# **Experiment No.1**

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

**Theory:**

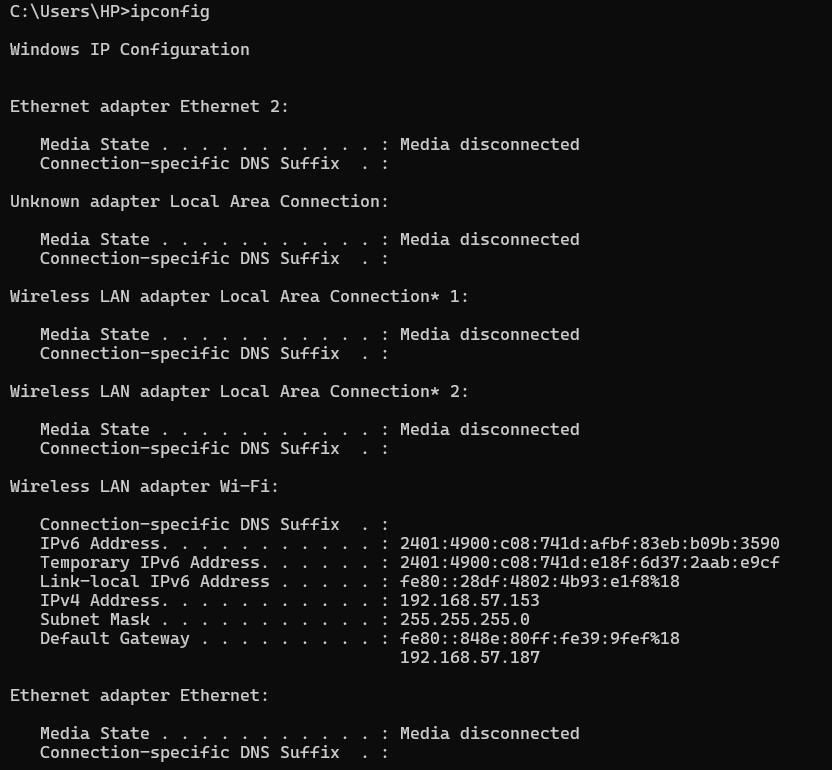
1. **ipconfig -** The ipconfig command is used in Windows to display and manage the network configuration of a computer. It provides details about the IP addresses, subnet masks, and default gateways for all network adapters.

**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.

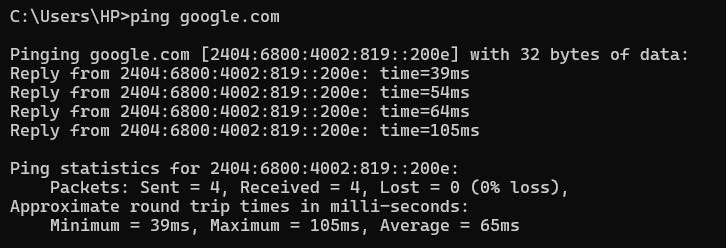
This command is useful for troubleshooting network issues like connectivity problems, incorrect IP configurations, and DNS resolution failures.

**ipconfig**



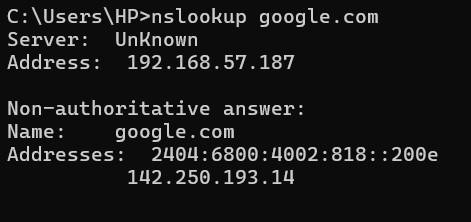
1. **ping -** The ping command is used to test the connectivity between your computer and another device (like a server or website) over a network. It sends small packets of data (ICMP Echo Requests) to the target and waits for a response.

**ping**



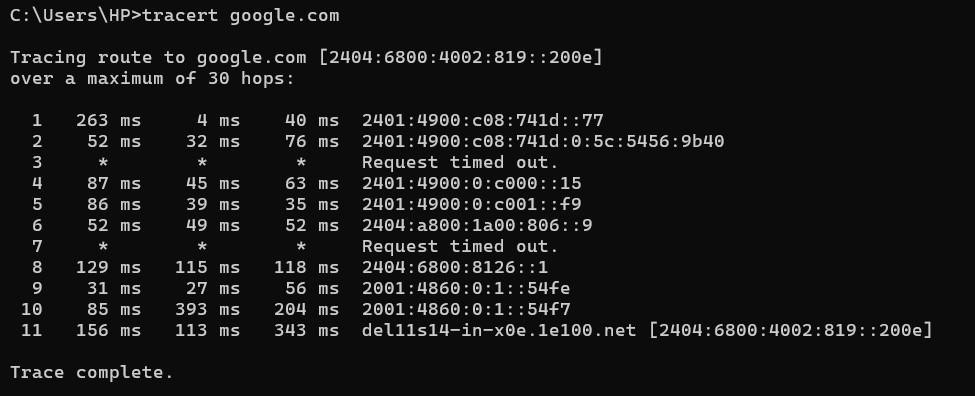
1. **nslookup -** The ping command is used to test the connectivity between your computer and another device (like a server or website) over a network. It sends small packets of data (ICMP Echo Requests) to the target and waits for a response.

**nslookup**

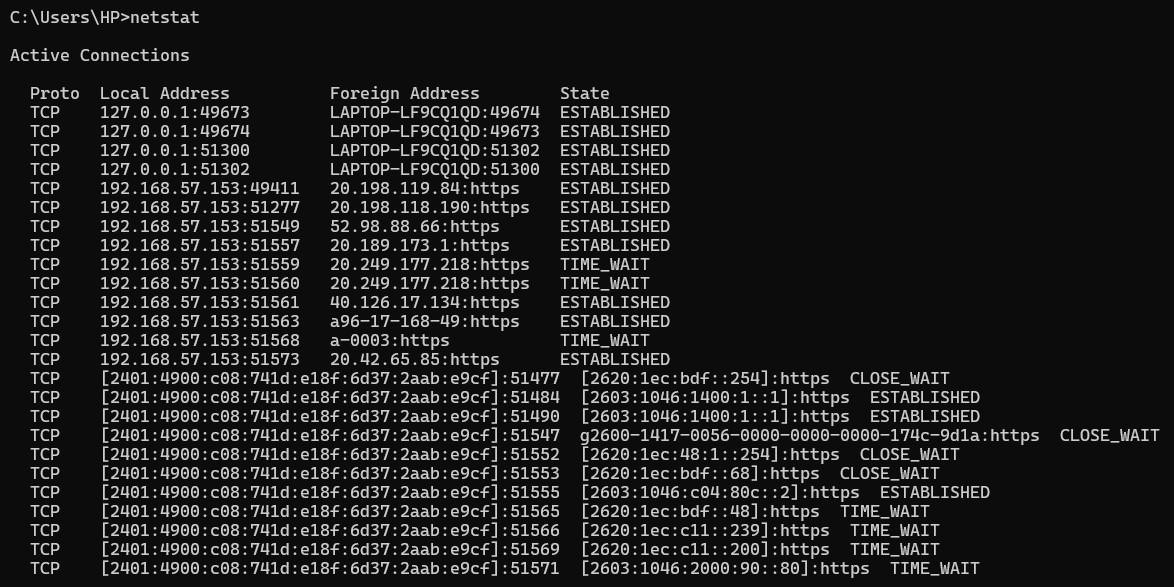


1. **tracert -** The tracert (Trace Route) command is used to track the path that packets take from your computer to a destination (such as a website or server). It helps identify network latency, routing issues, and the number of hops a packet takes to reach its destination.

**tracert**

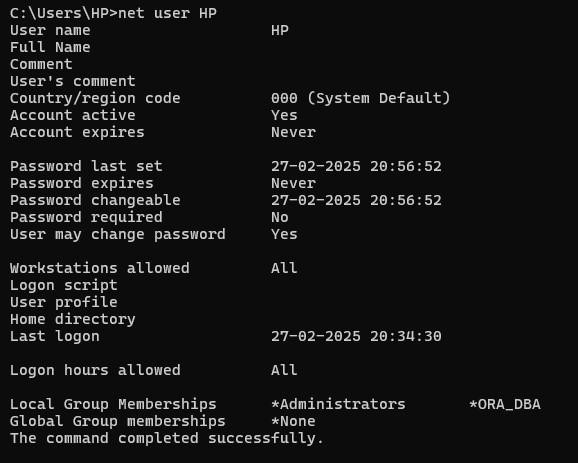


1. **netstat -** The netstat (Network Statistics) command is used to display active network connections, routing tables, and various network statistics. It helps in monitoring network activity and troubleshooting connectivity issues. – **netstat**

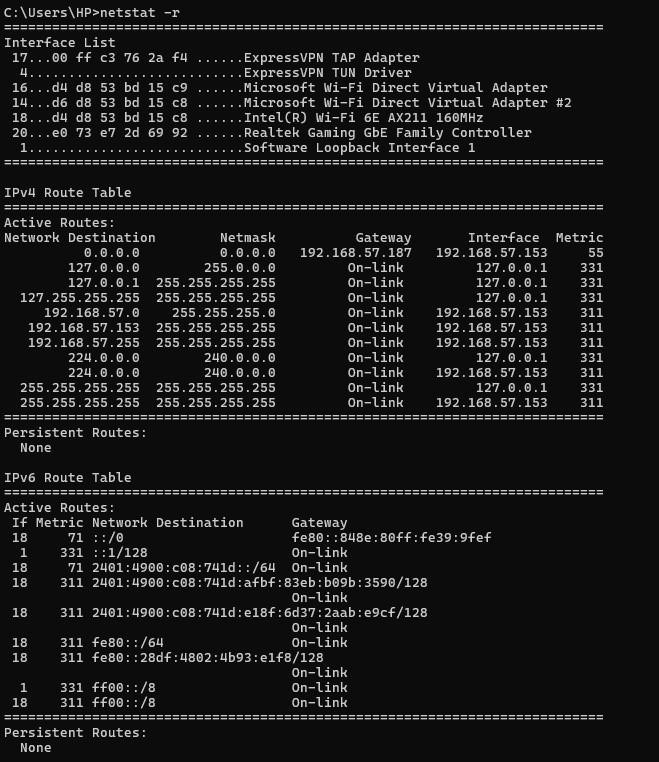


1. **net user <username> -** The net user <username> command is used in Windows to manage user accounts on a computer or a domain. It allows you to view, modify, create, or delete user accounts.

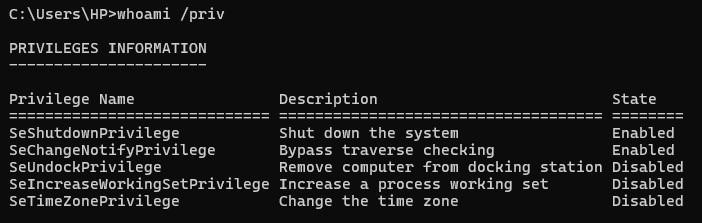
**Net user<username>**



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



1. **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**



# **Experiment No.2**

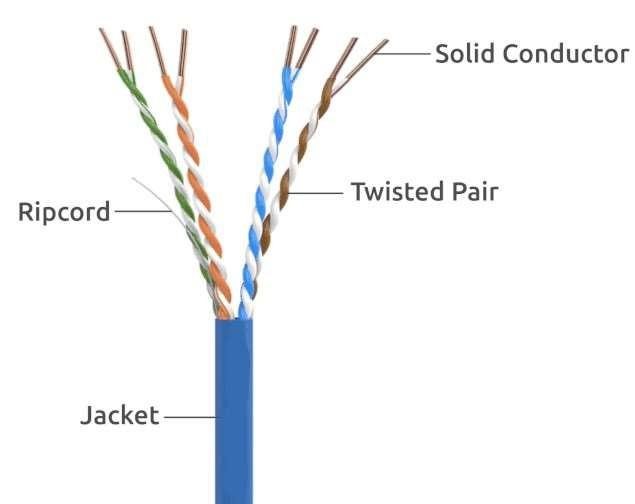
**Objective:** Familiarization with Transmission media and tools: Co-axial cable, UTP cable, Crimping tool, Connectors etc. Preparing the UTP cable for cross and direct connection using crimping tool.

**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

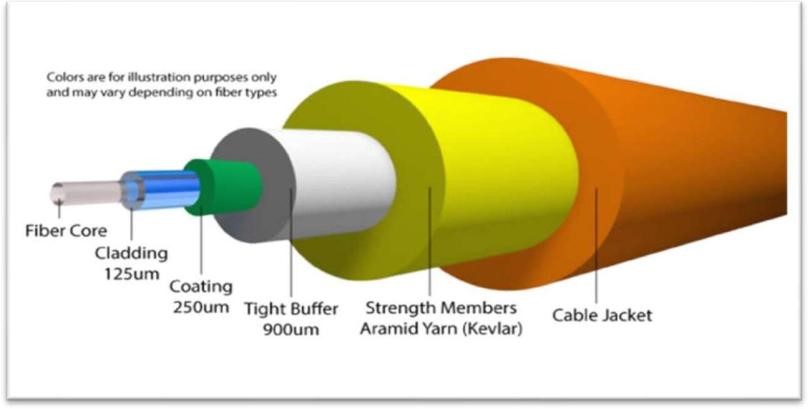
* High Speed – Supports speeds up to 100 Gbps or more.
* Long Distance – Can transmit data over hundreds of kilometers with minimal signal loss.
* Less Interference – Immune to electromagnetic interference (EMI) from electrical devices.

## 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)



1. **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.



1. **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.

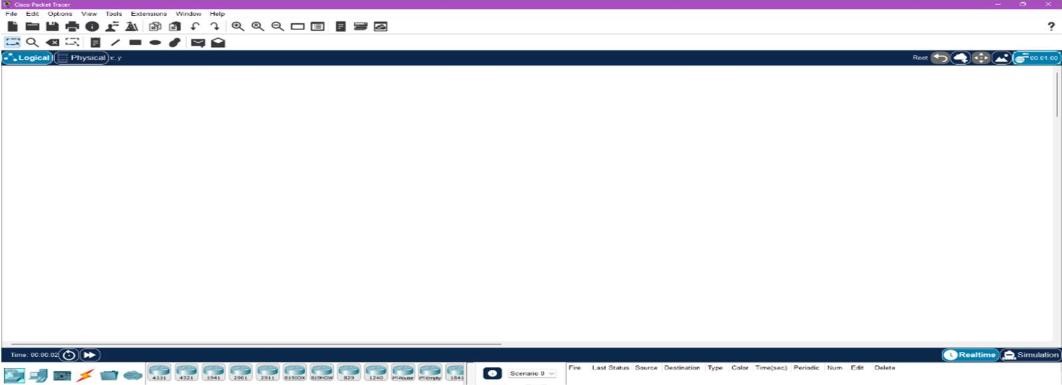
**Installation Steps**:

* 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

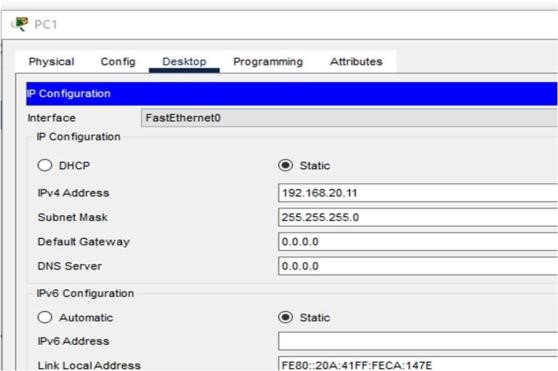
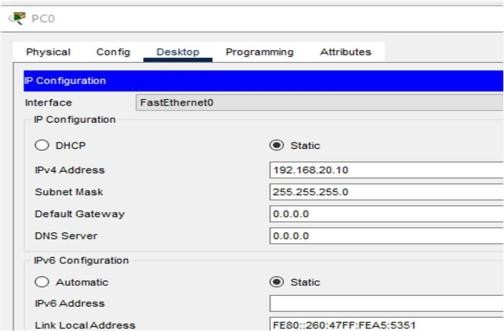
* In Cisco Packet Tracer, place the PCs and connect it.



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

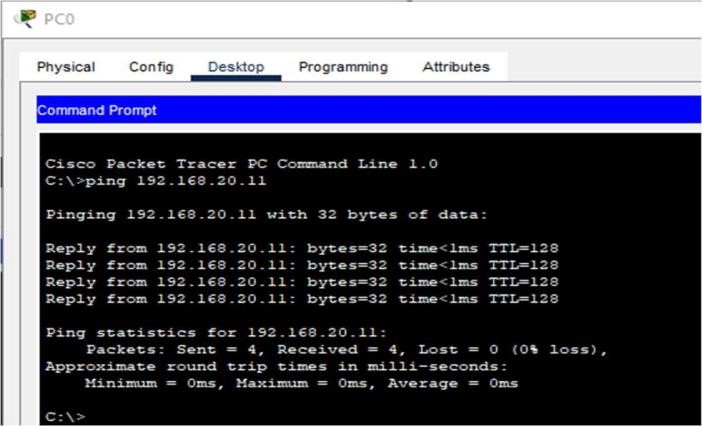
* For each PC, navigate to **Desktop > IP Configuration**.
* Assign the following IP addresses:

oPC0: 192.168.20.10 oPC1: 192.168.20.11



**Step 3**: Testing Connectivity

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

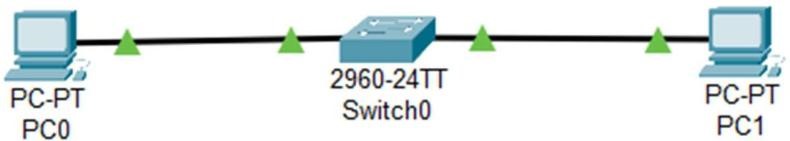


**Direct Connection Between End Devices Using a Switch**



**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.



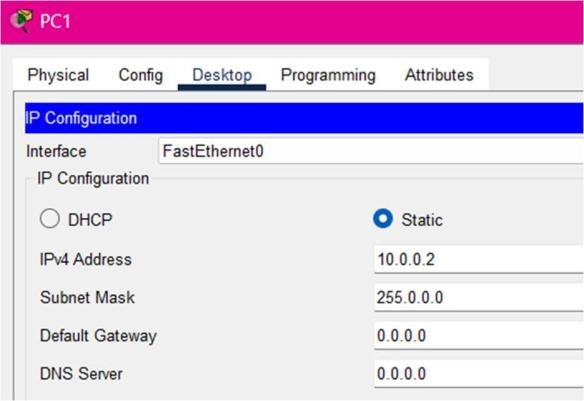
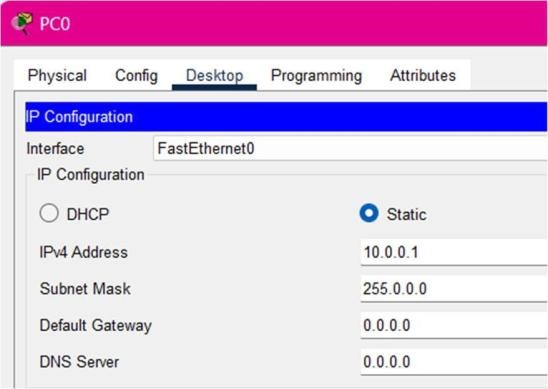
**Step 2: Configuring IP Addresses on End Devices**

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

2Assign the following IP address:

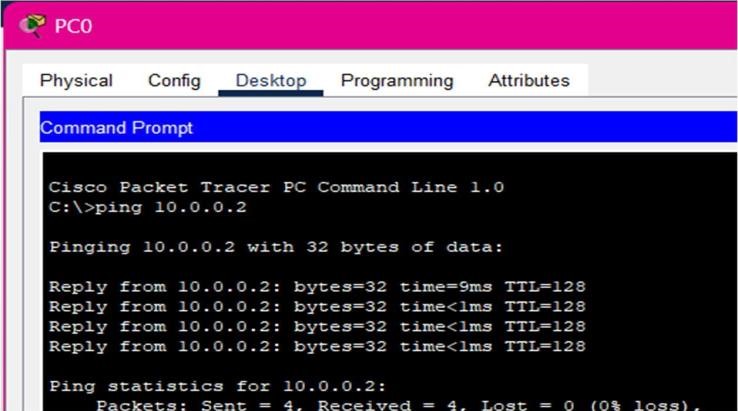
PC0: 10.0.0.1(Subnet Mask: 255.0.0.0):

PC1: 10.0.0.2 (Subnet Mask: 255.0.0.0)



**Step 3: Testing Connectivity**

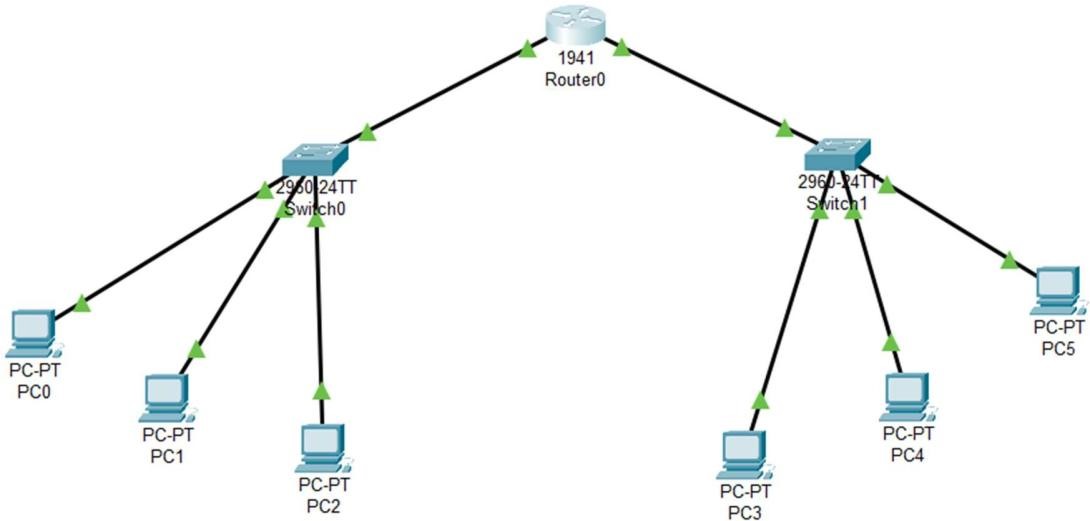
Open command prompt on PC0 and enter command ping 10.0.0.2



**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.



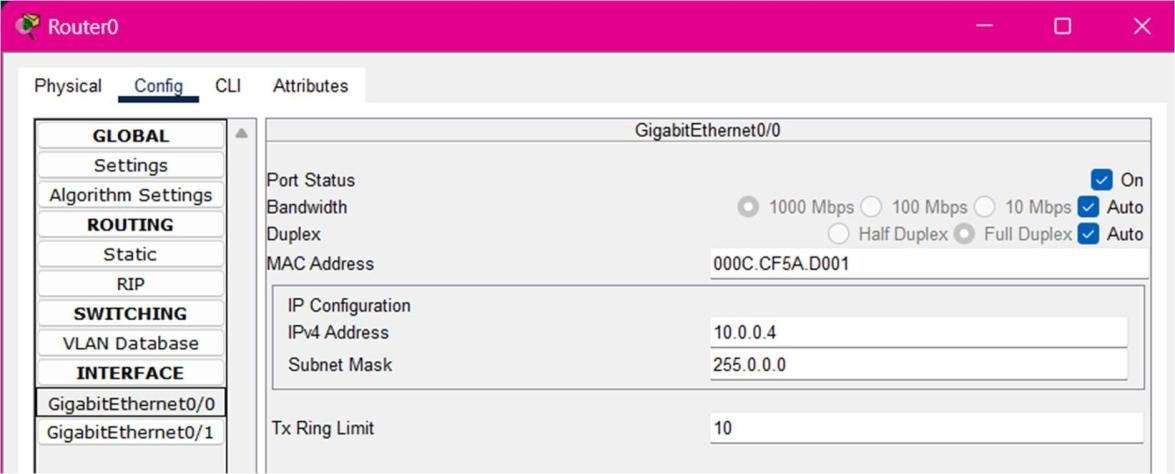
**Step 2: Configuring IP Addresses on End Devices**

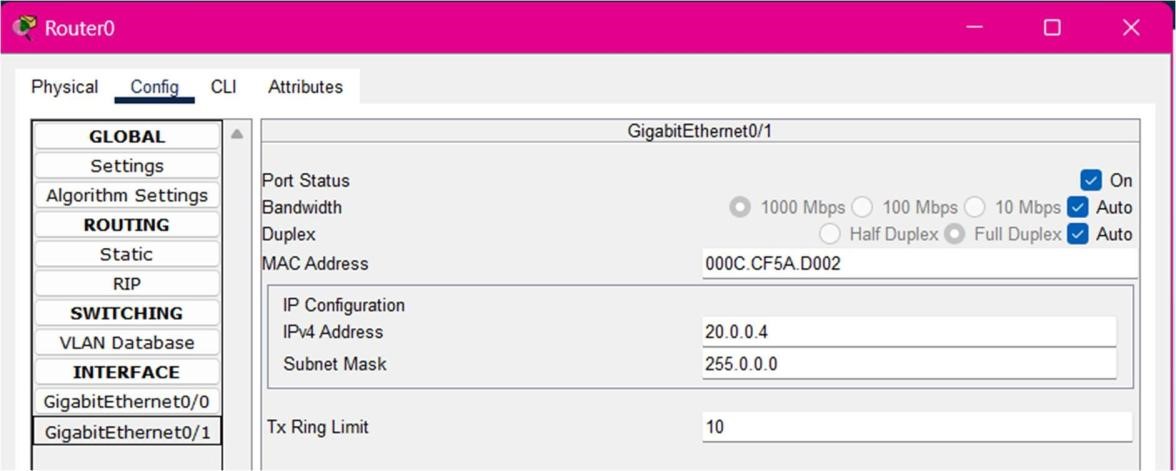
1. Click on each device, go to Desktop > IP Configuration.

* PC0: 10.0.0.1(Subnet Mask: 255.0.0.0) oPC1: 10.0.0.2(Subnet Mask: 255.0.0.0) oPC2: 10.0.0.3(Subnet Mask: 255.0.0.0) oPC3: 20.0.0.1(Subnet Mask: 255.0.0.0) oPC4: 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.



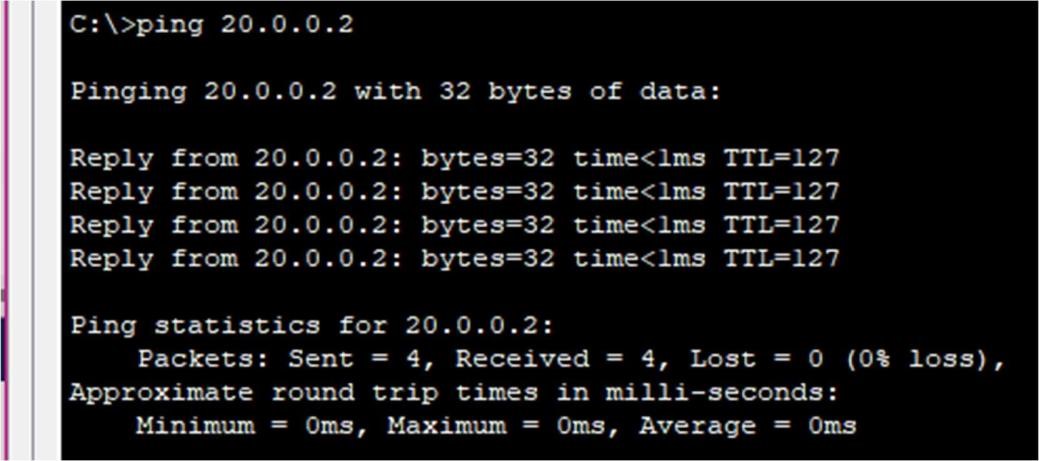


**Step 4: Set gateway**

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:



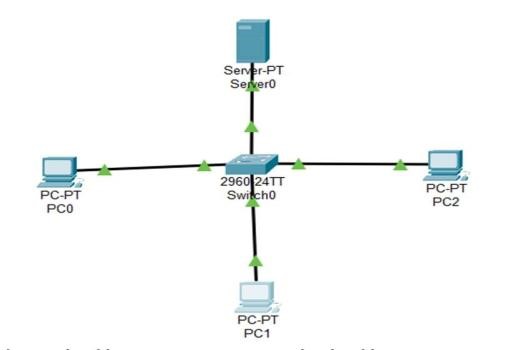
### Experiment No.5

**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)

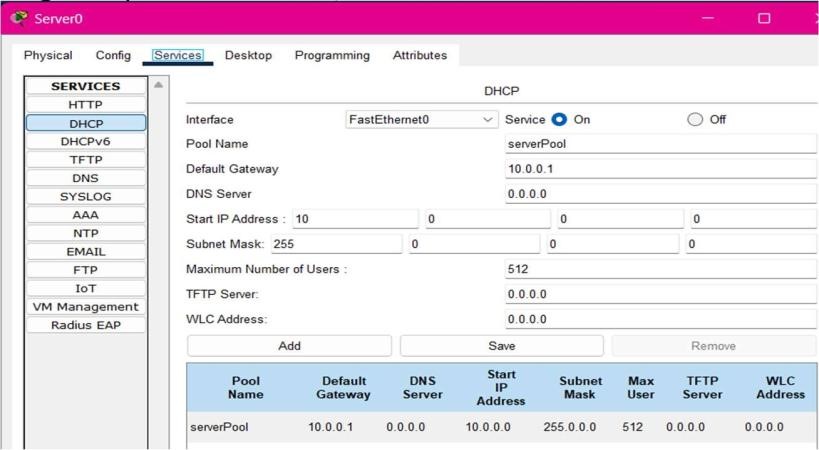
**Theory:** Dynamic Host Configuration Protocol (DHCP) is a network protocol that automatically assigns IP addresses and configuration settings to devices, reducing manual effort and preventing conflicts. It follows a DORA process (Discovery, Offer, Request, Acknowledgment) to allocate IPs dynamically.

**Procedure:**

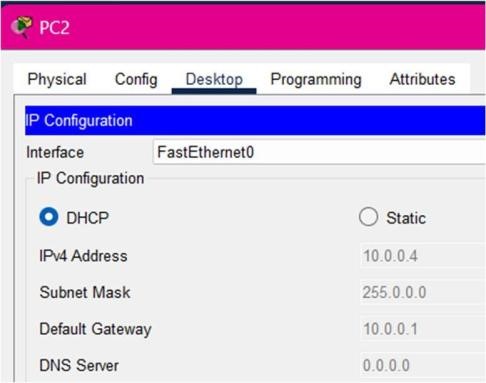
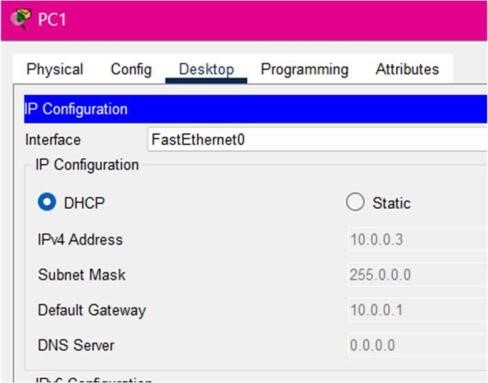
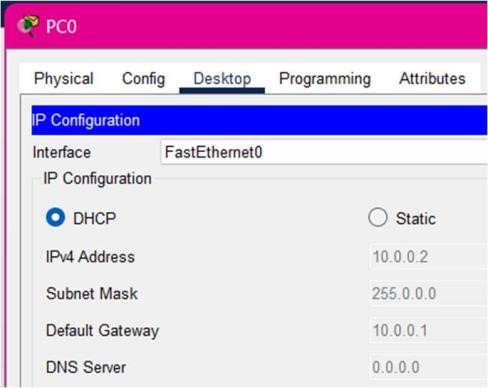
1. Connect multiple devices to a switch and add a server to the network.



1. 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.



1. 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

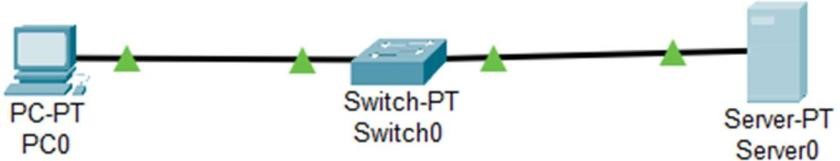


### Experiment No.6

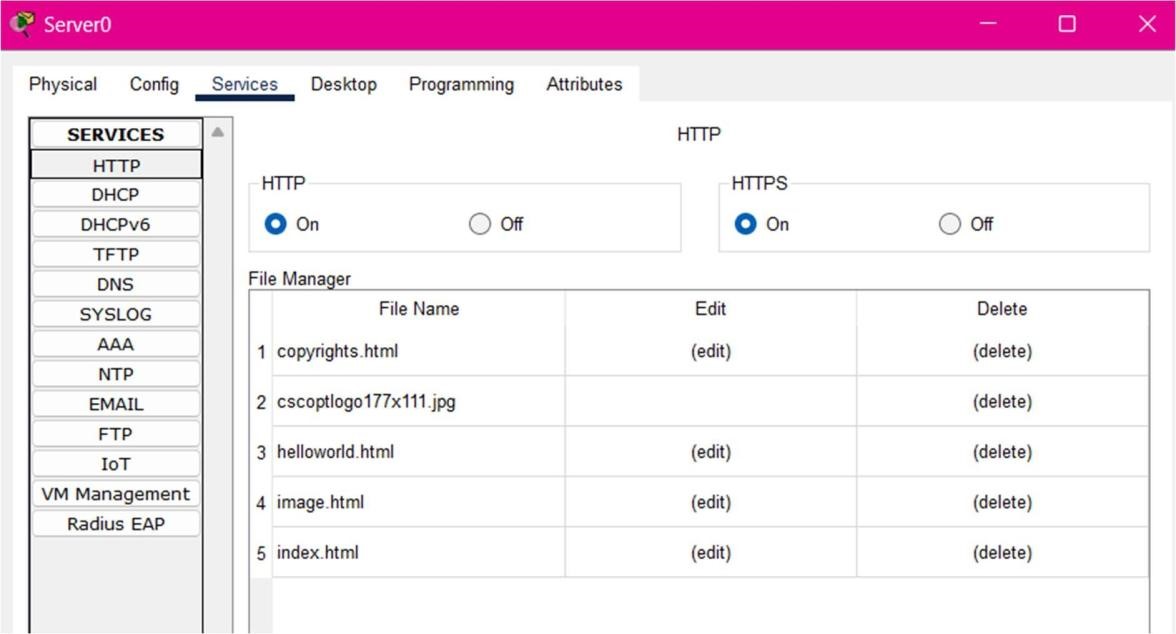
**Objective:** To configure a local DNS server to resolve domain names within a network. (Using packet Tracer).

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

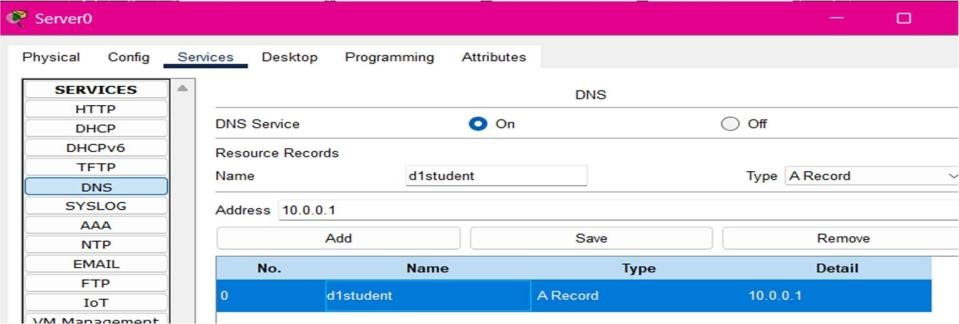
1. **Assemble the Network:** 
   * Connect the end device and switch to a server.



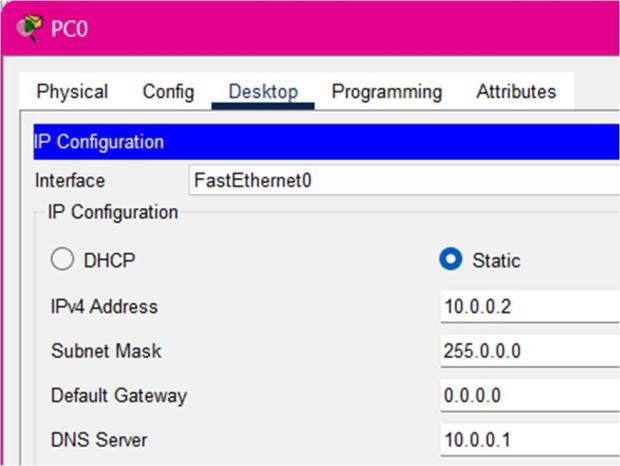
1. **Configure the Server:** 
   * Click on the server. o Assign an **IP address** to the server.
   * Set the **same IP address** as the **DNS server address**.
2. **Enable HTTP Service:** 
   * Click on **Services** in the server settings. o Go to the **HTTP** option.
   * Locate the **index file**,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



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



1. **Configure the End Device:** 
   * Assign an **IP address** to the end device and add the **DNS server address**



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

