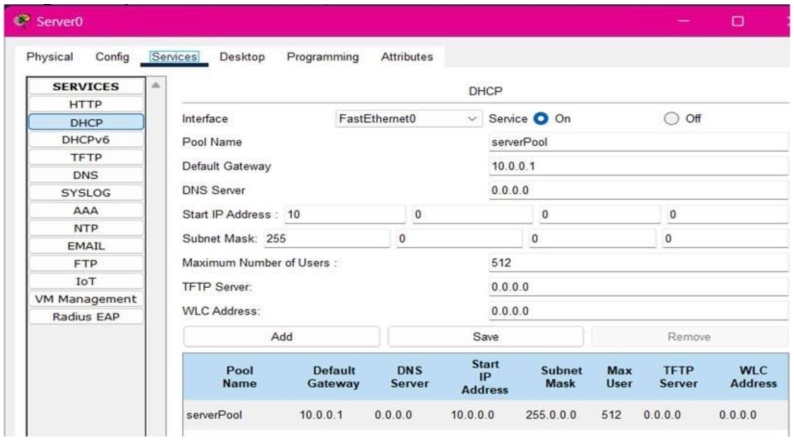
**Theory:** Dynamic Host Configuration Protocol (DHCP) is a network protocol that automatically assigns IP addresses and configuration settings to devices, reducing manual effort and preventing conflicts. It follows a DORA process (Discovery, Offer, Request, Acknowledgment) to allocate IPs dynamically.

**Procedure:**

1. Connect multiple devices to a switch and add a server to the network.



2. Assign an IP address to the server, navigate to the service section, enable DHCP, set the default gateway as the server's IP, and turn on the service.



Interface: FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 10.0.0.1

DNS Server: 0.0.0.0

Start IP Address : 10 0 0 0

Subnet Mask: 255 0 0 0

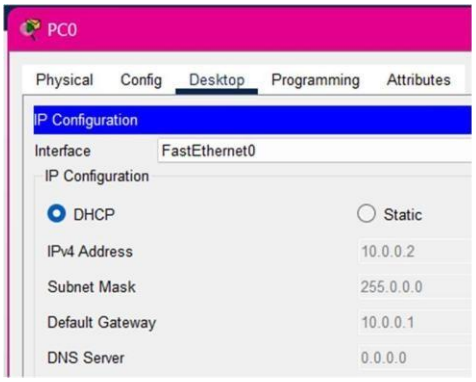
Maximum Number of Users : 512

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

| Pool Name | Default Gateway | DNS Server | Start IP Address | Subnet Mask | Max User | TFTP Server | WLC Address |
|---|---|---|---|---|---|---|---|
| serverPool | 10.0.0.1 | 0.0.0.0 | 10.0.0.0 | 255.0.0.0 | 512 | 0.0.0.0 | 0.0.0.0 |

3. On each device, go to the IP address settings, select the DHCP option, and obtain the assigned IP address and repeat the process for all remaining devices to ensure proper IP allocation



Interface: FastEthernet0

IP Configuration

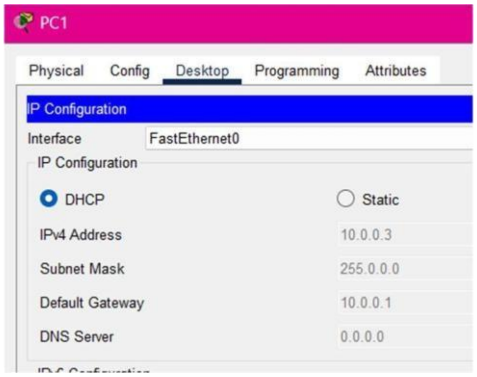
● DHCP ○ Static

IPv4 Address: 10.0.0.2

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server: 0.0.0.0



Interface: FastEthernet0

IP Configuration

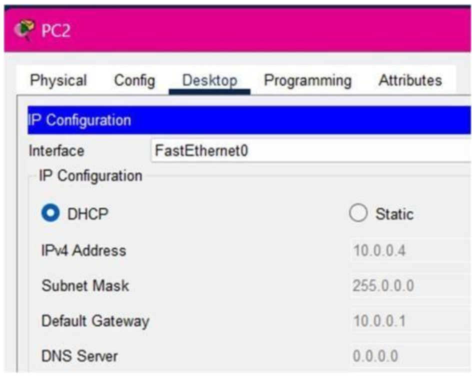
● DHCP ○ Static

IPv4 Address: 10.0.0.3

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server: 0.0.0.0



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 10.0.0.4

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

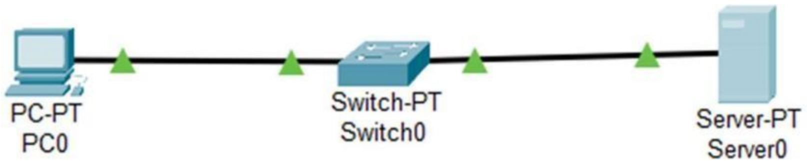
DNS Server: 0.0.0.0

## Experiment No.6

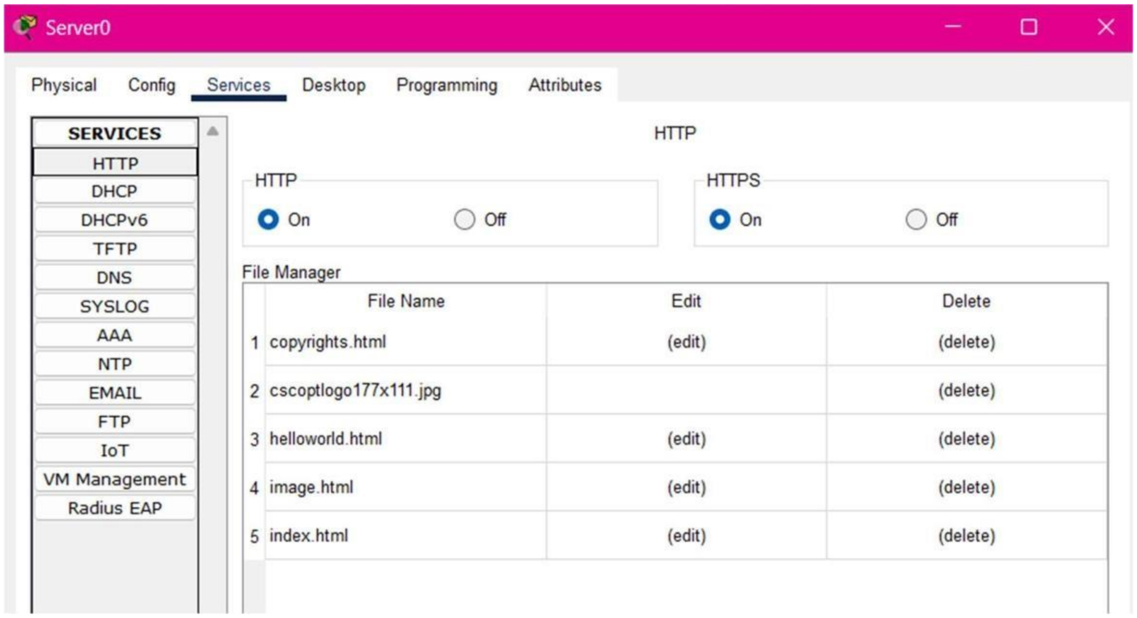
**Objective:** To configure a local DNS server to resolve domain names within a network. (Using packet Tracer).

**Steps to Configure the Network and Access the Web Page**

1. **Assemble the Network:**
   - Connect the end device and switch to a server.



2. **Configure the Server:**
   - Click on the server. o Assign an **IP address** to the server.
   - Set the **same IP address** as the **DNS server address**.
3. **Enable HTTP Service:**
   - Click on **Services** in the server settings. o Go to the **HTTP** option.
   - Locate the **index file**, edit it, and save the changes.



HTTP

HTTP ● On ○ Off

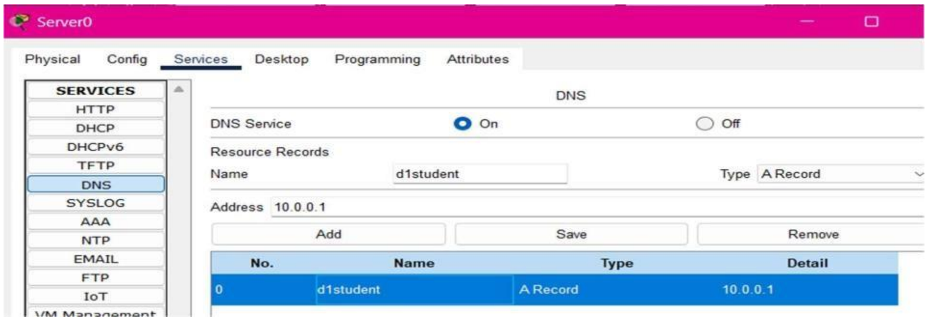
HTTPS ● On ○ Off

File Manager

| | File Name | Edit | Delete |
|---|---|---|---|
| 1 | copyrights.html | (edit) | (delete) |
| 2 | cscoptlogo177x111.jpg | | (delete) |
| 3 | helloworld.html | (edit) | (delete) |
| 4 | image.html | (edit) | (delete) |
| 5 | index.html | (edit) | (delete) |

4. **Configure DNS Service:**

- o Click on the **DNS** option and turn it **ON**. o Assign a **name** to the DNS entry.
- o Set the **DNS record address** the same as the **DNS server address**.



DNS Service ● On ○ Off

Resource Records

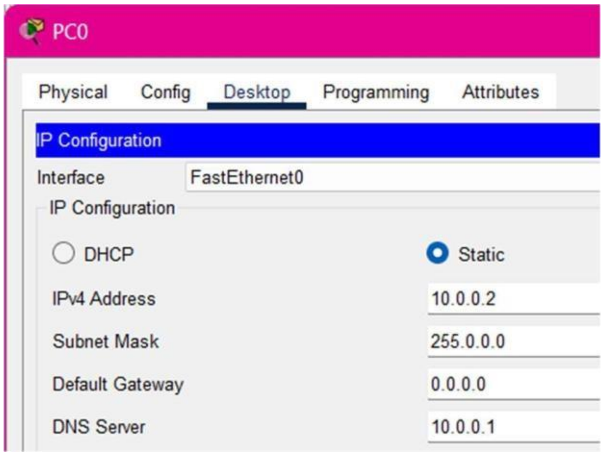
Name d1student Type A Record

Address 10.0.0.1

| No. | Name | Type | Detail |
|---|---|---|---|
| 0 | d1student | A Record | 10.0.0.1 |

5. **Configure the End Device:**

- o Assign an **IP address** to the end device and add the **DNS server address**



Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address 10.0.0.2

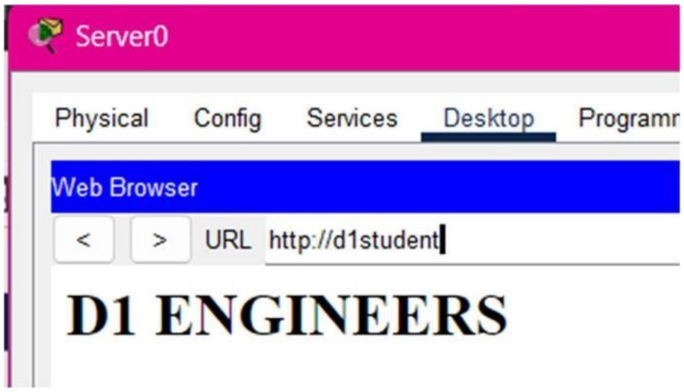
Subnet Mask 255.0.0.0

Default Gateway 0.0.0.0

DNS Server 10.0.0.1

6. **Test the Webpage:**

- o Go to the **server** and open the **web browser**.
- o **Search using the name** assigned in the DNS server settings. o Check the **result** to verify the webpage is loading correctly.



URL http://d1student

D1 ENGINEERS

# 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**

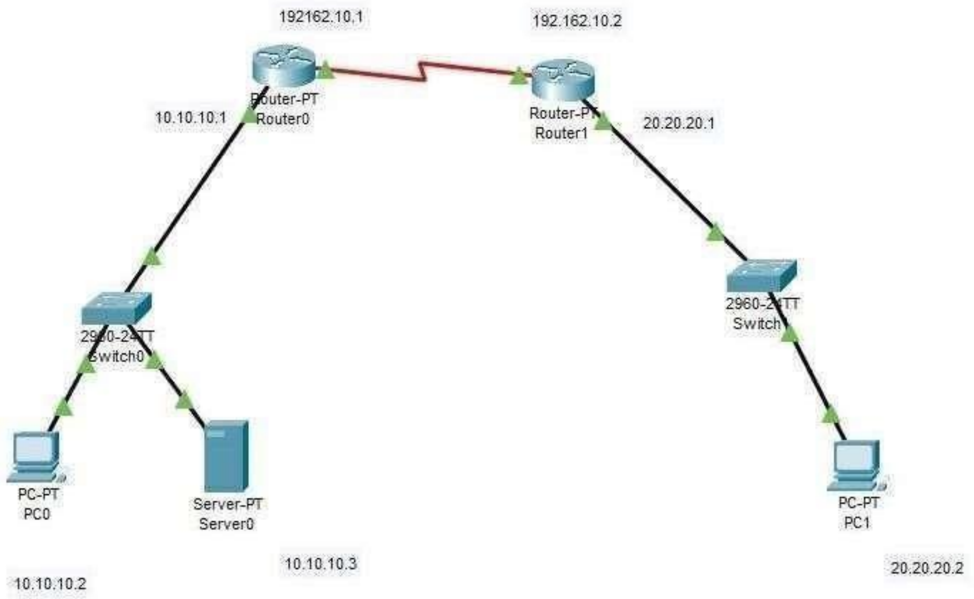
1. Open packet Tracer.

2. Add the following Devices to the workspace:

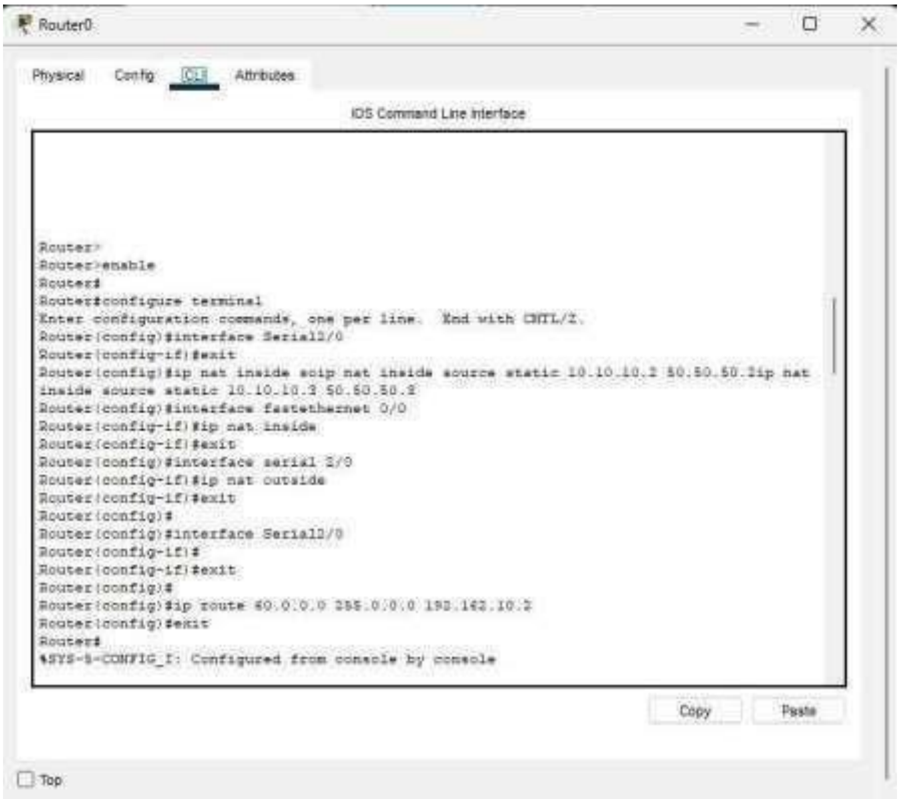
- 2 Router
- 2 PC
- 2 Switch
- 1 Server

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
```



```
Router>
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial2/0
Router(config-if)#exit
Router(config)#ip nat inside soip nat inside source static 10.10.10.2 50.50.50.2ip nat
inside source static 10.10.10.3 50.50.50.3
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
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

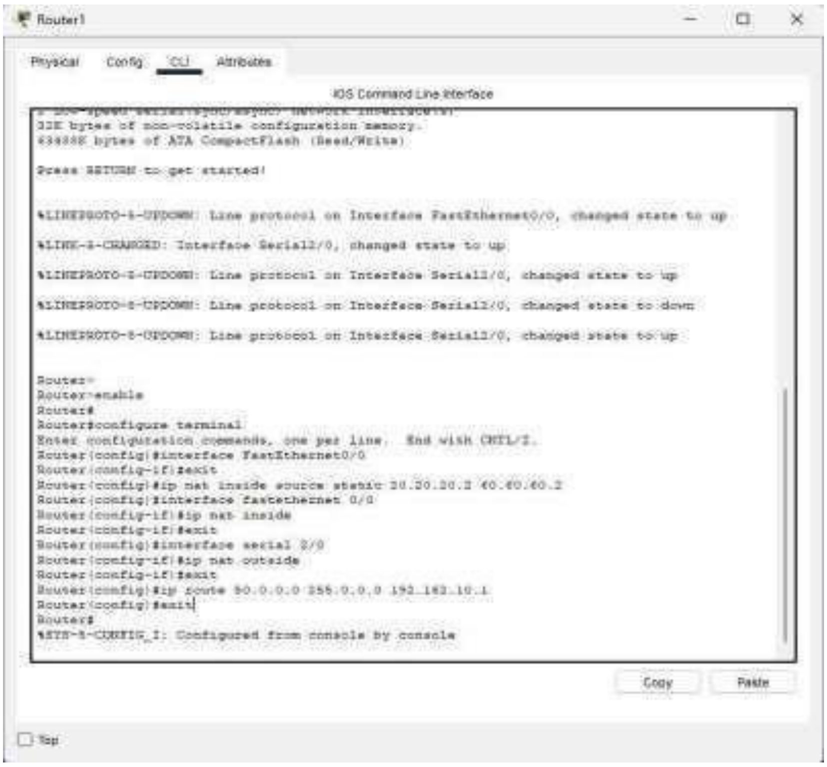
4. Assign IP address to router1 in Config.

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
```



```
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up


Router>
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
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

5. Configure the Server

a) Click on Server0

b) Go to the Services tab

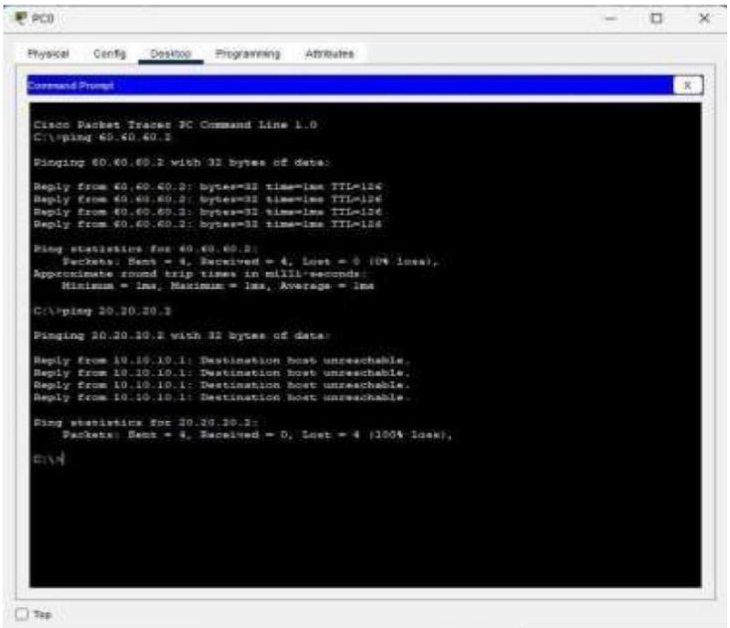
c) Click on HTTP.
d) Ensure the HTTP services is ON.

e) Edit text in index.html

6. Test the translation

1) Verify pass message PC0 to PC1

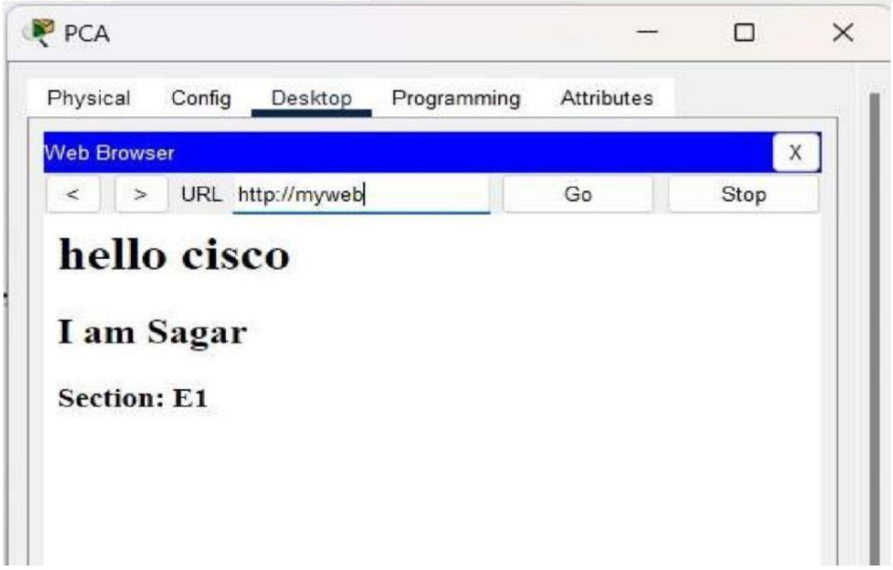
- Click on PC0
- Ping 60.60.60.2 (get reply)
- Ping 20.20.20.2 (unreachable hide ip private)



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 60.60.60.2

Pinging 60.60.60.2 with 32 bytes of data:

Reply from 60.60.60.2: bytes=32 time=1ms TTL=126
Reply from 60.60.60.2: bytes=32 time=1ms TTL=126
Reply from 60.60.60.2: bytes=32 time=1ms TTL=126
Reply from 60.60.60.2: bytes=32 time=1ms TTL=126

Ping statistics for 60.60.60.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

2) Check for server

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



URL http://myweb

hello cisco

I am Sagar

Section: E1

# 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

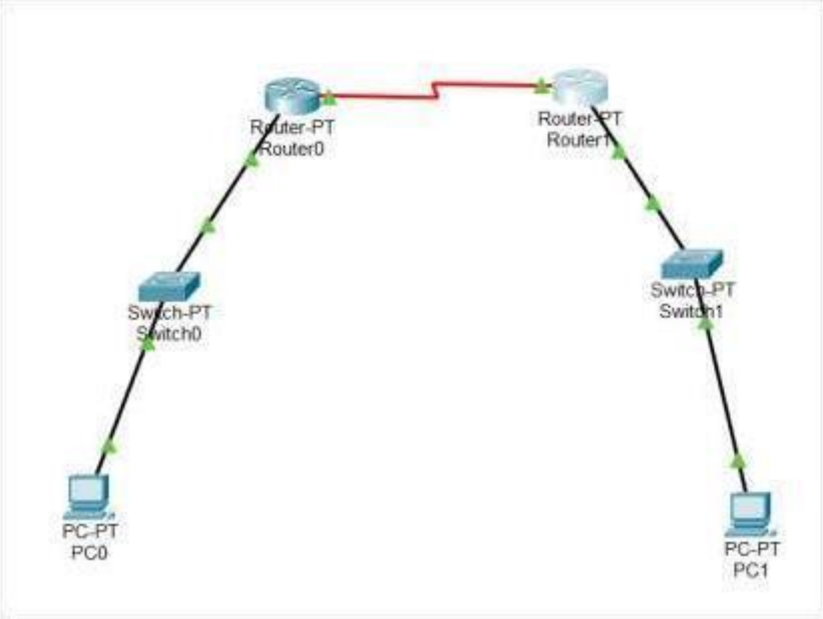
1. **Step 1: Set Up the Devices** ○ Open Cisco Packet Tracer. Add the following devices to the workspace:

- ✦ 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).

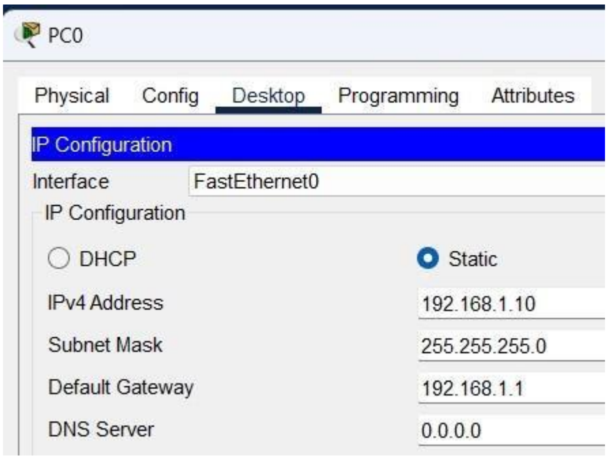


2. **Step 2: Assign IP Addresses (with an intentional error)** ○ **PC**

**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.*



IP Configuration

Interface: FastEthernet0

IP Configuration

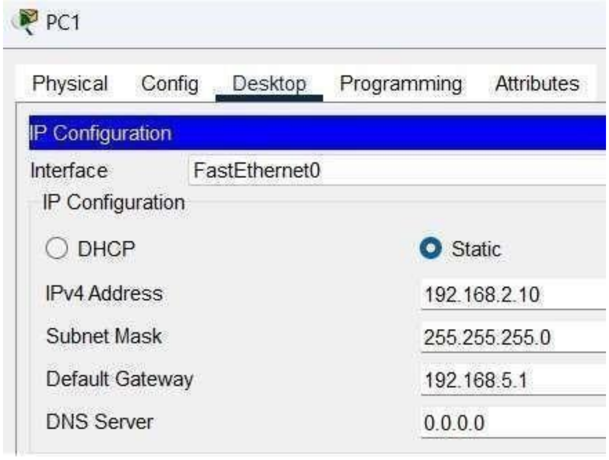
○ DHCP ● Static

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.2.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.5.1

DNS Server: 0.0.0.0

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

  Click Router0 → **CLI** tab. Enter:

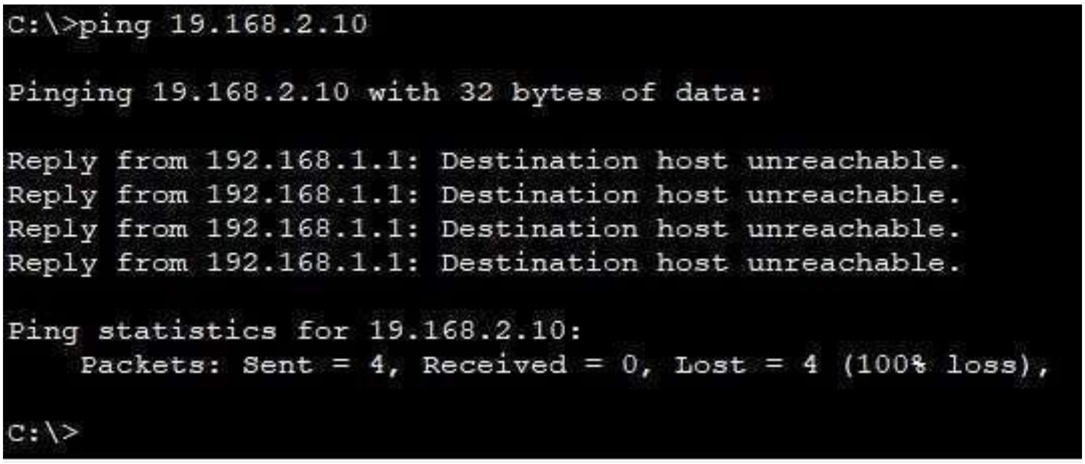
```
Router0> enable
Router0# configure terminal
Router0(config)# interface FastEthernet0/0
Router0(config-if)# ip address 192.168.1.1 255.255.255.0
Router0(config-if)# no shutdown
Router0(config-if)# exit
Router0(config)# interface Serial2/0
Router0(config-if)# ip address 10.0.0.1 255.255.255.252
Router0(config-if)#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

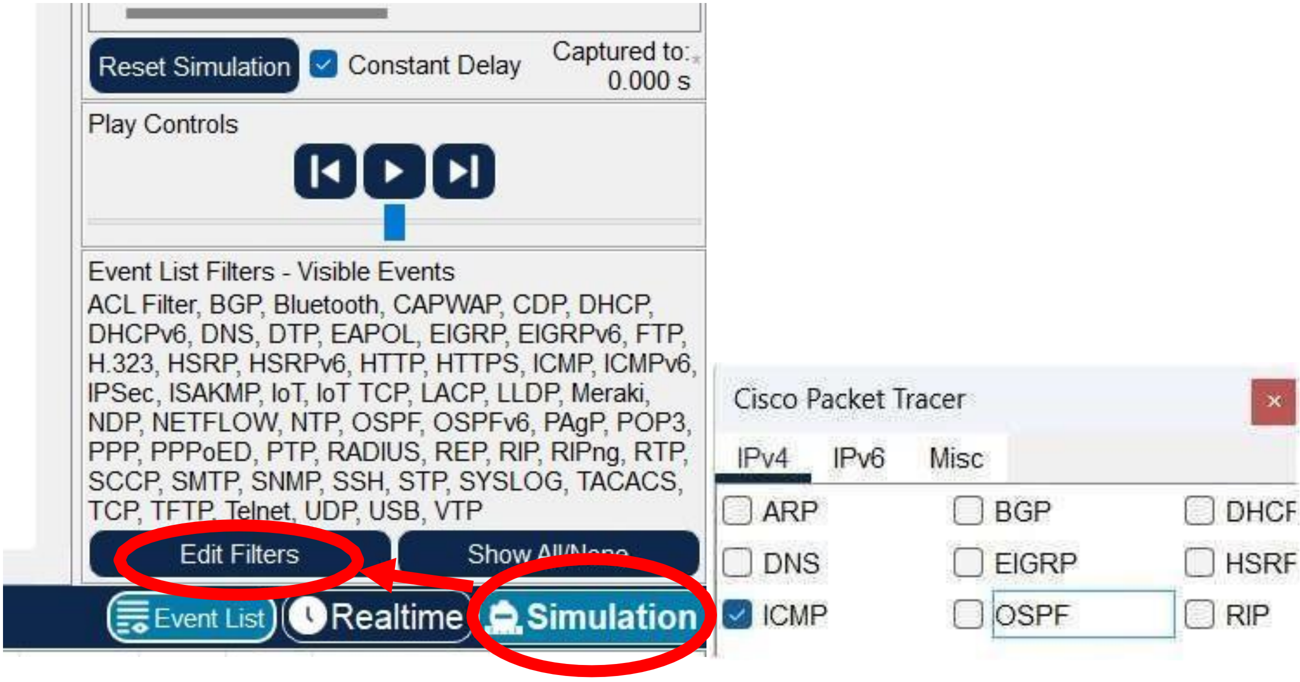
```
Router1> enable
Router1# configure terminal
Router1(config)# interface FastEthernet0/0
Router1(config-if)# ip address 192.168.2.1 255.255.255.0
Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1(config)# interface Serial2/0
Router1(config-if)# ip address 10.0.0.2 255.255.255.252
Router1(config-if)#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



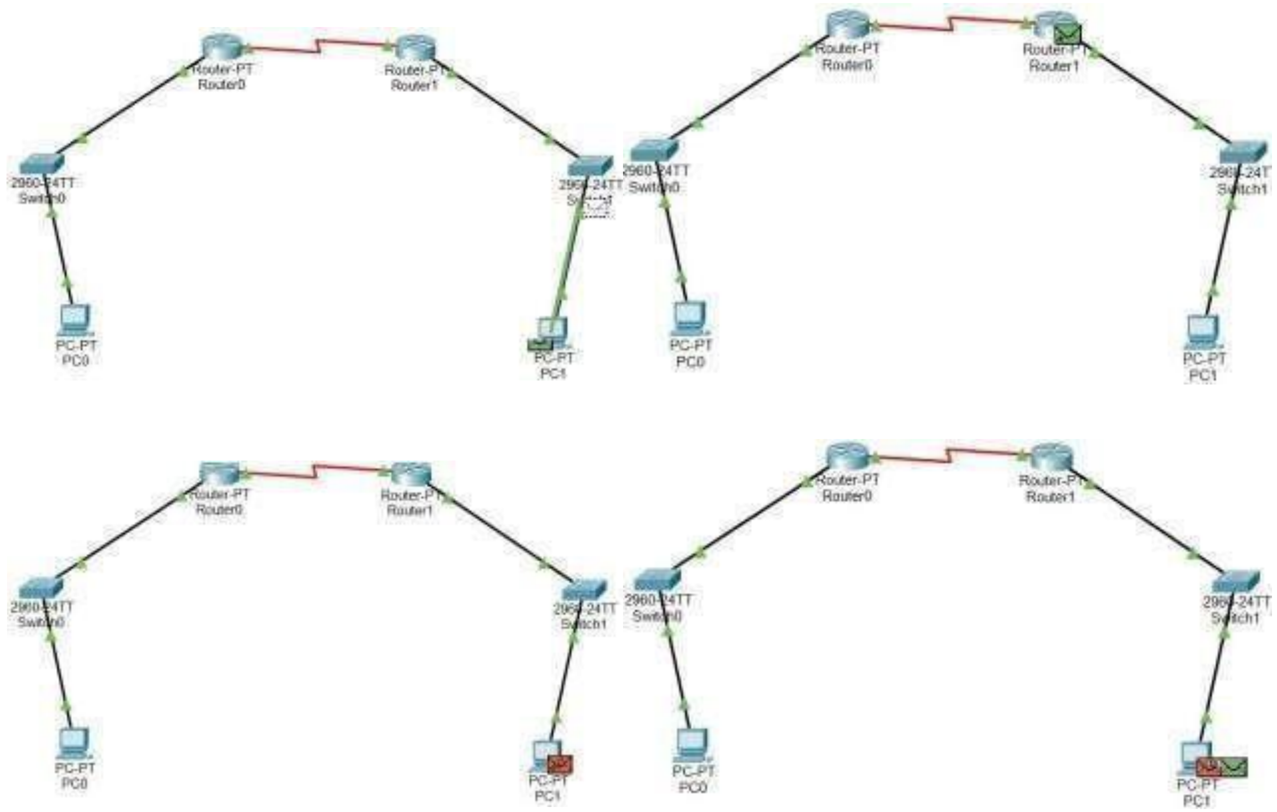
☑ Constant Delay

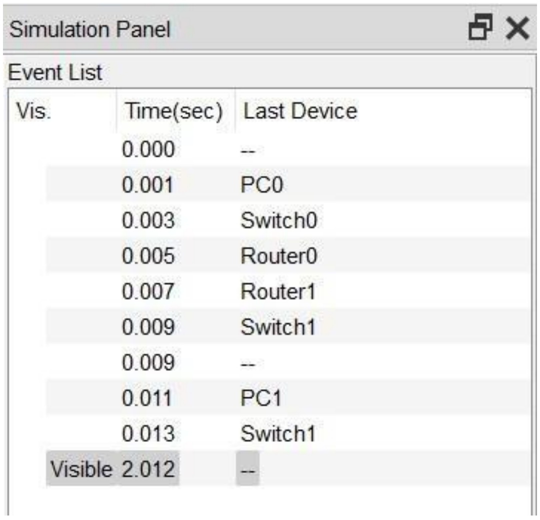
Event List Filters - Visible Events

ACL Filter, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

| | | |
|---|---|---|
| □ ARP | □ BGP | □ DHCF |
| □ DNS | □ EIGRP | □ HSRF |
| ☑ ICMP | □ OSPF | □ RIP |

- ○ 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).



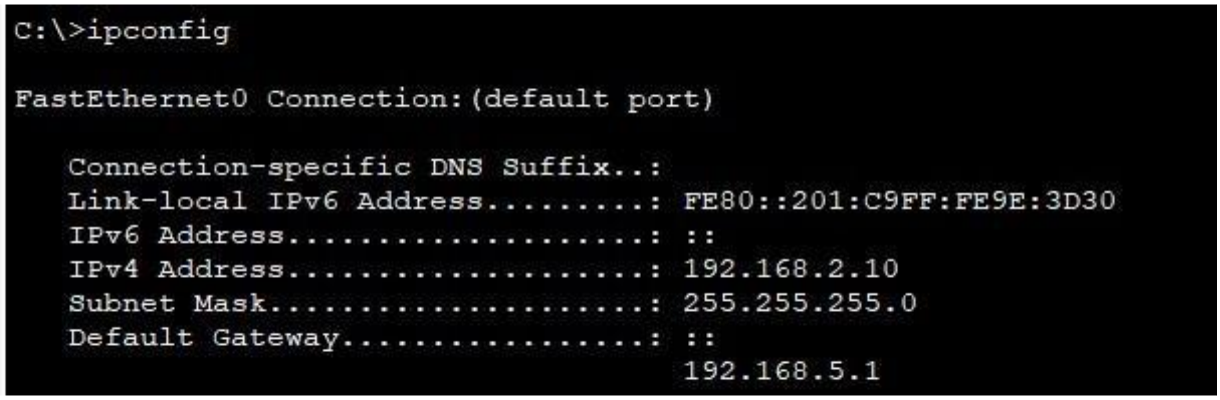


Event List

| 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).

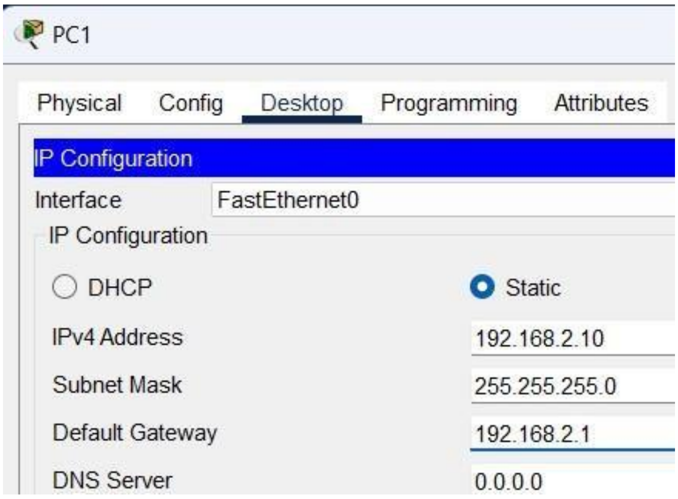
- Alternatively, on **Router1** CLI, use show ip interface brief to verify Router1's Fa0/0 address is 192.168.2.1, confirming the gateway should be that.

- 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.



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

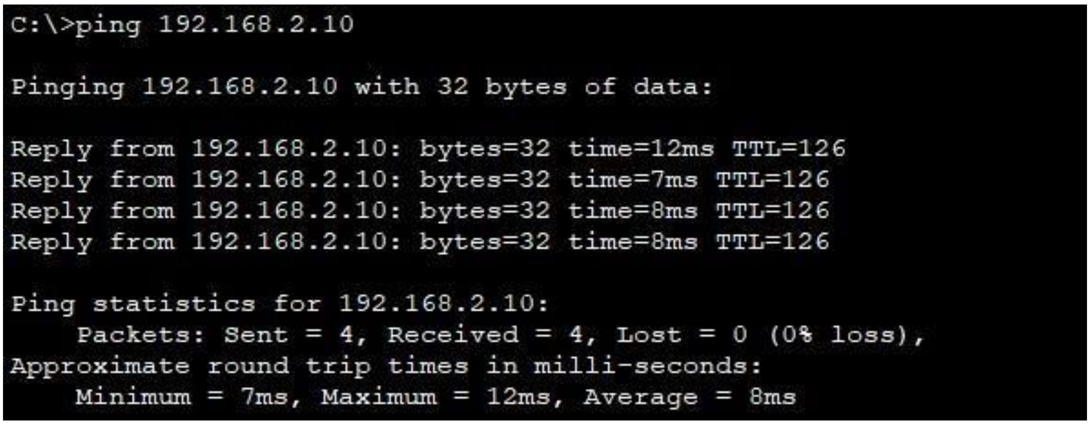
IPv4 Address: 192.168.2.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

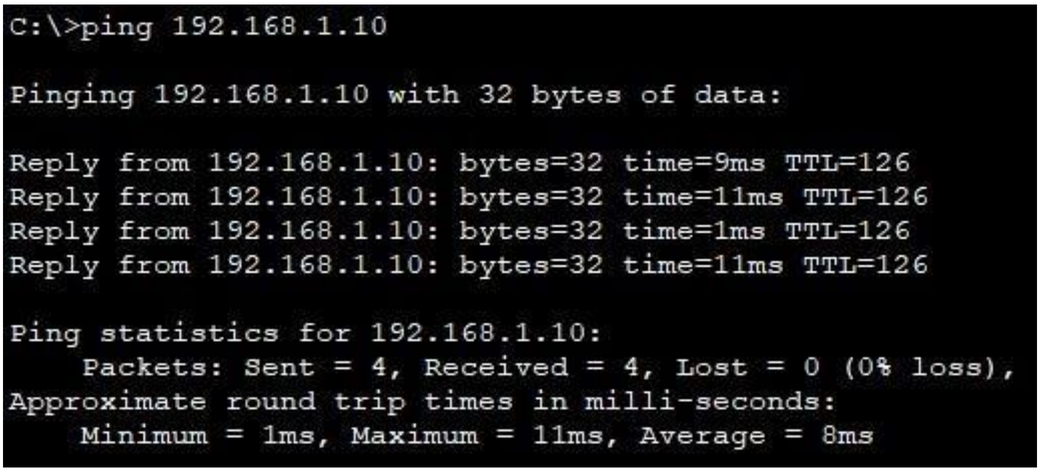
6. **Step 6: Verify Connectivity (Ping - Should Succeed)** On **PC0**, in Command Prompt, run the ping again: ○ PC> ping 192.168.2.10



```
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.

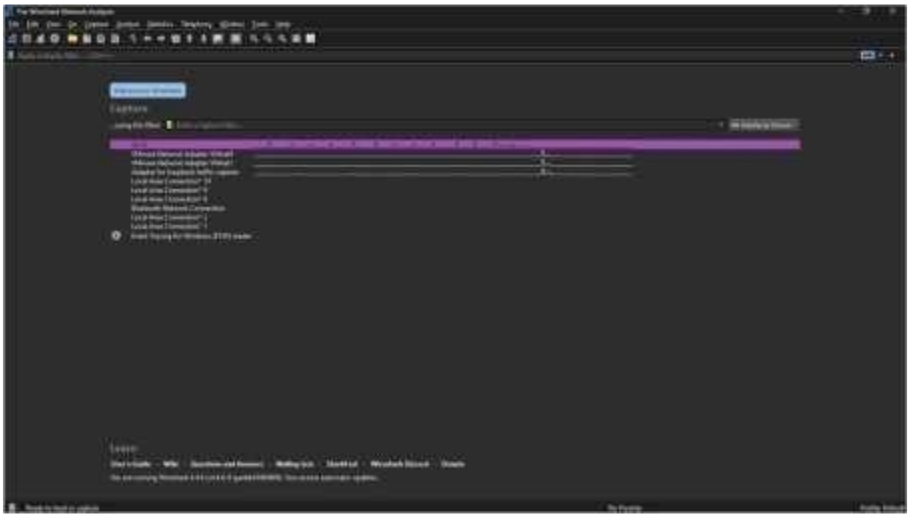
**Procedure**:

**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.

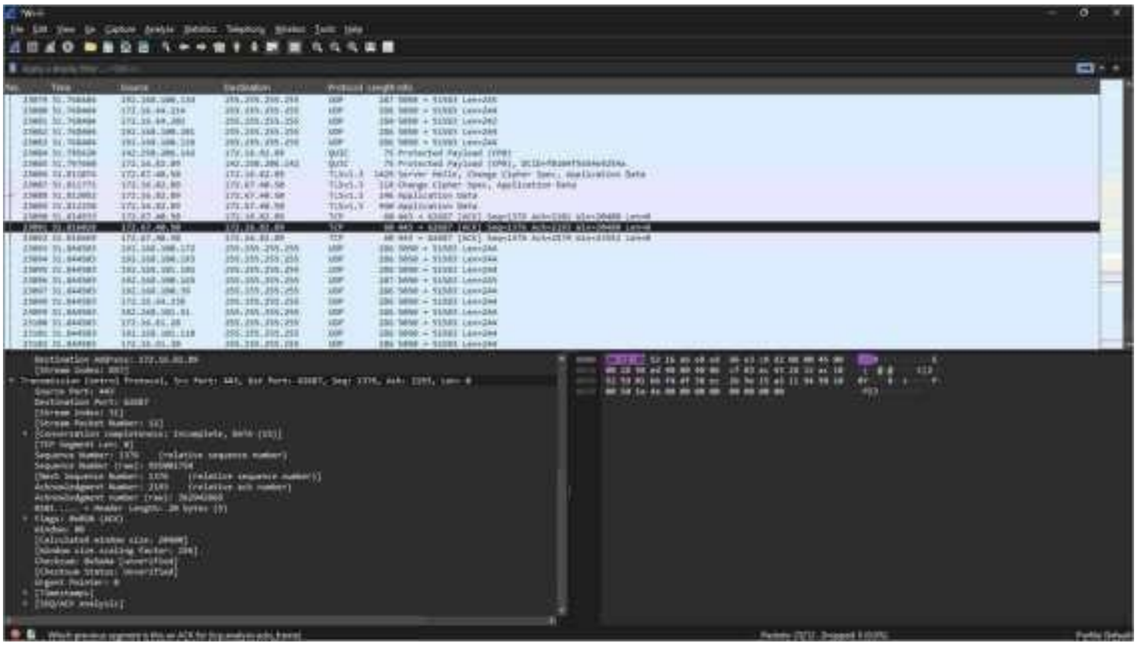
- Open a web browser and visit any website (e.g., [www.google.com](http://www.google.com)) to generate traffic.

**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.

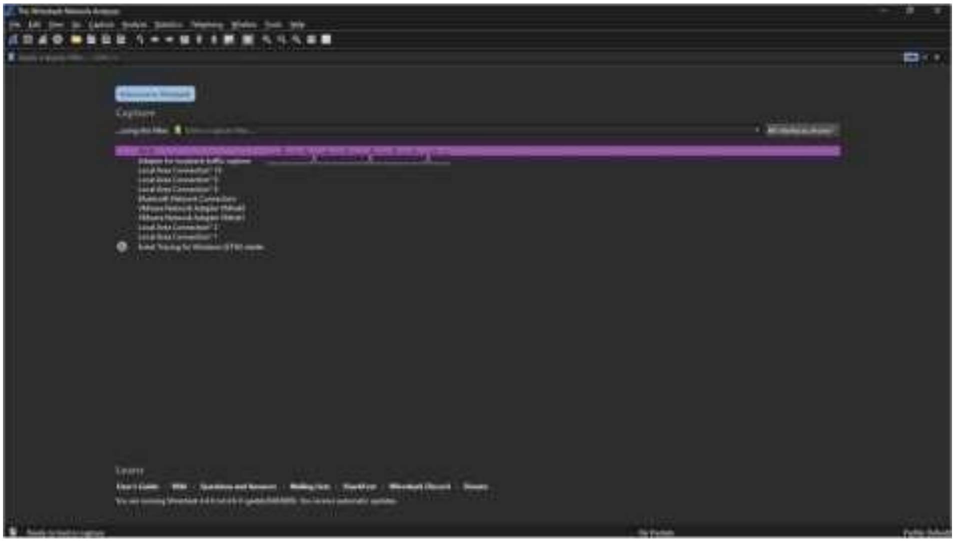
**Procedure**:

**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).


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Welcome to Wireshark
Capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Ready to load or capture
No Packets
Profile: Default

Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Local Area Connection* 2
Local Area Connection* 1
Event Tracing for Windows (ETW) reader

**Step 3**: Start capturing packets.

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

**Step 4**: Run Some TCP Traffic

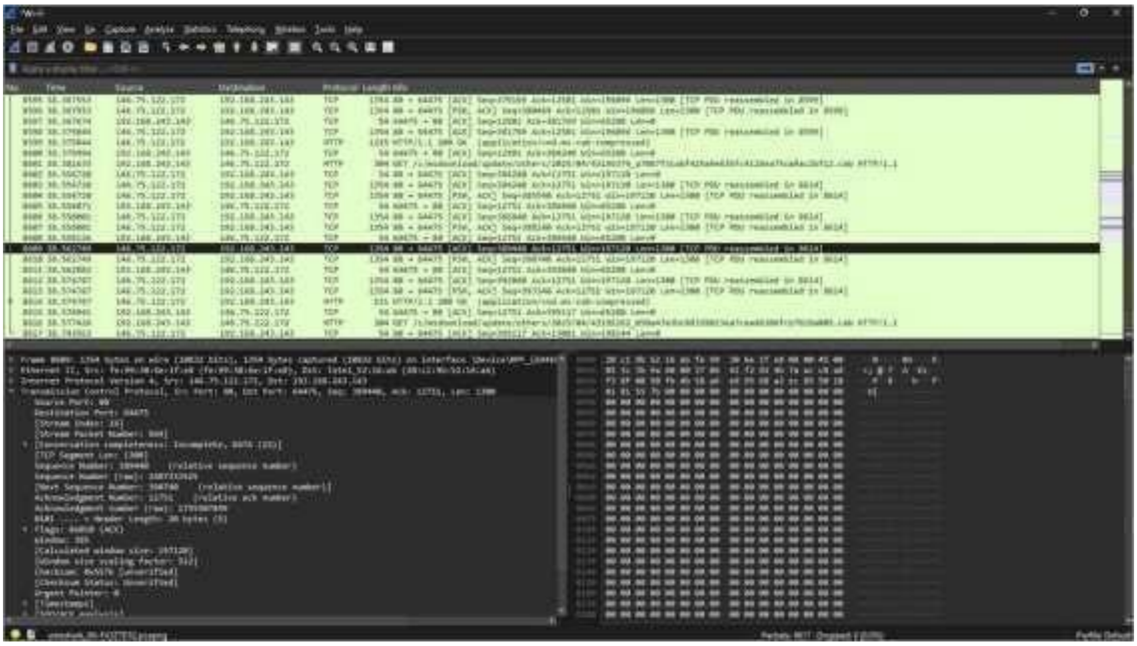
- Open a web browser (Chrome, Firefox, Edge).
- Visit a website like https://www.google.com or https://www.wikipedia.org. (Websites use TCP).

**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.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info

**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