Experiment No.1

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

Theory:

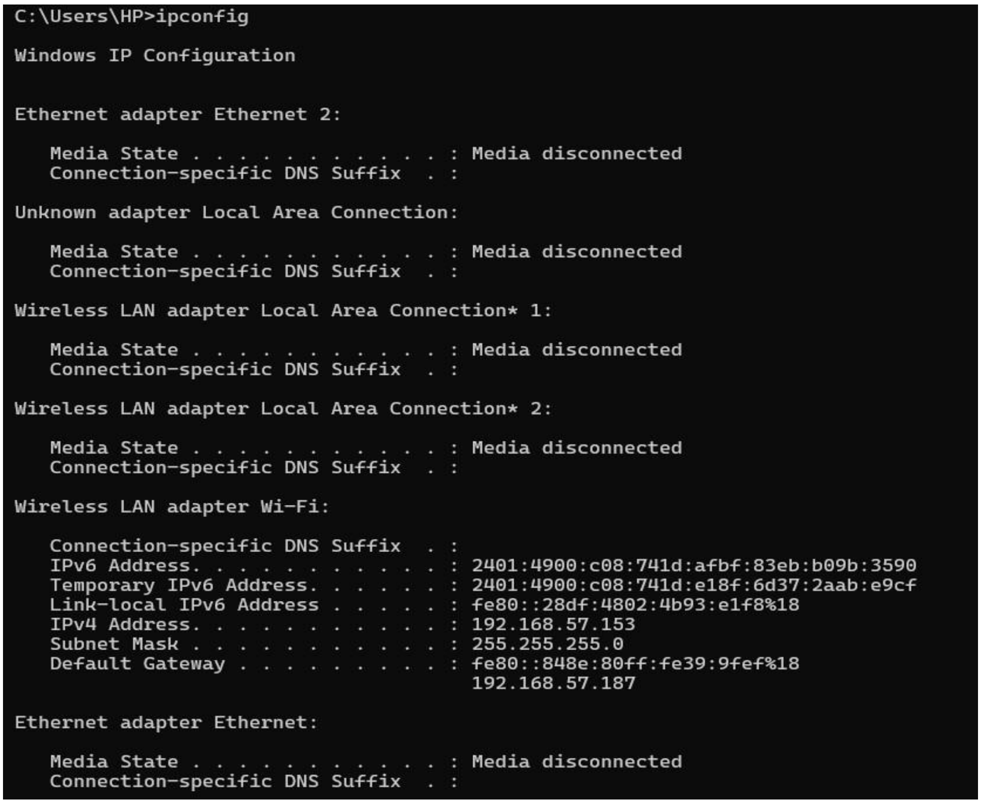
1) **ipconfig -** The ipconfig command is used in Windows to display and manage the network configuration of a computer. It provides details about the IP addresses, subnet masks, and default gateways for all network adapters.

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.

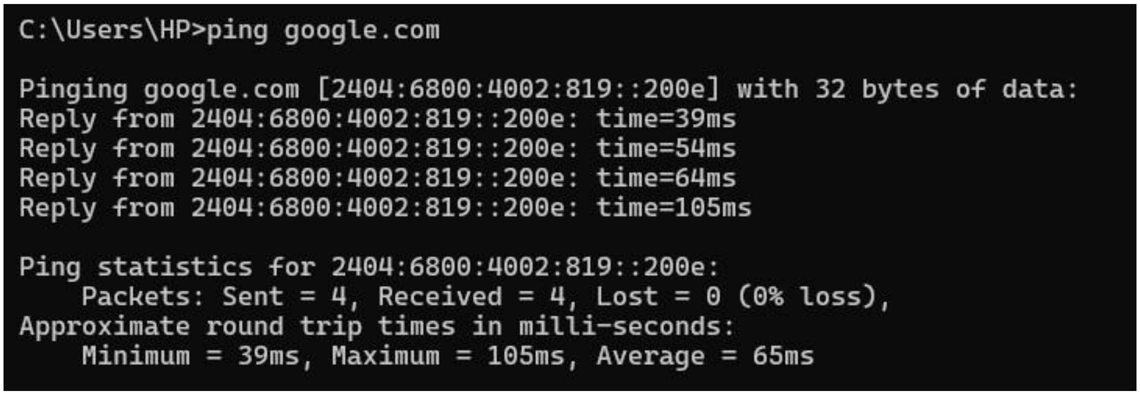
ipconfig



```
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.

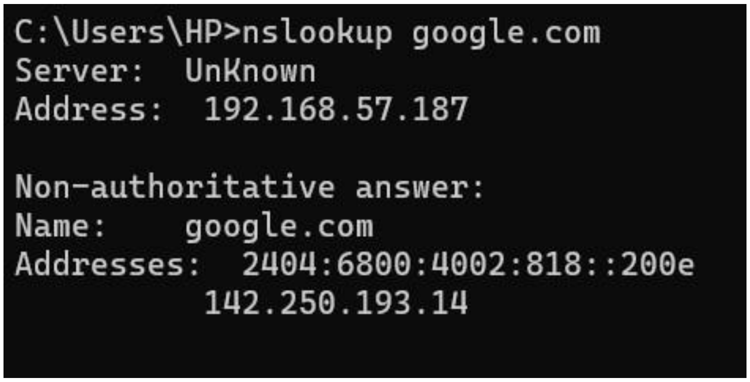
ping



```
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.

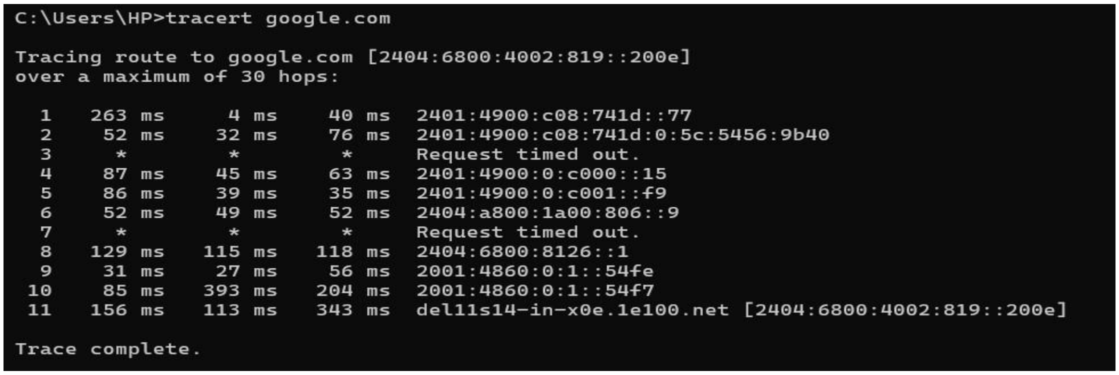
nslookup



```
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.

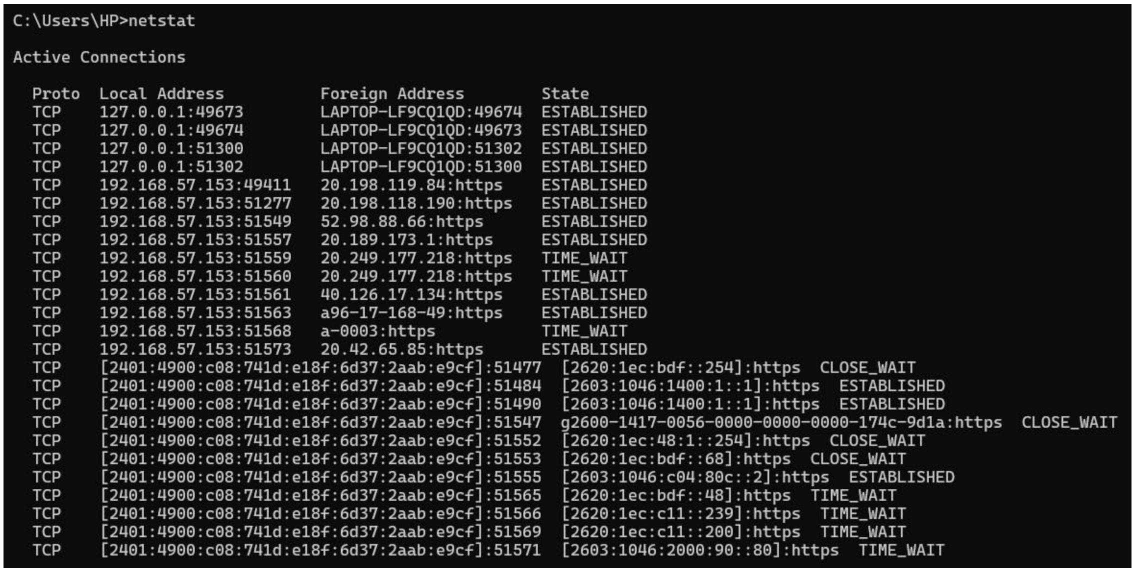
tracert



```
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. –

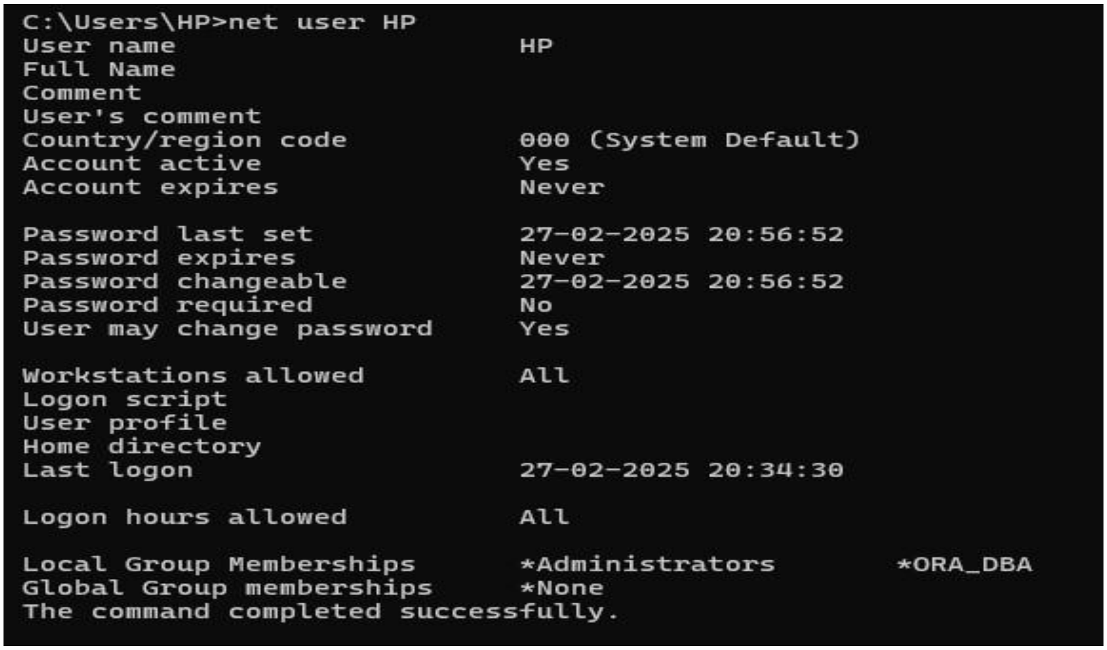
netstat



```
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.

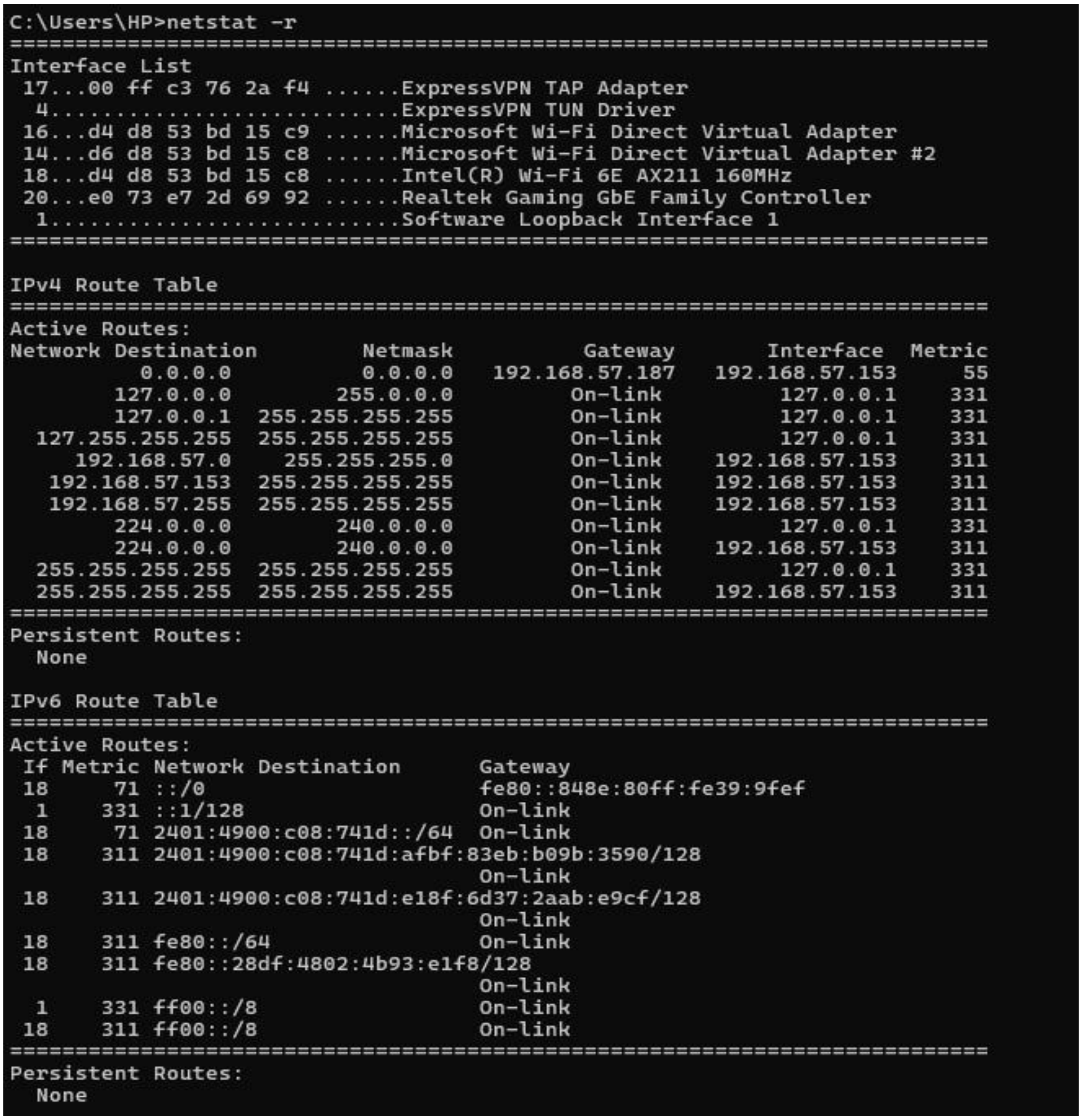
Net user<username>



```
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.

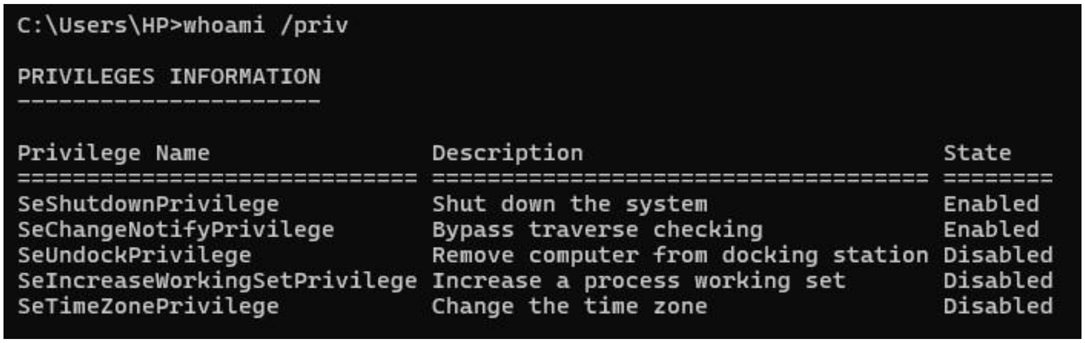
netstat -r



```
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

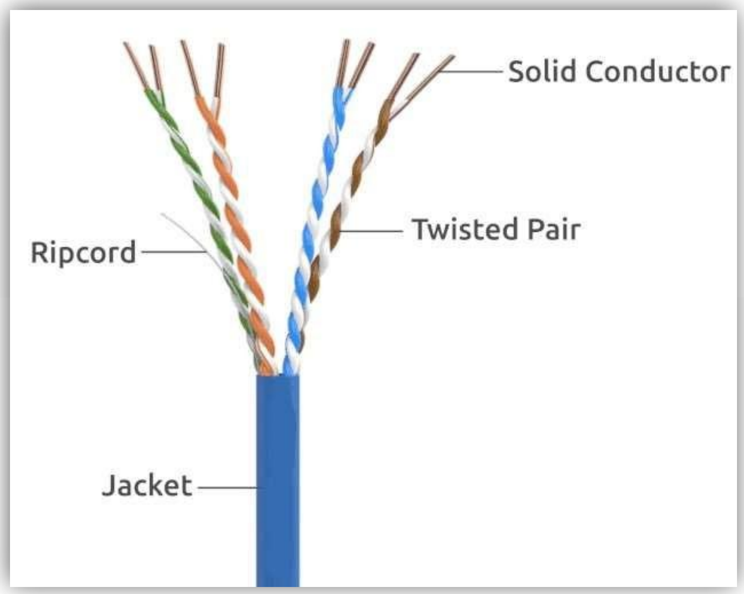
Objective: Familiarization with Transmission media and tools: Co-axial cable, UTP cable, Crimping tool, Connectors etc. Preparing the UTP cable for cross and direct connection using crimping tool.

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

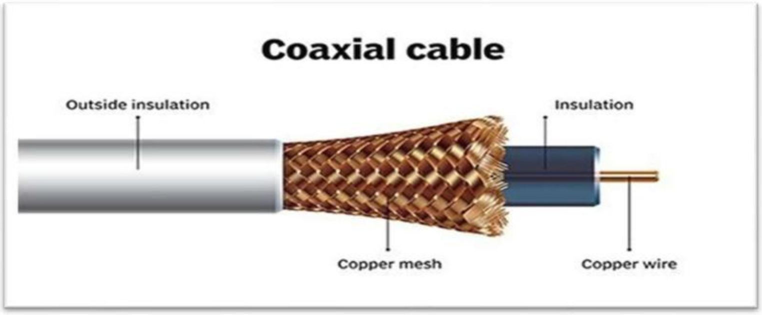
- High Signal Quality – Better resistance to interference than twisted pair cables.
- Durable and Shielded – Protects against electromagnetic and radio frequency interference.

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

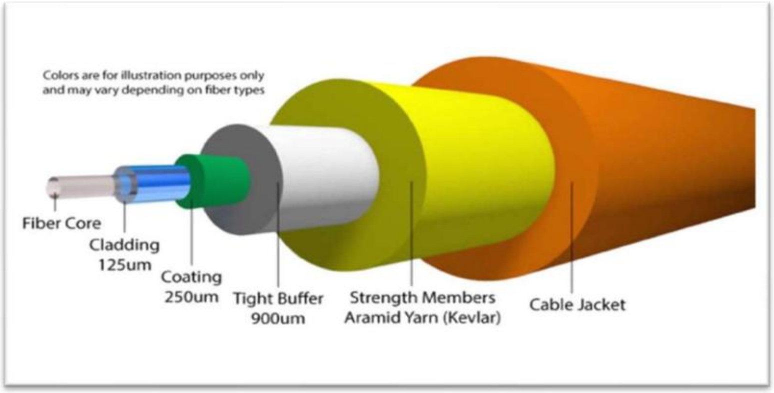
- High Speed – Supports speeds up to 100 Gbps or more.
- Long Distance – Can transmit data over hundreds of kilometers with minimal signal loss.
- Less Interference – Immune to electromagnetic interference (EMI) from electrical devices.

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.

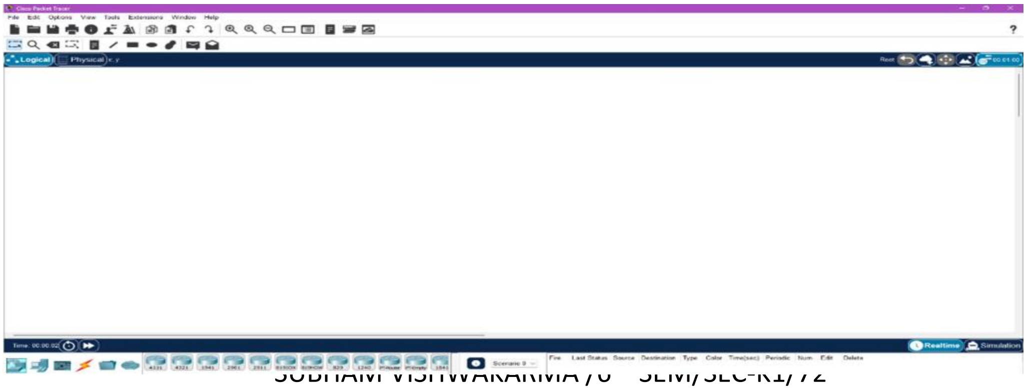
Installation Steps:

- 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.


Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
Root
Time: 00:00:02
Realtime
Simulation
4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841
Scenario 0
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete

Experiment No.4

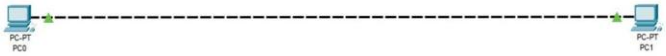
Objective: Build a simple network topology with routers, switches, and end devices such as PCs or laptops. Configure IP addresses and confirm connectivity between the devices using Packet Tracer.

Procedure:

Direct Connection Between End Devices:

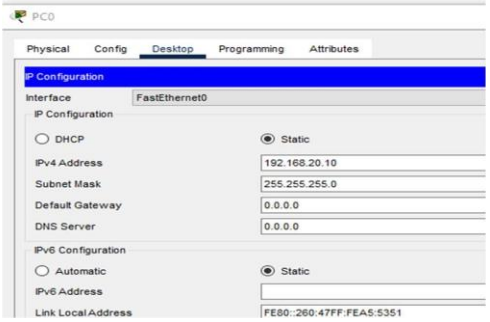
Step 1: Setting Up Network Devices

- 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

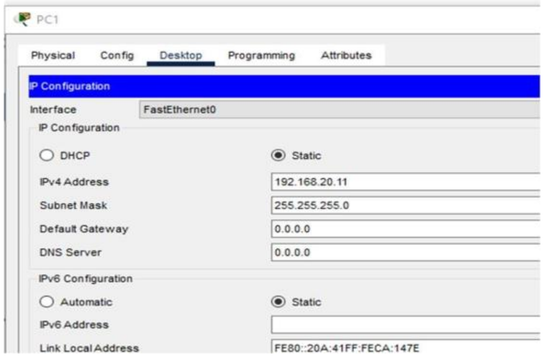
DNS Server: 0.0.0.0

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

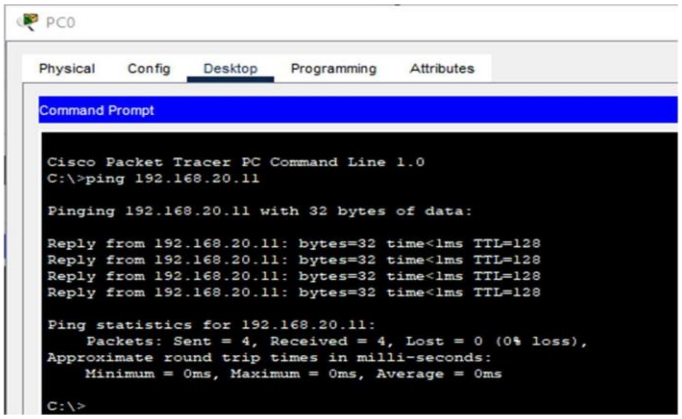
○ Automatic ● Static

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.

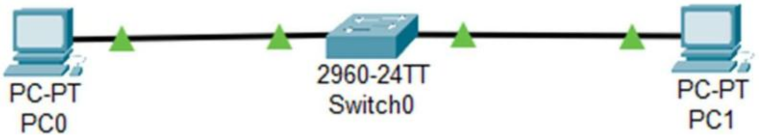


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.11

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.



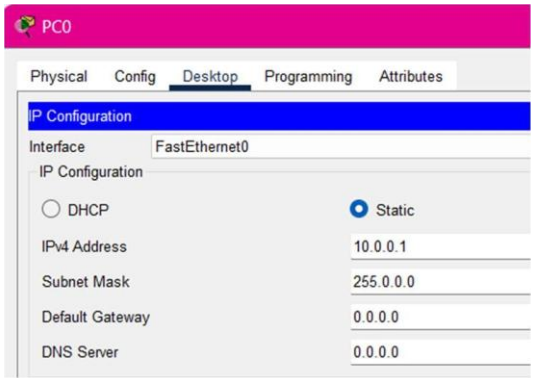
Step 2: Configuring IP Addresses on End Devices

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)



Interface: FastEthernet0

IP Configuration

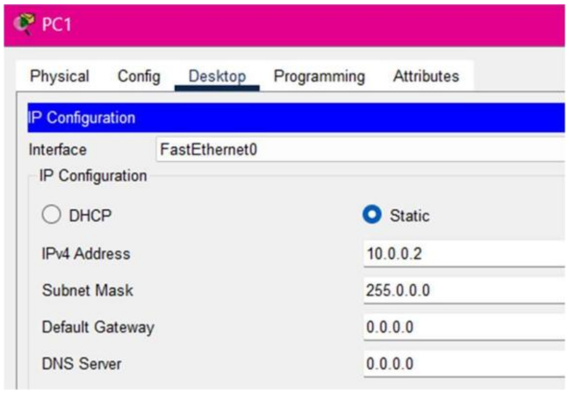
○ DHCP ● Static

IPv4 Address: 10.0.0.1

Subnet Mask: 255.0.0.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 10.0.0.2

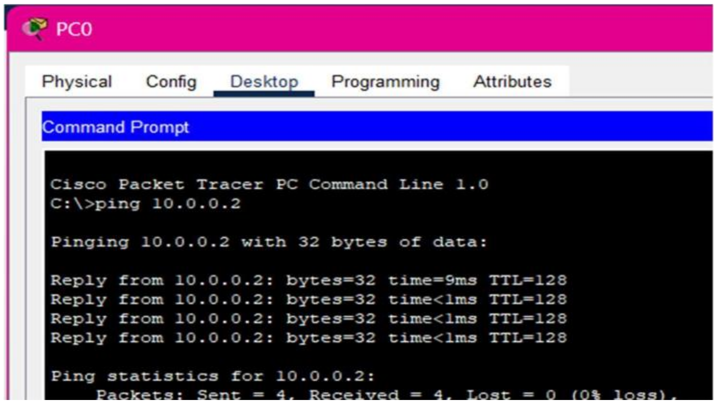
Subnet Mask: 255.0.0.0

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

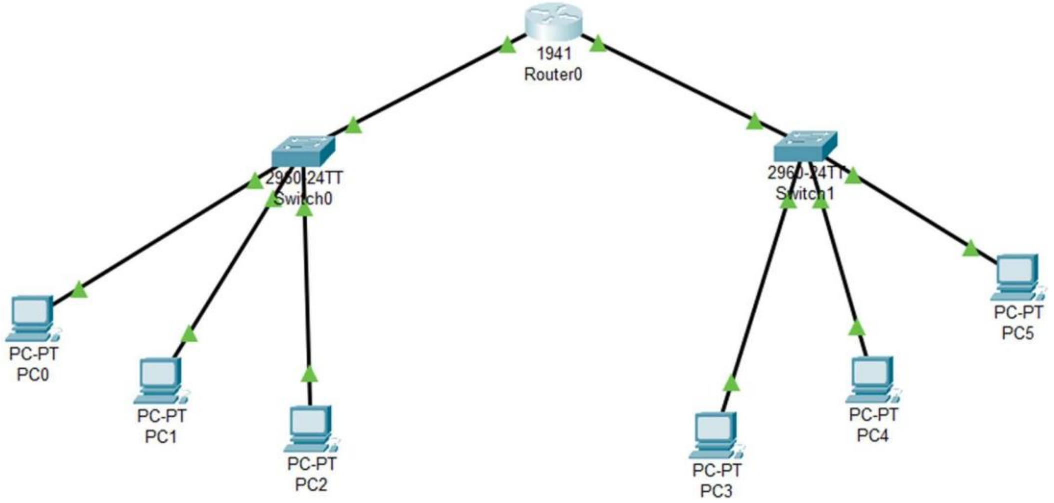


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

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.

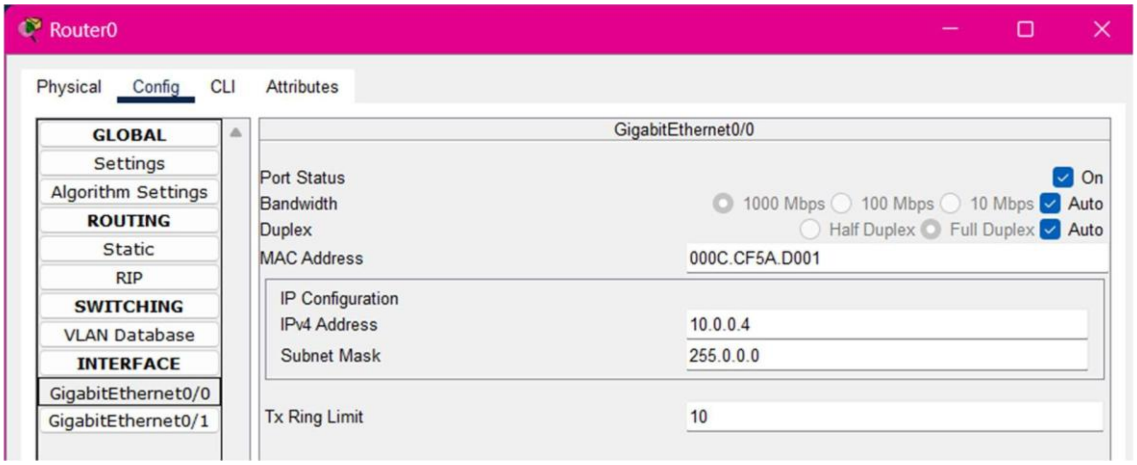


Step 2: Configuring IP Addresses on End Devices

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)

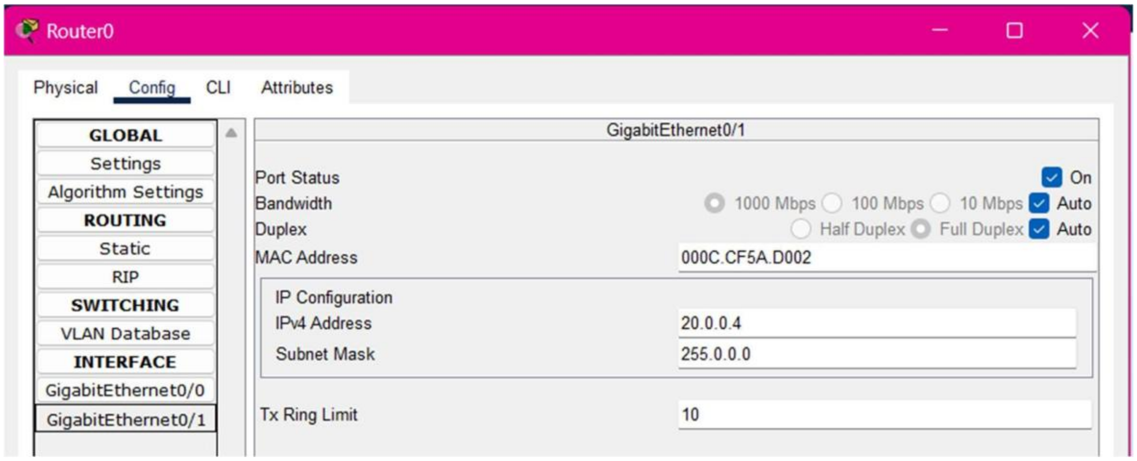
Step 3: Configuring the Router

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

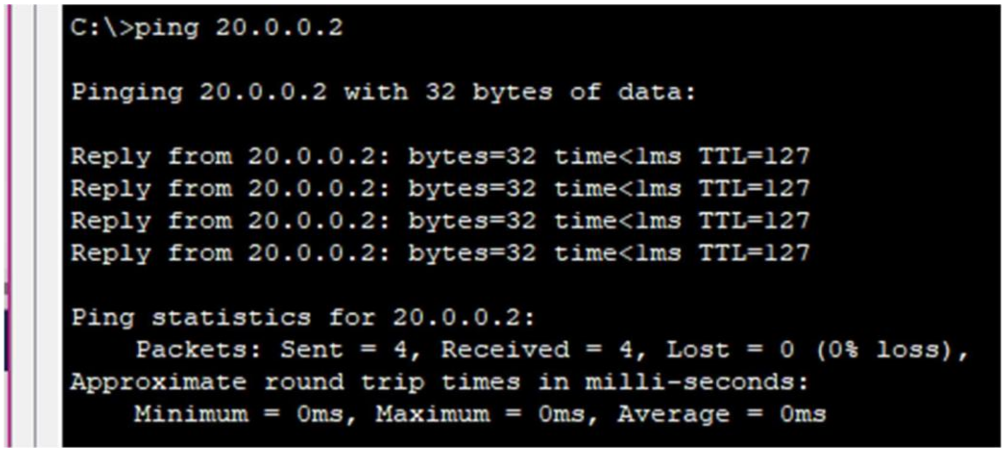
Port Status	☑ On
Bandwidth	● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto
Duplex	○ Half Duplex ● Full Duplex ☑ Auto
MAC Address	000C.CF5A.D002
IP Configuration	
IPv4 Address	20.0.0.4
Subnet Mask	255.0.0.0
Tx Ring Limit	10

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
```

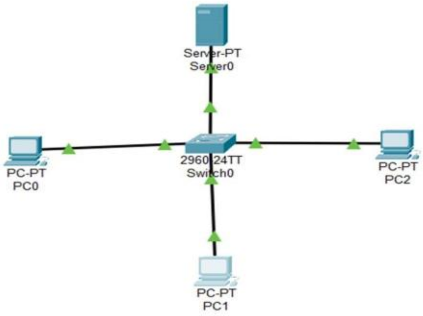
Experiment No.5

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)

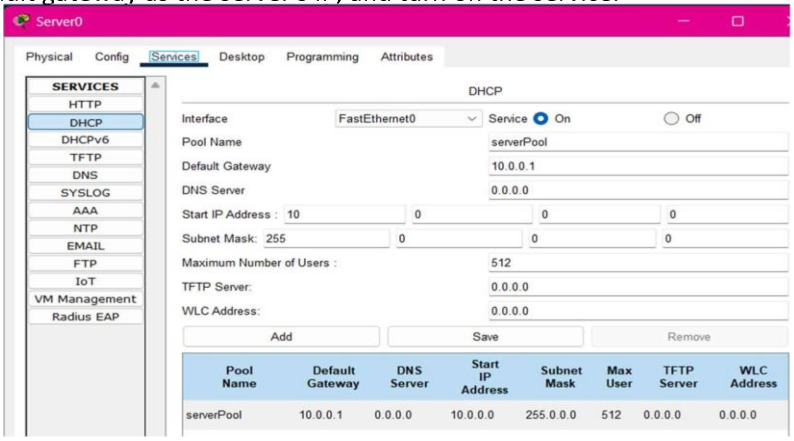
Theory: Dynamic Host Configuration Protocol (DHCP) is a network protocol that automatically assigns IP addresses and configuration settings to devices, reducing manual effort and preventing conflicts. It follows a DORA process (Discovery, Offer, Request, Acknowledgment) to allocate IPs dynamically.

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.

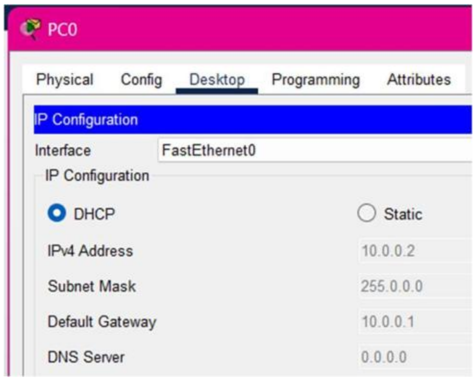


DHCP

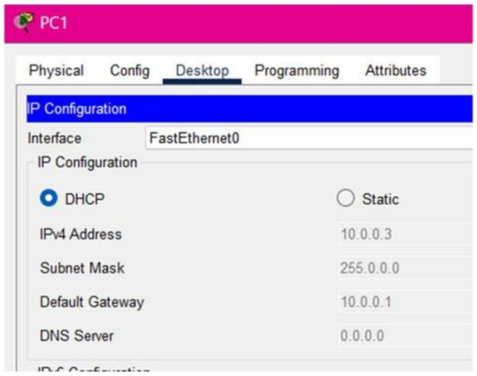
Interface: FastEthernet0
Service: ● On ○ Off
Pool Name: serverPool
Default Gateway: 10.0.0.1
DNS Server: 0.0.0.0
Start IP Address : 10 0 0 0
Subnet Mask: 255 0 0 0
Maximum Number of Users : 512
TFTP Server: 0.0.0.0
WLC Address: 0.0.0.0

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

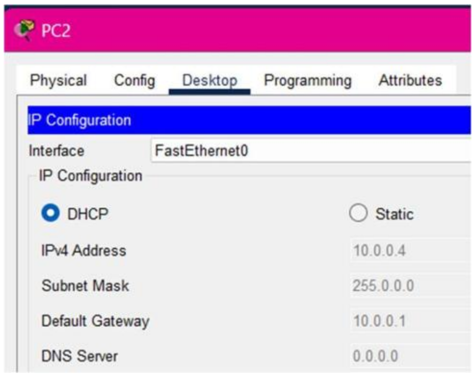
3. On each device, go to the IP address settings, select the DHCP option, and obtain the assigned IP address and repeat the process for all remaining devices to ensure proper IP allocation



IP Configuration
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



IP Configuration
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



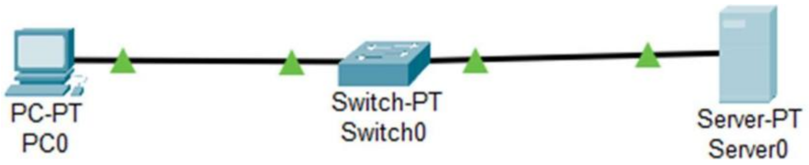
IP Configuration
Interface: FastEthernet0
IP Configuration
● DHCP ○ Static
IPv4 Address: 10.0.0.4
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server: 0.0.0.0

Experiment No.6

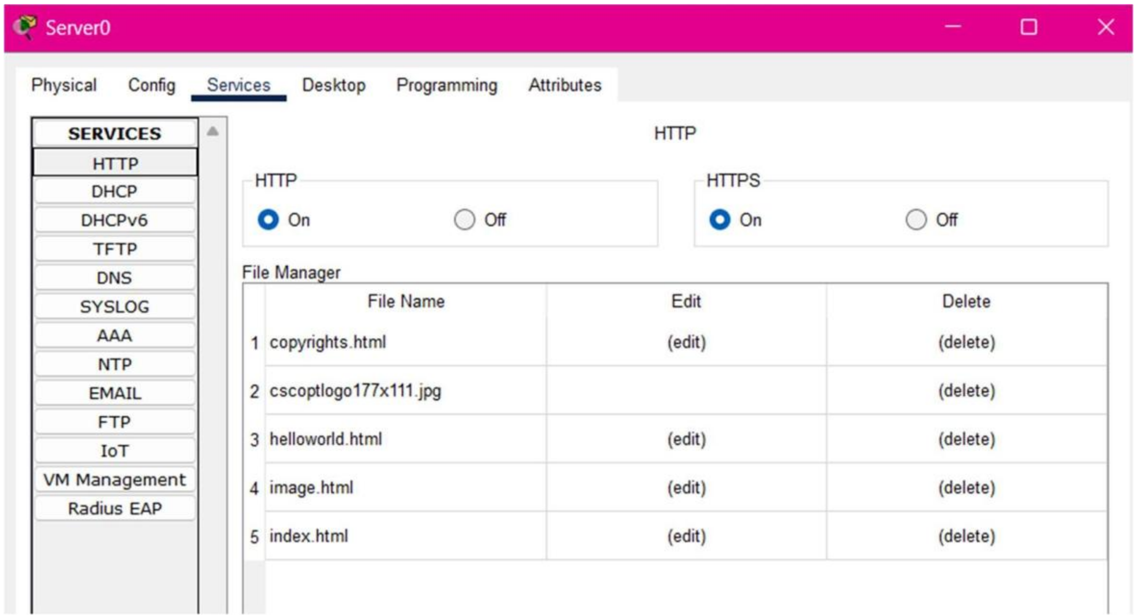
Objective: To configure a local DNS server to resolve domain names within a network. (Using packet Tracer).

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.
   - 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.
   - Go to the **HTTP** option.
   - Locate the **index file**, edit it, and save the changes.



HTTP

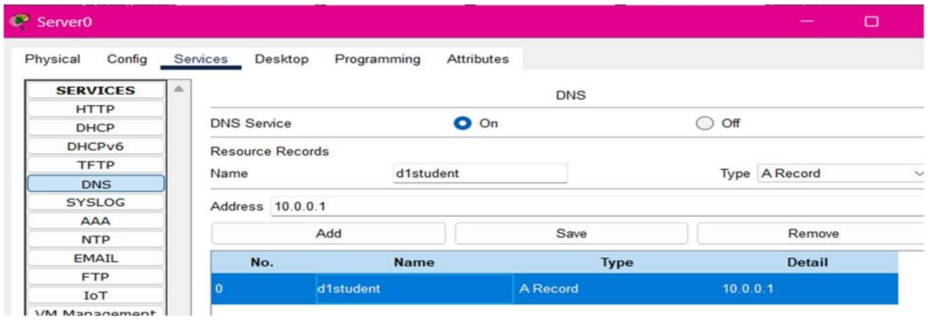
HTTP: ● On ○ Off

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



DNS

DNS Service ● On ○ Off

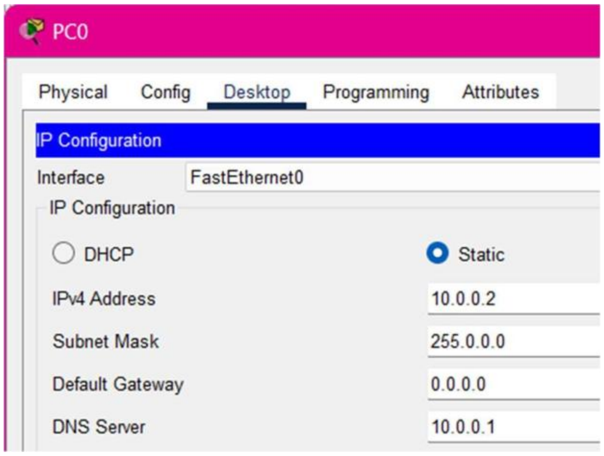
Resource Records

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



Interface FastEthernet0

IP Configuration

○ DHCP ● Static

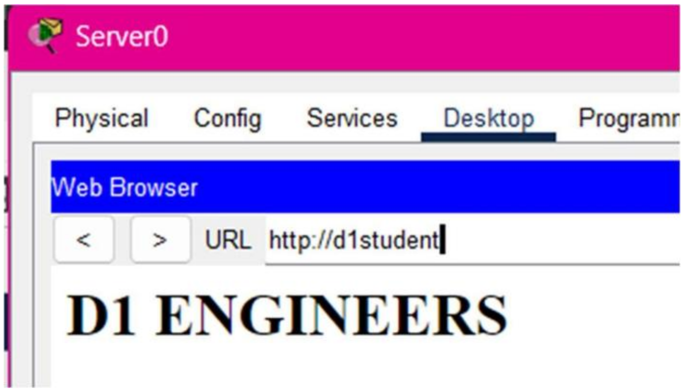
IPv4 Address 10.0.0.2

Subnet Mask 255.0.0.0

Default Gateway 0.0.0.0

DNS Server 10.0.0.1

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



URL http://d1student

D1 ENGINEERS