I.K. GUJRAL PUNJAB TECHNICAL UNIVERSITY, KAPURTHALA

Department of Computer Science & Engineering

PRACTICAL FILE

COMPUTER NETWORKS LAB

BTCS507-18

Submitted By:

Name –Ansh Bhogal
Roll No. – 2323445
Semester – 5th

Submitted to:

Mr Gagandeep

Session: 2025-2026

INDEX

TASK 1 : To Study different types of network cables and different Topologies .

What is Network cables ?

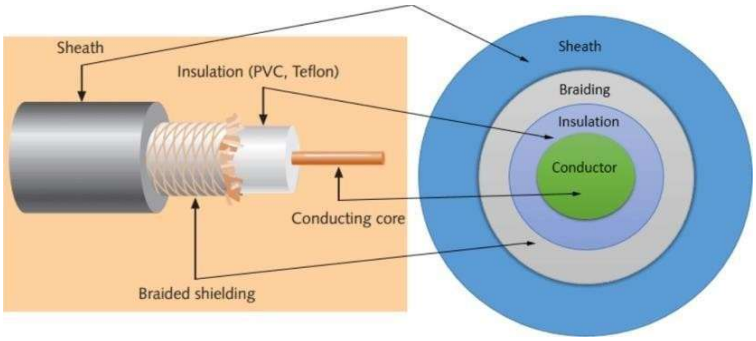
A network cable is a type of cable used to connect and transfer data between computers, routers, switches, and storage area networks. These cables are essential for creating wired networks, allowing devices to communicate with each other and share resources.

Different types of Network cables are :

Coaxial cable

This cable contains a conductor, insulator, braiding, and sheath. The sheath covers the braiding, the braiding covers the insulation, and the insulation covers the conductor.

The following image shows these components.



Sheath : This is the outer layer of the coaxial cable. It protects the cable from physical damage.

Braided shield : This shield protects signals from external interference and noise. This shield is built from the same metal that is used to build the core.

Insulation : Insulation protects the core. It also keeps the core separate from the braided shield. Since both the core and the braided shield use the same metal, without this layer, they will touch each other and create a short-circuit in the wire.

Conductor : The conductor carries electromagnetic signals.

Based on conductor a coaxial cable can be define into two types ; single-core coaxial cable and multi-core coaxial cable.

single-core coaxial cable uses a single central metal (usually copper) conductor .

multi-core coaxial cable uses multiple thin strands of metal wires.


Single core coaxial cable


Multi-core coaxial cable

Twisted-pair cables

The twisted-pair cable was primarily developed for computer networks. This cable is also known as **Ethernet cable**. Almost all modern LAN computer networks use this cable.

This cable consists of color-coded pairs of insulated copper wires. Every two wires are twisted around each other to form pair. Usually, there are four pairs. Each pair has one solid color and one stripped color wire. Solid colors are blue, brown, green, and orange. In stripped color, the solid color is mixed with the white color.

Based on how pairs are stripped in the plastic sheath, there are two types of twisted-pair cable; UTP and STP.

In the **UTP (Unshielded twisted-pair) cable**, all pairs are wrappedin a single plastic sheath.

- **Cat5:** Supports up to 100 Mbps speeds and is suitable for older networks.
- **Cat5e:** Enhanced version of Cat5, supports up to 1 Gbps speeds and is commonly used in modern LANs.
- **Cat6:** Supports up to 10 Gbps speeds over short distances (up to 55 meters) and is suitable for more demanding networks.
- **Cat6a:** Augmented Cat6, supports 10 Gbps speeds over longer distances (up to 100 meters) and has better shielding to reduce interference.
- **Cat7:** Supports up to 10 Gbps speeds, with extensive shielding for reduced interference and higher frequency support.
- **Cat8:** Supports up to 40 Gbps speeds, designed for high-performance data centers and shorter cable runs.

In the **STP (Shielded twisted-pair) cable**, each pair is wrapped with an additional metal shield, then all pairs are wrapped in a single outer plastic sheath.

Similar to UTP but includes shielding to reduce electromagnetic interference (EMI) and crosstalk.

Similarities and differences between STP and UTP cables

- Both STP and UTP can transmit data at 10Mbps, 100Mbps, 1Gbps, and 10Gbps.
- Since the STP cable contains more materials, it is more expensive than the UTP cable.
- Both cables use the same RJ-45 (registered jack) modular connectors.
- Both cables can accommodate a maximum of 1024 nodes in each segment.
- The STP provides more noise and EMI resistance than the UTP cable.
- The maximum segment length for both cables is 100 meters or 328 feet.

Fiber optic cable

This cable consists of a core, cladding, buffer, and jacket. The core is made from thin strands of glass or plastic that can carry data over a long distance. The core is wrapped in the cladding; the cladding is wrapped in the buffer, and the buffer is in the jacket.

- Core carries the data signals in the form of light.
- Cladding reflects light back to the core.
- Buffer protects the light from leaking.
- The jacket protects the cable from physical damage.

Fiber optic cable is completely immune to EMI and RFI. This cable can transmit data over a long distance at the highest speed.

It can transmit data up to 40 kilometers at the speed of 100Gbps.

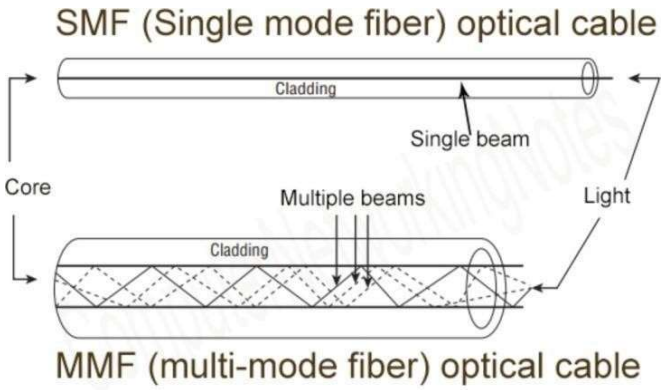
Fiber optic uses light to send data. It reflects light from one endpoint to another. Based on how many beams of light are transmitted at a given time, there are two types of fiber optical cable; SMF and MMF.

SMF (Single-mode fiber) optical cable :

This cable carries only a single beam of light. This is more reliable and supports much higher bandwidth and longer distances than the MMF cable. This cable uses a laser as the light source and transmits 1300 or 1550 nano-meter wavelengths of light.

MMF (multi-mode fiber) optical cable :

This cable carries multiple beams of light. Because of multiple beams, this cable carries much more data than the SMF cable. This cable is used for shorter distances. This cable uses an LED as the light source and transmits 850 or 1300 nano-meter wavelengths of light.



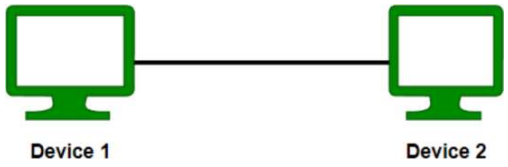
What is Topologies ?

Topology refers to the arrangement of various elements (links, nodes, etc.) in a network. It is essentially the layout or organizational hierarchy of interconnected devices.

Here are some common types of network topologies:

Point to Point Topology

Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



Advantages of Point to Point Topology :

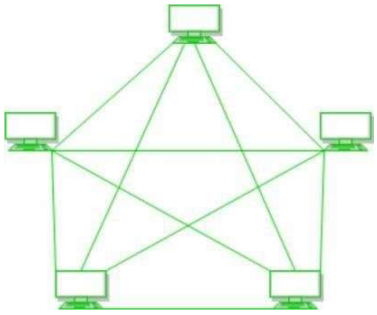
- The straightforward design makes it easy to implement and understand.
- Easier to set up and configure compared to more complex network topologies.
- Direct communication between two points can result in faster data transfer rates.
- Reduced latency as data does not need to pass through intermediate nodes.
- Enhanced security since the communication is direct and less prone to interception.
- Easier to implement security measures and encryption.

Disadvantages of Point to Point Topology :

- Not scalable for larger networks; adding new devices requires additional direct connections.
- Becomes complex and costly as the number of connections increases.
- Lack of redundancy; if the connection fails, communication between the two devices is lost.
- No alternative paths for data transmission.
- Requires dedicated resources for each connection, which can be expensive over long distances.
- Higher maintenance costs due to the need for managing multiple direct connections.

Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



Advantages of Mesh Topology :

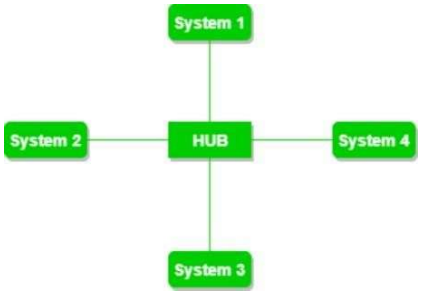
- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Disadvantages of Mesh Topology :

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc



Advantages of Star Topology :

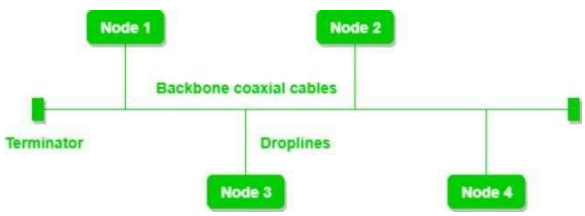
- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

Disadvantages of Star Topology :

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes ,various MAC protocols are followed by LAN ethernet connections like TDMA.



Advantages of Bus Topology :

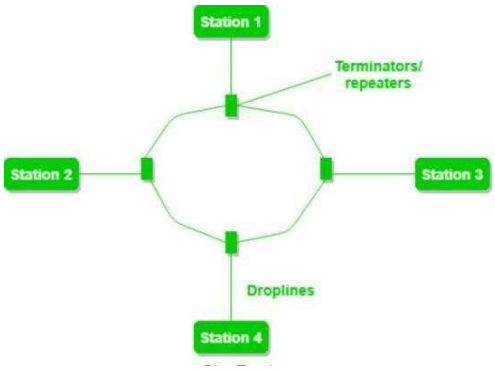
- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.

Disadvantages of Bus Topology :

- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.



Advantages of Ring Topology :

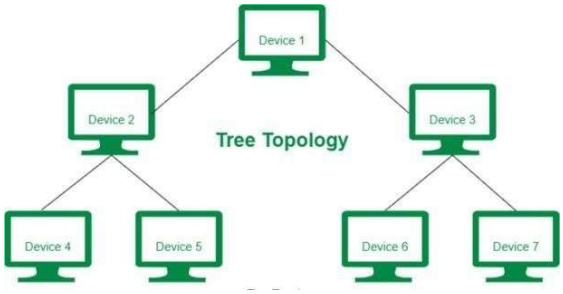
- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

Disadvantages of Ring Topology :

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.

Tree Topology

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used.



Advantages of Tree Topology :

- It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.
- We can add new devices to the existing network.
- Error detection and error correction are very easy in a tree topology.

Disadvantages of Tree Topology :

- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

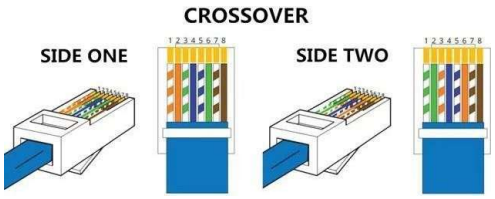
TASK 2 : Practically implement and test the cross-wired cable and straight through cable using clamping tool and network lab cable tester.

Materials Needed: RJ45 connectors , Clamping tool (crimping tool) , Cable stripper , Network lab cable tester , Wire cutters (optional) , Ethernet cable (Cat5e or Cat6).

Steps :

1. **Strip the Cable**: Remove 1-2 inches of the outer jacket from both ends.
2. **Untwist Wires**: Separate and straighten the wire pairs.
3. **Arrange Wires**:
   - **Straight-Through**: Use T568A or T568B on both ends.
   - **Crossover**: Use T568A on one end, T568B on the other.
4. **Trim Wires**: Ensure all wires are of equal length.
5. **Insert Wires into RJ45 Connector**: Slide wires into the connector, maintaining order.
6. **Crimp the Connector**: Use the crimping tool to secure the wires in the connector.
7. **Repeat for Other End**: Follow the same process for the second end.
8. **Test with Cable Tester**: Plug both ends into the tester to verify the wiring is correct.

Cross-Wired Cable (Crossover Cable) : A cross-wired cable, commonly referred to as a crossover cable, is used to directly connect two similar network devices, such as two computers, two switches, or two routers, without the need for a hub, switch, or router between them.

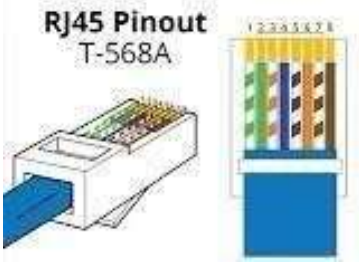


Wiring Standard for Crossover Cable : To create a crossover cable, you must use different wiring standards on each end of the cable.

End 1: T568A Standard

T568A Standard (End 1)

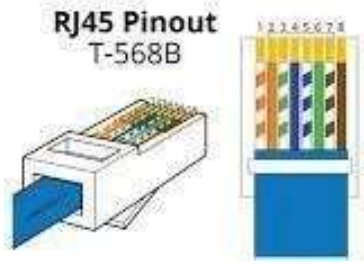
Pin 1: White/Green
Pin 2: Green
Pin 3: White/Orange
Pin 4: Blue
Pin 5: White/Blue
Pin 6: Orange
Pin 7: White/Brown
Pin 8: Brown



End 2: T568B Standard

T568B Standard (End 2)

Pin 1: White/Orange
Pin 2: Orange
Pin 3: White/Green
Pin 4: Blue
Pin 5: White/Blue
Pin 6: Green
Pin 7: White/Brown
Pin 8: Brown

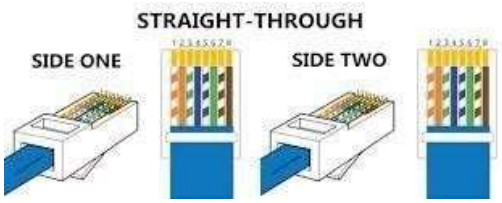


Uses of Crossover Cable:

- **Computer to Computer**: Directly connect two computers for file sharing or networking.
- **Switch to Switch**: Link two network switches together directly.
- **Router to Router**: Connect two routers for network segmentation or redundancy.
- **Hub to Hub**: Join two hubs to expand a network without using a switch.
- **Connecting Older Network Devices**: Some older devices that don't support auto MDI/MDIX require a crossover cable to connect similar devices.

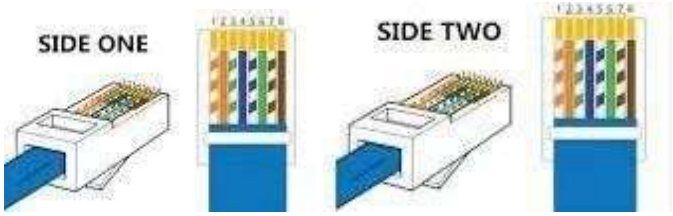
Straight through cable : A straight-through cable is a type of Ethernet cable that has identical wiring on both ends, following the same wiring standard (either T568A or T568B). It is commonly used to connect different types of devices, such as:

- Computer to Router
- Computer to Switch
- Router to Switch



Wiring Standards for Straight through cable: You can choose either T568A or T568B, but the same standard must be used on both ends.

Pin 1: White/Orange
Pin 2: Orange
Pin 3: White/Green
Pin 4: Blue
Pin 5: White/Blue
Pin 6: Green
Pin 7: White/Brown
Pin 8: Brown



Uses of Straight through cable:

Computer to Switch: Connect a computer to a network switch to access a local network.
Computer to Router: Link a computer to a router for internet access or network configuration.
Router to Modem: Connect a router to a modem for internet connectivity.
Switch to Router: Link a switch to a router to allow multiple devices on the network to access the internet.
Computer to Network Printer: Directly connect a computer to a network printer.
Access Point to Switch: Connect a wireless access point to a wired network switch.

TASK 3 : Study and familiarization with various network devices .

Network devices : are the hardware components that facilitate communication and resource sharing in a network.

Here's a list of various network devices:

1. Router

- **Function**: A router is responsible for forwarding data packets between different networks. It determines the best path for data to travel from the source to the destination. Routers can connect multiple networks, such as a home network to the internet.
- **Example**: In a typical home setup, a router connects to the internet service provider's network via a modem and routes data between the internet and the home's devices, such as computers, smartphones, and smart TVs.

2. Switch

- **Function**: A switch operates at the data link layer (Layer 2) of the OSI model and connects multiple devices within the same local area network (LAN). Unlike a hub, which broadcasts data to all devices, a switch intelligently forwards data to the specific device that needs it, using MAC addresses to make this decision.

- **Example**: In an office environment, a switch connects all the computers, printers, and servers in the network, allowing them to communicate with each other efficiently.

3. Hub

- **Function**: A hub is a basic networking device that connects multiple Ethernet devices in a network. It broadcasts incoming data packets to all connected devices, regardless of the destination. This makes hubs less efficient than switches, as they can cause network collisions.
- **Example**: Hubs were commonly used in older or simpler network setups to connect a few computers within a small LAN.

4. Modem

- **Function**: A modem (short for modulator-demodulator) converts digital signals from a computer into analog signals that can travel over telephone or cable lines and vice versa. This conversion allows for communication over long distances, typically for internet access.
- **Example**: A DSL or cable modem connects a home or office network to the internet via the ISP's infrastructure.

5. Access Point (AP)

- **Function**: An access point is a device that allows wireless devices to connect to a wired network using Wi-Fi. It acts as a bridge between wireless devices and the wired LAN, extending the network's coverage area.
- **Example**: In a large office, multiple access points are placed throughout the building to provide Wi-Fi coverage in all areas, ensuring that wireless devices can connect seamlessly to the network.

6. Firewall

- **Function**: A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access and threats.
- **Example**: Enterprises use firewalls to protect their internal networks from external cyber threats by filtering out potentially harmful data and blocking unauthorized access attempts.

7. Network Interface Card (NIC)

- **Function**: A Network Interface Card (NIC) is a hardware component that allows a computer or device to connect to a network, either through a wired Ethernet connection or wirelessly via Wi-Fi. The NIC provides the necessary physical connection and the interface to process network communications.
- **Example**: Most modern computers come with a built-in NIC that enables them to connect to wired or wireless networks for internet access and file.

8. Gateway

- **Function**: A gateway is a device that serves as an entry and exit point between two networks, often connecting a local network to an external network (like the internet). It can translate between different protocols and perform functions such as routing, security filtering, and data format conversion.
- **Example**: A home router often acts as a gateway, connecting the home's internal network to the internet, managing the traffic, and providing security functions like NAT (Network Address Translation).

9. Bridge

- **Function**: A bridge is a network device that connects and filters traffic between two different segments of a local area network (LAN). Operating at the data link layer, it divides a large network into smaller segments to reduce traffic congestion and improve performance. Bridges filter traffic by examining the MAC addresses to determine whether to forward or block data.
- **Example**: In a large building with multiple floors, bridges can be used to connect the networks on each floor, allowing them to communicate while managing the traffic between them.

10. Repeater

- **Function**: A repeater is a device that regenerates and amplifies signals in a network to extend the distance over which data can be transmitted without degradation. Repeaters are often used in long-distance data transmission to ensure that signals remain strong and clear.
- **Example**: In a large office or warehouse where a single wireless signal cannot cover the entire area, repeaters can be used to extend the Wi-Fi signal to reach all corners of the space.

11. Proxy Server

- **Function**: A proxy server acts as an intermediary between a client and a server, forwarding requests from clients seeking resources from other servers. Proxy servers are often used for filtering content, improving performance through caching, and hiding the client's IP address for anonymity.
- **Example**: Organisations often use proxy servers to control and monitor internet usage, block access to certain websites, and cache frequently accessed content to reduce bandwidth usage.

12. Load Balancer

- **Function**: A load balancer distributes incoming network traffic across multiple servers to ensure that no single server is overwhelmed with too much traffic. This helps in maintaining high availability and reliability of applications and services, especially in high-traffic environments.
- **Example**: Websites with a large number of visitors, such as e-commerce sites, use load balancers to distribute user requests across multiple web servers, ensuring smooth performance and preventing any single server from failing due to excessive load.

Task 4 : Familiarization with Packet Tracer Simulation tool/any other related tool.

Packet Tracer : Packet Tracer is a powerful network simulation tool developed by Cisco, widely used for learning and practicing networking concepts, especially for those studying for Cisco certifications like CCNA (Cisco Certified Network Associate).

Advantages of Cisco Packet Tracer

1. **User-Friendly Interface**:
    - **Easy to Learn**: The interface is intuitive, making it accessible even for beginners with little to no prior networking experience.
    - **Drag-and-Drop Functionality**: Users can easily add devices and create network topologies using drag-and-drop.
2. **Cost-Effective**:
    - **Free Access**: Cisco offers Packet Tracer for free to students and educators through the Cisco Networking Academy, making it an affordable option for learning networking.
3. **Supports a Wide Range of Cisco Devices**:
    - **Device Simulation**: Packet Tracer includes a variety of Cisco devices (routers, switches, PCs, etc.), allowing users to simulate complex network scenarios.
    - **IoT Simulation**: It supports the simulation of IoT (Internet of Things) devices, which is useful for understanding modern network setups.
4. **Educational Focus**:
    - **Built-in Tutorials**: It includes various tutorials and labs that align with Cisco's certification programs, such as CCNA.
    - **Learning Environment**: Designed to help students learn and practice networking concepts in a controlled environment.
5. **Real-Time and Simulation Modes**:
    - **Real-Time Mode**: Shows the immediate state of the network, similar to a real network.
    - **Simulation Mode**: Allows users to visualize and analyze packet flow, which is helpful for understanding network protocols and troubleshooting issues.
6. **Cross-Platform Compatibility**:
    - **Runs on Multiple Operating Systems**: Packet Tracer is available on Windows, macOS, and Linux, making it accessible to a wide range of users.

Disadvantages of Cisco Packet Tracer

1. **Limited to Cisco Devices**:
    - **Vendor Lock-In**: While Packet Tracer is excellent for learning Cisco-specific networking, it doesn't support devices from other vendors, limiting its usefulness for those needing to learn about multi-vendor environments.
2. **Simulation Limitations**:
    - **Not a Full Emulator**: Packet Tracer is a simulator, not an emulator. It approximates the behavior of Cisco devices but doesn't run actual IOS images, which means it may not replicate every command or feature exactly as it would be on real hardware.
    - **Simplified Environment**: Some advanced networking features and protocols are either not supported or are simplified, making it less suitable for in-depth or high-level network design and testing.
3. **Performance Constraints**:
    - **Resource Intensive**: Although not as demanding as some other network simulators, Packet Tracer can still be resource-intensive, especially with large and complex topologies.
5. **Less Suitable for Advanced Users**:
    - **Not Ideal for Professional Use**: While it is excellent for educational purposes, professionals may find Packet Tracer lacking when it comes to advanced network design, testing, and troubleshooting in a production environment.
6. **No Support for Non-Cisco Certifications**:
    - **Focused on Cisco Curriculum**: The tool is primarily designed to align with Cisco's certification paths, so it might not be as useful for those pursuing non-Cisco certifications like CompTIA Network+ or vendor-neutral networking knowledge.

1. Getting Started with Packet Tracer

Installation

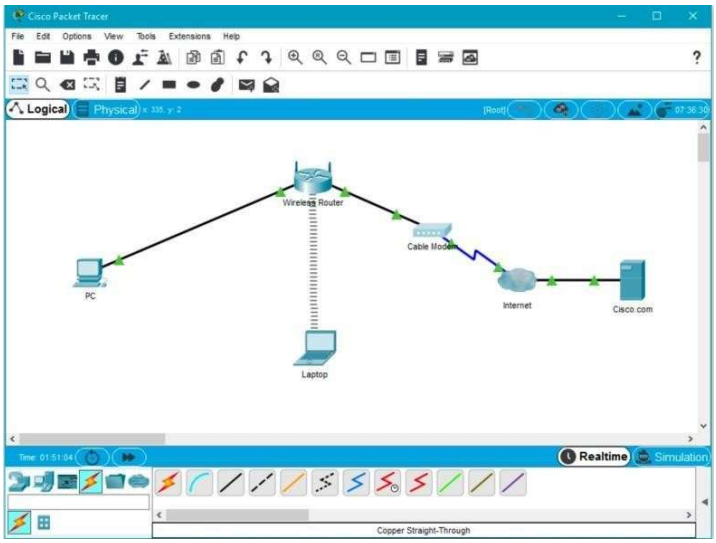
- **Download**: You can download Packet Tracer from the Cisco Networking Academy website. It is available for Windows, macOS, and Linux.
- **Installation**: Follow the

CISCO PACKET TRACER 8.2.2 OFFICIAL DOWNLOAD PAGE

installation instructions for your operating system.

2. Creating a Simple Network

1. **Adding Devices**: Drag and drop devices like routers, switches, and PCs from the left panel onto the workspace .
2. **Connecting Devices**: Use cables (straight-through, crossover, etc.) to connect the devices. The correct cable type is often automatically selected, but you can manually choose the type if necessary.
3. **Configuring Devices**: Click on a device to access its configuration menu. You can configure IP addresses, subnet masks, and routing protocols.
4. **Testing Connectivity**: Use the ping command from a PC's command prompt to test connectivity between devices.



3. Using Simulation Mode

- **Packet Visualisation**: In simulation mode, you can create and trace the flow of data packets across your network. This is useful for understanding how protocols like TCP/IP work.
- **Troubleshooting**: If a network connection fails, use the simulation mode to identify where the packet fails, helping you understand the problem.

4. Advanced Features

- **Protocol Simulation**: Packet Tracer supports many network protocols, including RIP, OSPF, EIGRP, and STP, allowing you to simulate complex network scenarios.
- **IoT Devices**: You can also simulate Internet of Things (IoT) devices and create smart home networks.
- **Multiuser Collaboration**: Packet Tracer allows multiple users to collaborate on the same network topology, useful for group projects.

Task 5 : Study and Implementation of IP Addressing Schemes.

IPV6 Address : - An Internet Protocol Version 6 address is a numerical label that is used to identify a network interface of a computer or other network node participating in an IPv6 network. An IP address serves the purpose of uniquely identifying an individual network interface of a host, locating it on the network, and thus permitting the routing of IP packets between hosts IPv6 is an Internet Protocol (IP) for packet-switched internet working that specifies the format of packets (also called datagram) and the addressing scheme across multiple IP networks. In comparing the two protocols IPv6 expands upon the addressing and routing capabilities of IPv4 in a number of ways including:

- In IPv6 the IP address size is increased from 32 bits to 128 bits.
- IPv6 supports a greater number of addressable nodes.
- IPv6 provides more levels of addressing hierarchy.
- IPv6 offers simpler auto-configuration of addresses.
- IPv6 also supports simplified header format.

1. Unicast Addresses

- **Purpose**: Identify a single interface on a device. Data sent to a unicast address goes directly to the interface it specifies.
- **Examples**:
  - **Global Unicast**: These are globally unique addresses that are routable on the public internet. They typically start with the prefix 2000::/3.
  - **Link-Local Unicast**: Used only for communication within a single local network (or link), such as a LAN. They start with fe80::/10 and are automatically configured without a need for a router.
  - **Unique Local (ULA)**: These are intended for local communications within a site and are not routable on the global internet. They start with the prefix fc00::/7.

2. Multicast Addresses

- **Purpose**: Identify a group of interfaces, often on multiple devices. Data sent to a multicast address is delivered to all interfaces in the group.
- **Prefix**: IPv6 multicast addresses start with ff00::/8.
- **Use Cases**:
  - Multicast addresses are commonly used for services like video streaming or group communication where data must reach multiple recipients simultaneously.

3. Any cast Addresses

- **Purpose**: Assigned to multiple interfaces, typically located on different devices. Data sent to an any cast address is delivered to the nearest interface with that address, based on the network topology.
- **Use Cases**: Any cast is often used for load balancing, where the nearest or most optimal server can respond to a user's request.

4. Special Addresses

- **Loopback Address**: Used by a device to send a message to itself. In IPv6, the loopback address is ::1, equivalent to 127.0.0.1 in IPv4.
- **Unspecified Address**: Represented by :: , an address of all zeros. It is used when a device does not yet have an IP address, such as during the initial stages of configuration.

5. Reserved Addresses

- **Purpose**: Reserved for future use or special functions.
- **Examples**:
  - Addresses in the ::/8 range are reserved for specific uses, such as IPv4-mapped IPv6 addresses (which allow IPv4 addresses to be embedded within IPv6) and other experimental purposes.

Working modes of router: - There are 5 mail modes of router: User Execution Mode, Privilege Mode, ROM Monitor Mode, Sub interface Configuration Mode, Interface Configuration Mode, Global Configuration Mode.

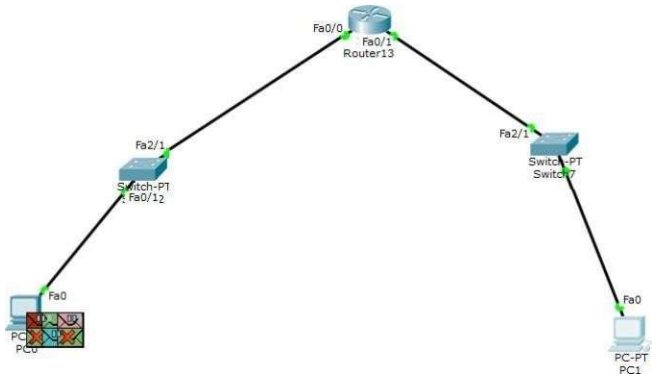
Link local :

1. A link local address is an IPv6 unicast address that can be automatically/ manually configured on anyinterface using the prefix "FE80:"
2. These addresses mostly used for addressing on a single link for purposes such as automatic addressconfiguration and neighbour discovery.
3. All IPv6 enabled interfaces have a link local unicast address.

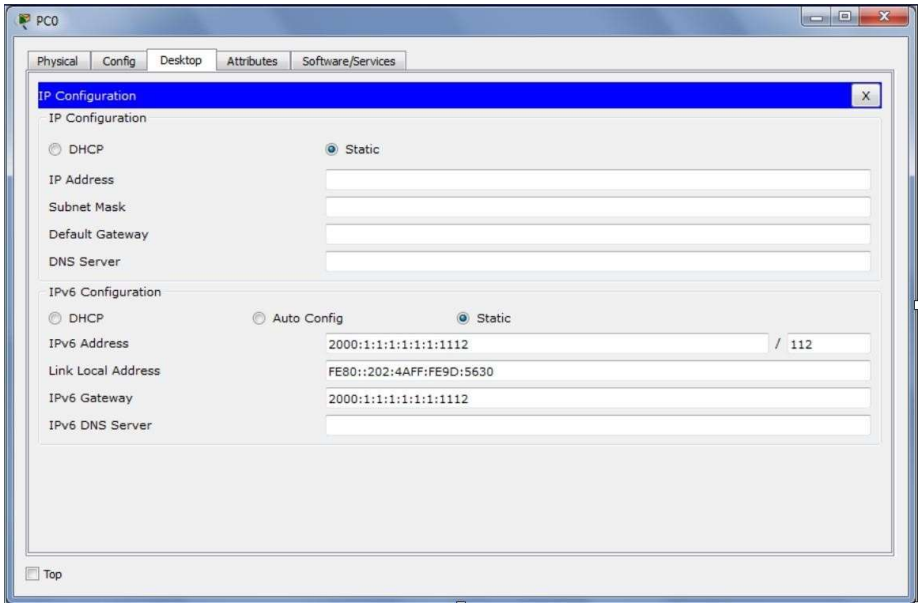
- **No shutdown:** This command enables an interface and brings it up. It is mostly used for newinterfaces or troubleshooting purposes.
- **Show IP route:** It is used to show the list of the networks that router can reach, their metric.
- **Show IP interface:** It is used to list all the interface brief of all IP's connected.

Steps:

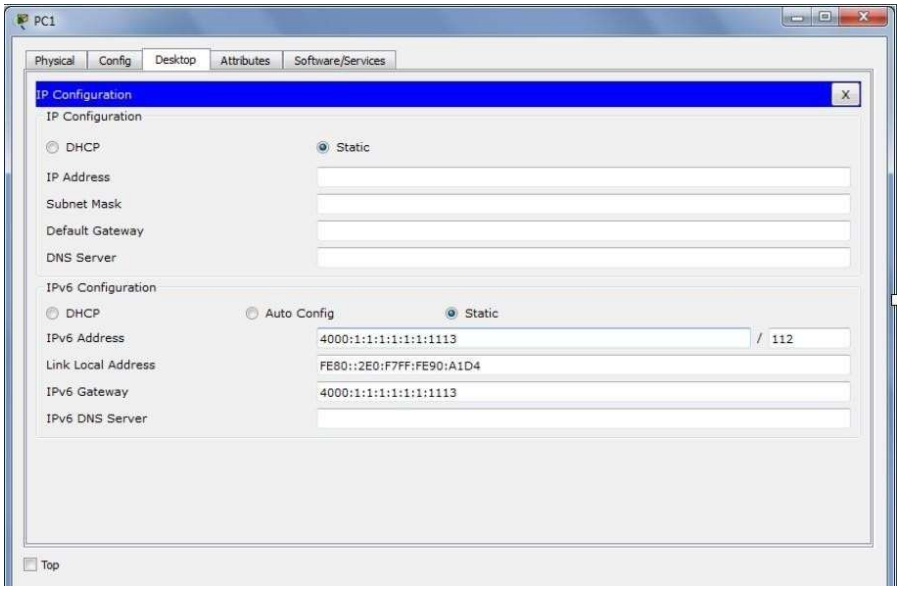
1: Scenario Created



2: To configure IPV6 address on PC0.



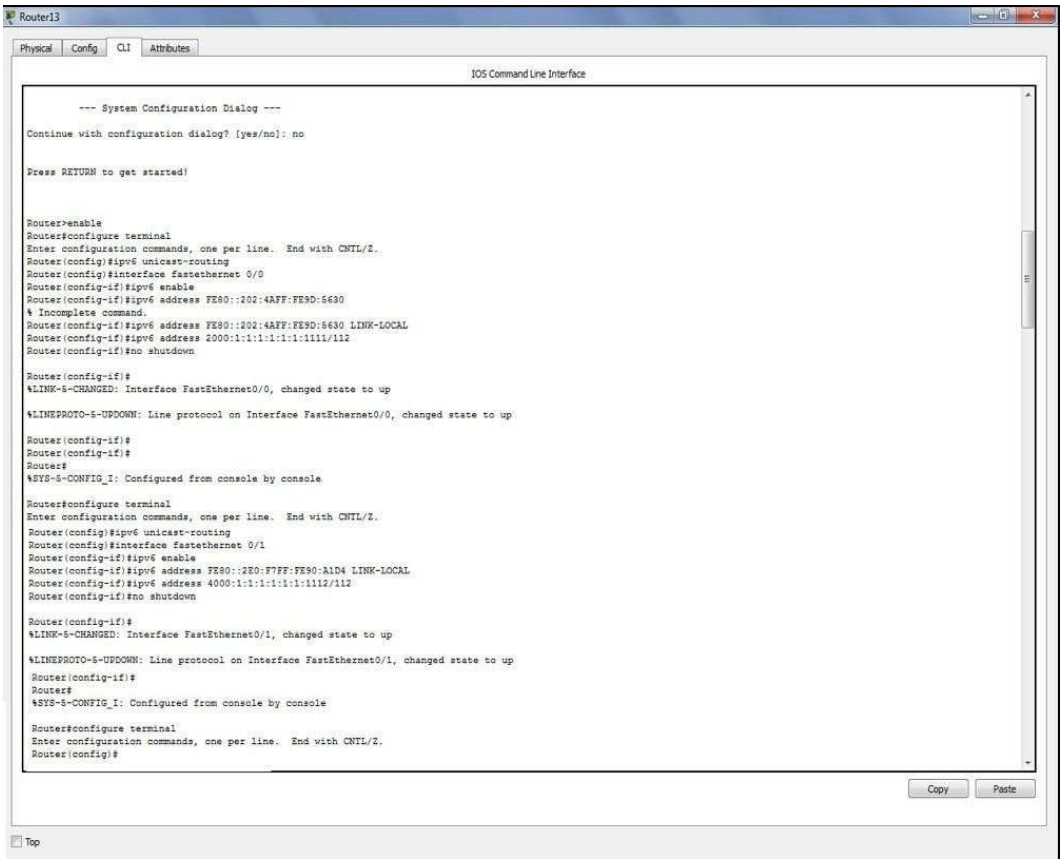
3: To configure IPV6 address on PC1.

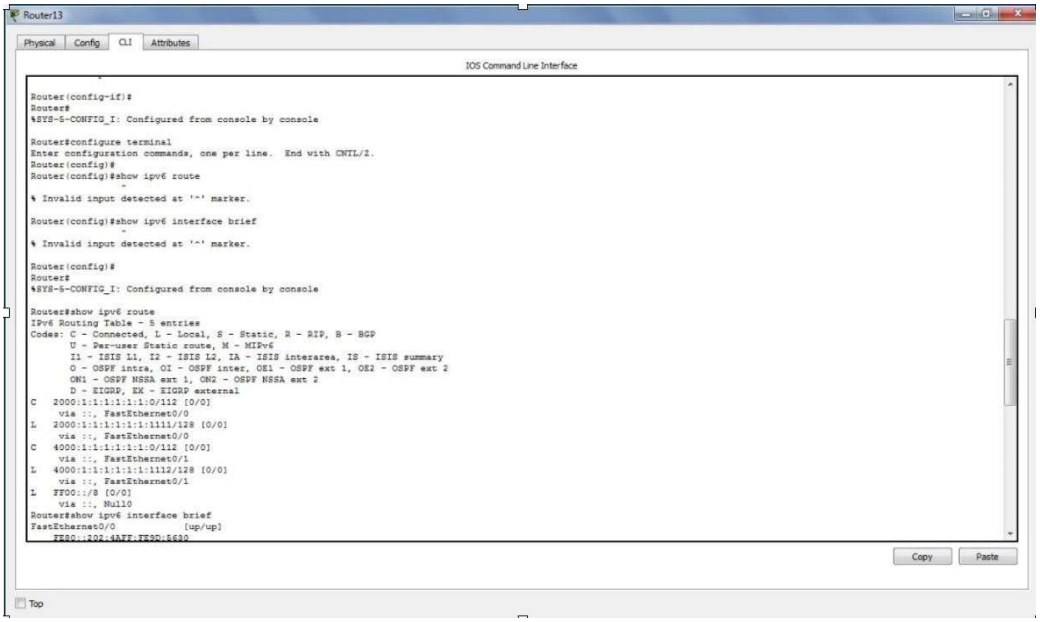


4: To configure iPv6 routing in the network. Go to cmd interface of router0 and type followingcommands:

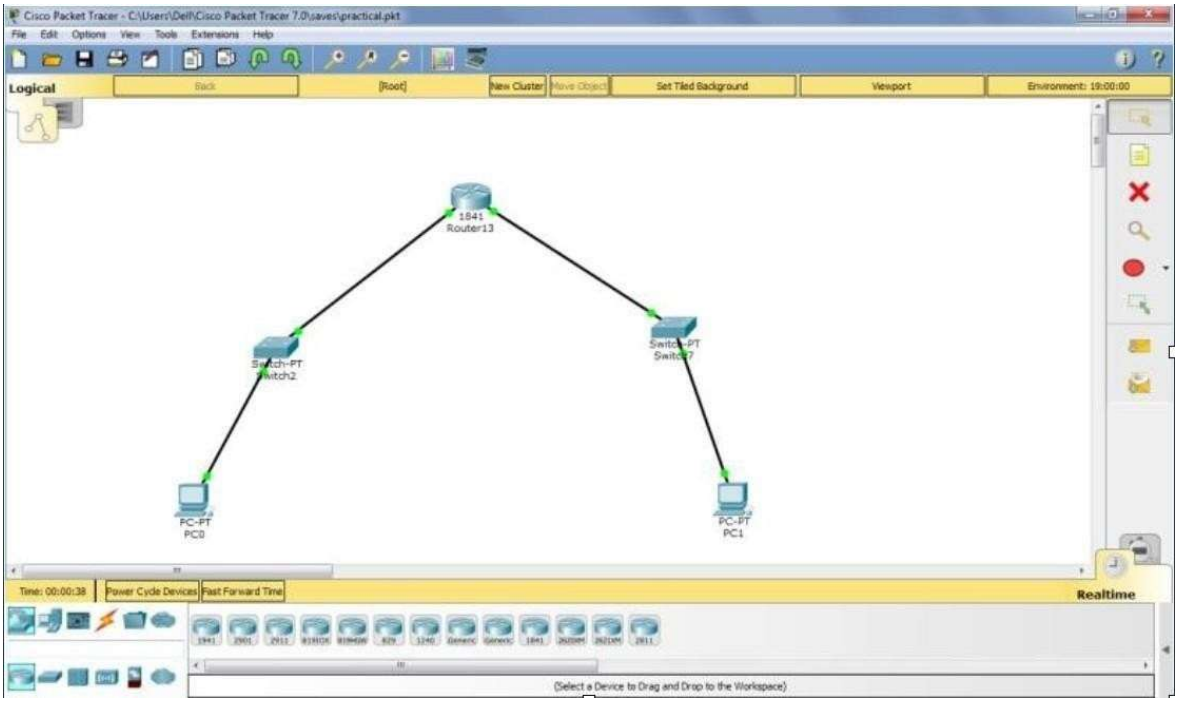
- Enable
- Configure terminal
- Ipv6 unicast-routing
- Interface casteth Ernst 0/0
- Ipv6 enable
- Ipv6 address FE80::202:4AFF:FE9D:5630 LINK-LOCAL
- Ipv6 address 2000:1:1:1:1:1:1:1111/112

- No shutdown
- Press “CTRL” to exit from current working mode of router
- Ipv6 enable
- Ipv6 address FE80::202:4AFF:FE9D:5630 LINK-LOCAL
- Ipv6 address 4000:1:1:1:1:1:1:1112/112
- No shutdown
- Press “CTRL” to exit from current working mode of router





5: After completely executing these commands the IPV6 address scheme plan will be enabledand all connections will be established.

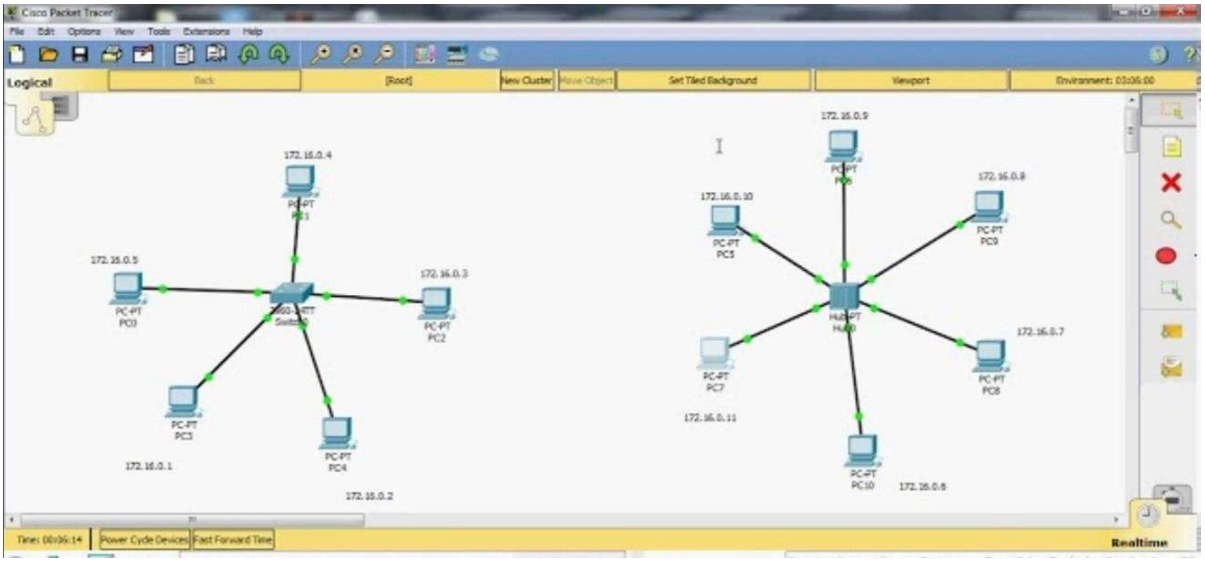


Task 6 : Creation of Simple Networking topologies using hubs and switches.

Creating simple network topologies with hubs and switches in Cisco Packet Tracer is a great way to understand how devices communicate within a local network. Here's a guide to setting up basic topologies:

1. Star Topology Using a Hub

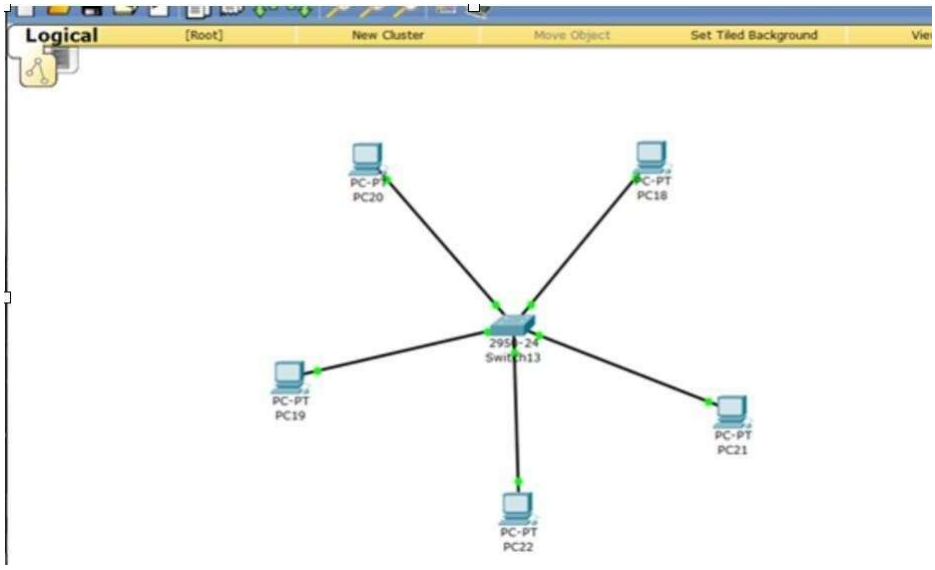
- **Add Devices**: Drag one hub and a few end devices (PCs) onto the workspace in Packet Tracer.
- **Connect Devices to Hub**: Use copper straight-through cables to connect each PC to the hub.
- **Assign IP Addresses**: Go to each PC, open the IP Configuration tab, and assign each a unique IP address within the same subnet (e.g., 192.168.1.1 to 192.168.1.4 with a subnet mask of 255.255.255.0).
- **Test Connectivity**: Use the ping command in the Command Prompt of each PC to test communication. For example, type ping 192.168.1.2 from PC1 to check if it can reach PC2.



2. Star Topology Using a Switch

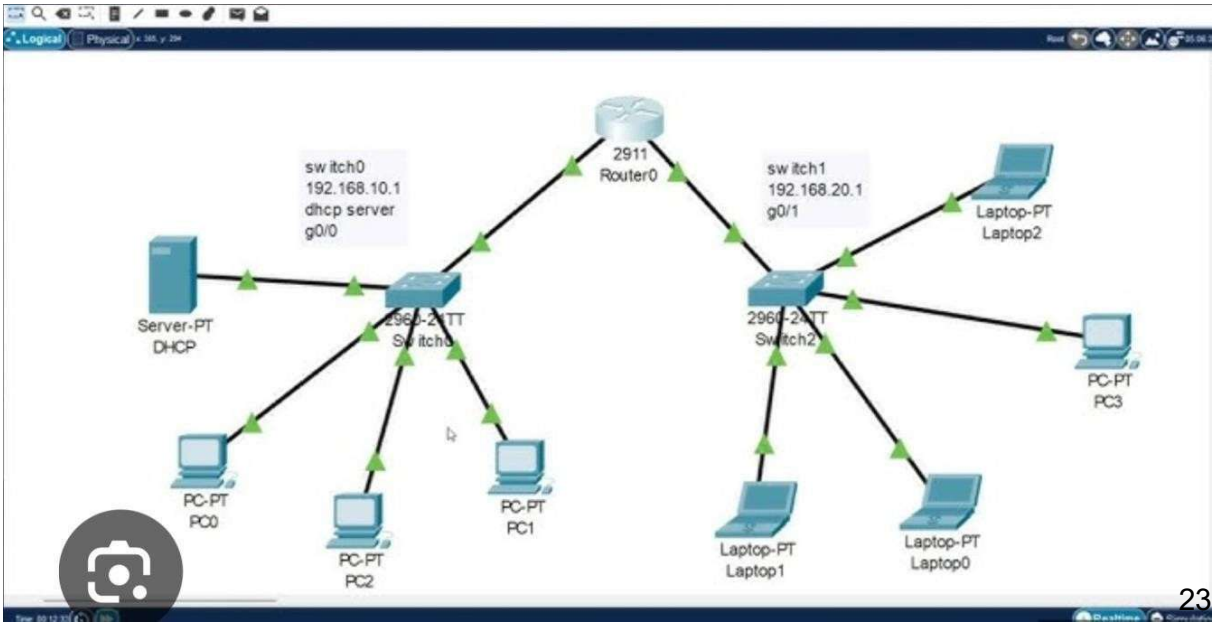
- **Add Devices**: Place one switch and a few PCs onto the workspace.
- **Connect Devices to Switch**: Use copper straight-through cables to connect each PC to the switch.
- **Assign IPAddresses**: Follow the same steps as above to assign each PC a unique IP within the same subnet.

- **Test Connectivity**: Use the ping command to verify communication between PCs. Unlike a hub, a switch learns which devices are on which ports, so it sends data only to the intended recipient, making it more efficient.



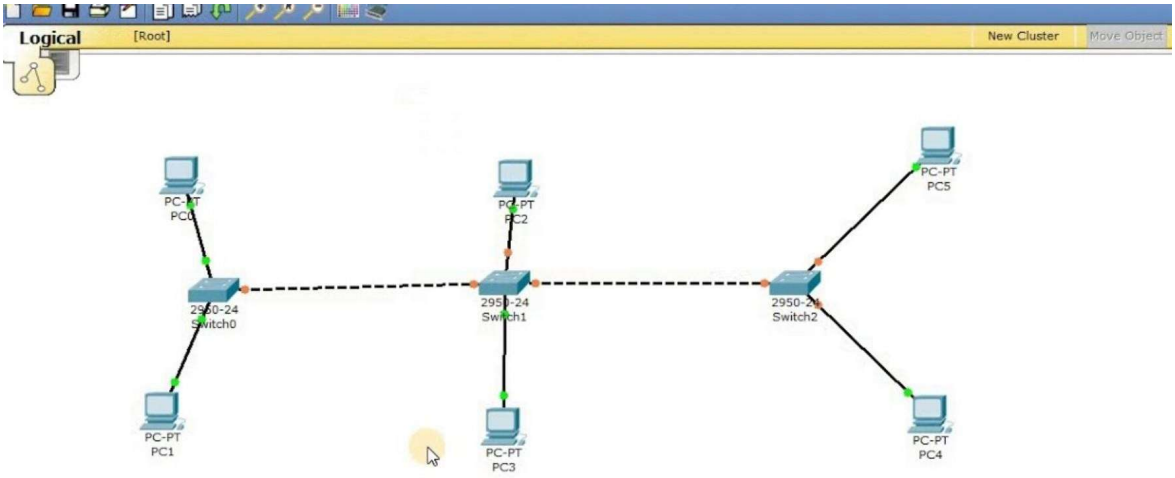
3. Extended Star Topology with Multiple Switches

- **Add Devices**: Place two switches and several PCs on the workspace.
- **Connect Switches and PCs**: Use copper straight-through cables to connect each PC to one of the switches. Then, connect the two switches to each other using another straight-through cable.
- **Assign IPAddresses**: Ensure all devices are in the same subnet so they can communicate.
- **Test Connectivity**: Ping PCs across the two switches to confirm the extended network allows devices to communicate seamlessly.



4. Bus Topology Simulation with Hubs and Switches

- While Packet Tracer doesn't directly support bus topology, you can simulate it by chaining hubs or switches to emulate a bus-like network.
- **Add Devices and Connect**: Connect each PC to a hub or switch, then chain the hubs/ switches together.
- **Assign IPs and Test**: Give each PC an IP and use ping to test communication across the simulated bus setup.



Task 7 : Simulation of web traffic in Packet Tracer Task.

Steps: To simulate web traffic in Cisco Packet Tracer, you can set up a basic network with devices like PCs, servers, and routers, and then generate web traffic to see how data flows through the network. Here's a step-by-step guide to accomplish this:

1. Set Up the Network Topology

- Add Devices: Add at least two PCs, a server (to act as a web server), a switch, and optionally a router if you want to simulate inter-network traffic.
- Connect Devices: Use copper straight-through cables to connect the PCs and the server to the switch. If you're using a router, connect it to the switch with a similar cable.

2. Configure IP Addresses

- Assign IP Addresses to PCs and Server: Go to each device, enter the IP configuration settings, and assign IP addresses and subnet masks to each PC and the server.
- Configure the Gateway (if using a router): Set the default gateway on each device to the router's IP if you're simulating traffic across different networks.

3. Configure the Web Server

- Select the server, go to the Services tab, and enable the HTTP (web) service. This will allow other devices to access the web server.

4. Generate Web Traffic

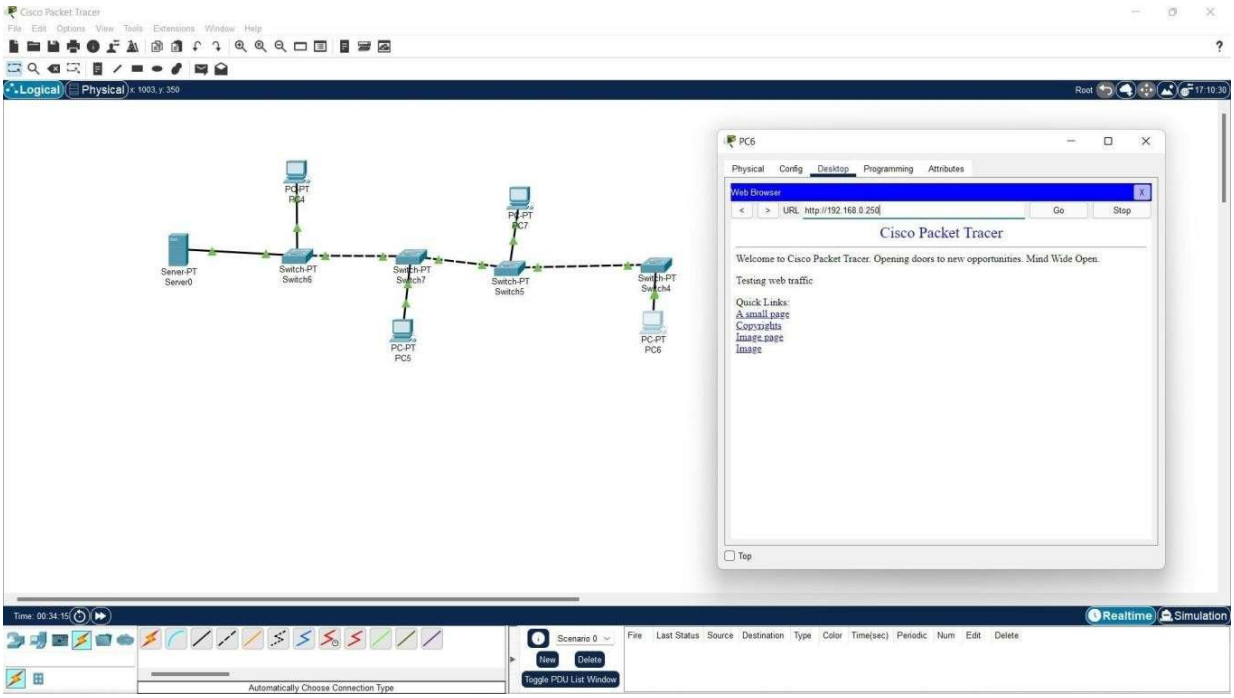
- On a PC, open the Web Browser application, enter the server's IP address in the address bar, and press Enter. This simulates a user accessing a webpage hosted on the server.
- Observe the Packet Flow: Packet Tracer will show the web traffic path, illustrating the process of data packets traveling from the PC to the web server and back.

5. Use Simulation Mode

- Switch to Simulation Mode (from Realtime Mode), which lets you visualise the packets as they travel through the network.
- Start the web traffic again by accessing the server from a PC. Packet Tracer will display each packet's journey, showing the path through the switch, router, or any other device.

6. Analyze Traffic Flow

- In Simulation Mode, click on individual packets to view details like source and destination IP addresses, protocols used (e.g., HTTP), and the stages of the packet as it moves through the network.



Task 8 : Study and implementation of various router configuration commands

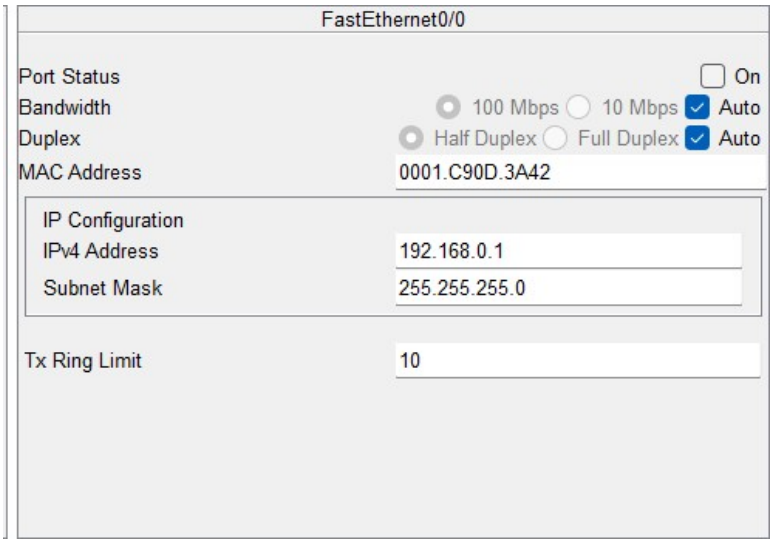
Steps : To help with studying and implementing router configuration commands in Packet Tracer, here are some essential commands and their uses for configuring routers:

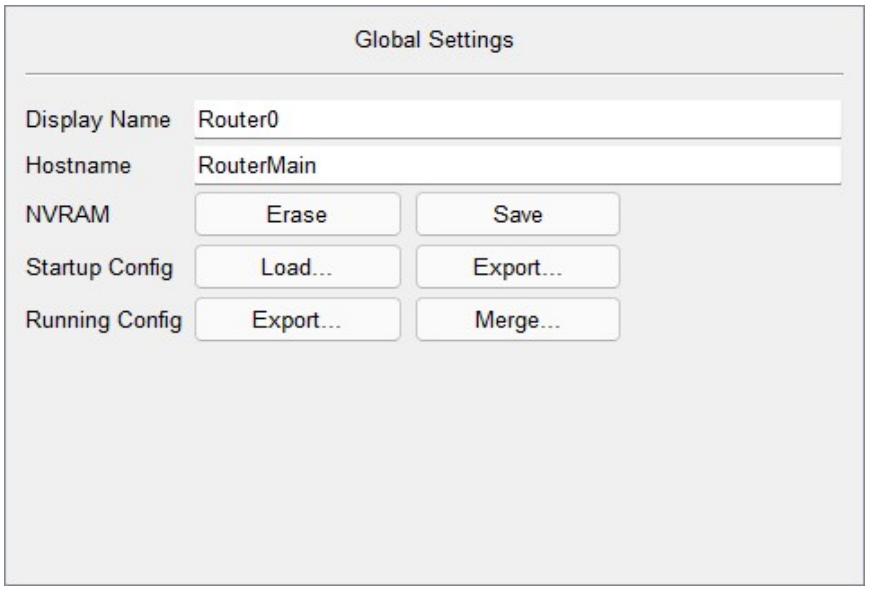
- Select 'Router' from the toolbar and select any router.
- Click on the router and then from the window select the CLI option and focus the terminal.
- In the terminal write 'enable' and then press enter. This will enable the router cli now we can runcommands on the terminal.
- Perform some basic commands like giving the hostname, password, setting up an interface, give Ip addressand subnet mask etc.
- For this first type 'configure terminal' and press enter.
- To give host name type 'hostname [hostname]' here (MainRouter)
- To give a password enter 'enable secret [password]' e.g., 123
- To set up an interface use 'interface f0/0'
- To then set an IP address to this interface use 'Ip address [ip_address] [subnet_mask]' e.g., 192.168.0.1255.255.255.0
- To exit the terminal use 'exit' to go back

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterMain
RouterMain(config)#enable secret 123
RouterMain(config)#no ip domain-lookup
RouterMain(config)#interface gigabitethernet 0/8
%Invalid interface type and number
RouterMain(config)#interface
% Incomplete command.
RouterMain(config)#interface gigabitethernet 0/8
%Invalid interface type and number
RouterMain(config)#ip address 192.168.0.1 255.255.255.0
                   ^
% Invalid input detected at '^' marker.

RouterMain(config)#ip 192.168.0.1 255.255.255.0
                   ^
% Invalid input detected at '^' marker.

RouterMain(config)#
RouterMain#
%SYS-5-CONFIG_I: Configured from console by console
enable
RouterMain#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterMain(config)#interface f0/0
RouterMain(config-if)#ip address 192.168.0.1 255.255.255.0
RouterMain(config-if)#exit
RouterMain(config)#
```

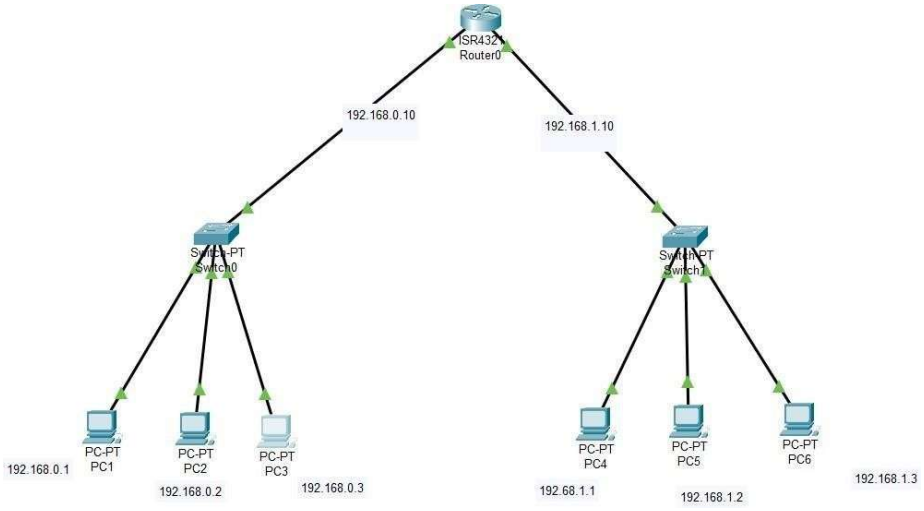

FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.C90D.3A42
IP Configuration
IPv4 Address
192.168.0.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10

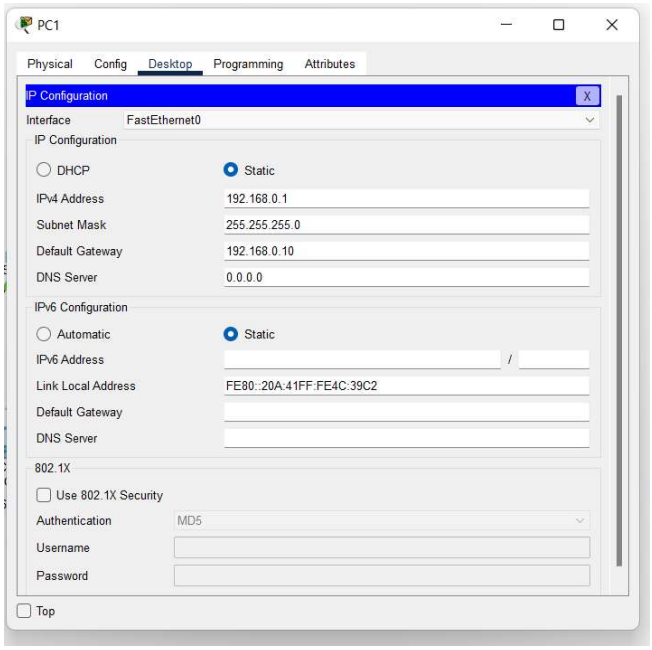

Global Settings
Display Name
Router0
Hostname
RouterMain
NVRAM
Erase
Save
Startup Config
Load...
Export...
Running Config
Export...
Merge...

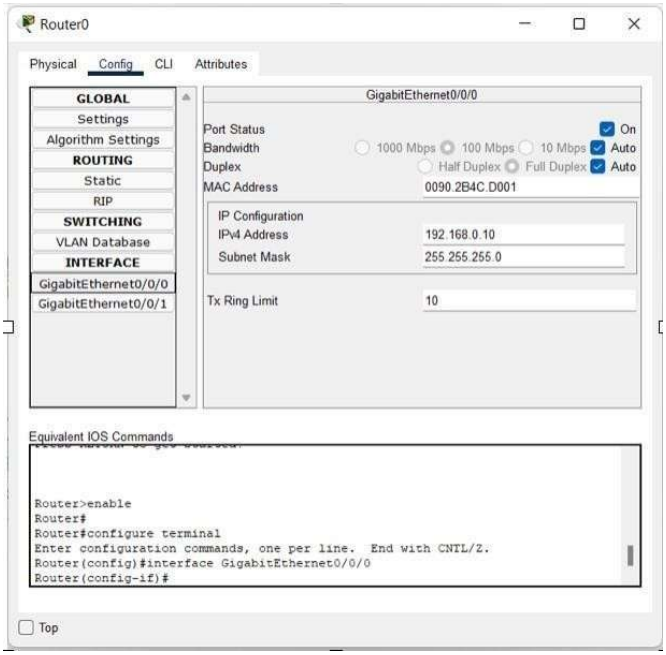
Task 9 : Creation of Networks using routers.

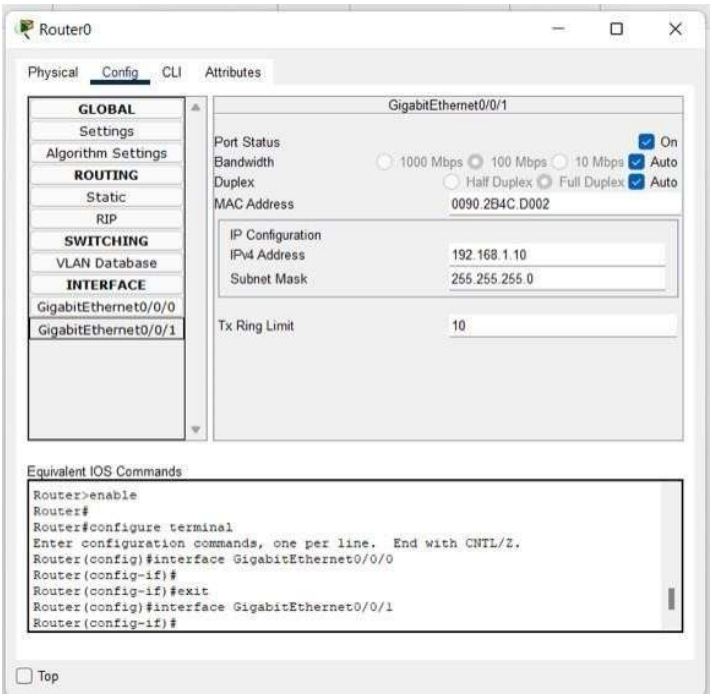
Steps :

- Toolbox ->Routers -> Any required Router e.g., 4321
- Toolbox -> End devices -> 6 PCs
- Toolbox -> Switches -> 2 switches
- Toolbox -> cables -> Cooper straight through cable to connect PCs with router
- Click on Router-0 and open ‘Config’
- Go to Interface ->
    - Gigbitethernet0/0/0: IP address 192.168.0.10 and ‘on’ the Port Status
    - Gigbitehernet0/0/1: IP address 192.168.1.10 and ‘on’ the Port Status
- Go to PC1, PC2, PC3 and give them IP addresses starting from 192.168.0.1 and default gatewayas 192.168.0.10
- Go to PC4, PC5, PC6 and give them IP addresses starting from 192.168.1.1 and default gatewayas 192.168.1.10
- Send a packet and test.




PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.0.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.0.10
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::20A:41FF:FE4C:39C2
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
GigabitEthernet0/0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0090.2B4C.D001
IP Configuration
IPv4 Address
192.168.0.10
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Top


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
GigabitEthernet0/0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0090.2B4C.D002
IP Configuration
IPv4 Address
192.168.1.10
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Top

Task 10 : Configuring networks using the concept of subnetting.

Configuring networks with subnetting is crucial for managing large networks efficiently. Subnetting involves dividing a larger network into smaller, manageable sub-networks (or subnets). Here's how to configure networks using subnetting in Packet Tracer.

Example Scenario

Let's assume you have an IP address range of `192.168.1.0/24` and need to divide this into four subnets for different departments.

Step 1: Determine Subnet Requirements

With `192.168.1.0/24`, you have 256 IP addresses (from `192.168.1.0` to `192.168.1.255`). Dividing it into four subnets requires **changing the subnet mask** to provide smaller subnets:

- **New Subnet Mask**: Changing from `/24` to `/26` (255.255.255.192) provides four subnets, each with 64 addresses.
- **Subnets**:
  - Subnet 1: `192.168.1.0/26` (usable IPs: `192.168.1.1` to `192.168.1.62`)
  - Subnet 2: `192.168.1.64/26` (usable IPs: `192.168.1.65` to `192.168.1.126`)
  - Subnet 3: `192.168.1.128/26` (usable IPs: `192.168.1.129` to `192.168.1.190`)
  - Subnet 4: `192.168.1.192/26` (usable IPs: `192.168.1.193` to `192.168.1.254`)

Each subnet now has 62 usable IPs, which can be assigned to devices.

Step 2: Set Up Network Devices in Packet Tracer

- **Add Routers and Switches**: Place a router to manage communication between the subnets. Add four switches, one for each subnet.
- **Connect the Devices**: Use copper straight-through cables to connect each PC to its respective switch. Connect each switch to the router.

Step 3: Configure IP Addresses on Each Subnet

- For each PC in each subnet, assign an IP within its designated range. Example:
  - **Subnet 1 (Department A)**: `192.168.1.1/26` to `192.168.1.62/26`
  - **Subnet 2 (Department B)**: `192.168.1.65/26` to `192.168.1.126/26`
  - **Subnet 3 (Department C)**: `192.168.1.129/26` to `192.168.1.190/26`

- **Subnet 4 (Department D)**: `192.168.1.193/26` to `192.168.1.254/26`
  - **Configure Default Gateways**: Set the default gateway on each PC to the router's IP for that subnet (e.g., `192.168.1.1` for Subnet 1).

Step 4: Configure the Router

- **Assign IP Addresses to Router Interfaces**:
  - The router needs an interface in each subnet. In Packet Tracer, use sub-interfaces if your router has only one physical interface.
  - Example configuration for Router sub-interfaces:

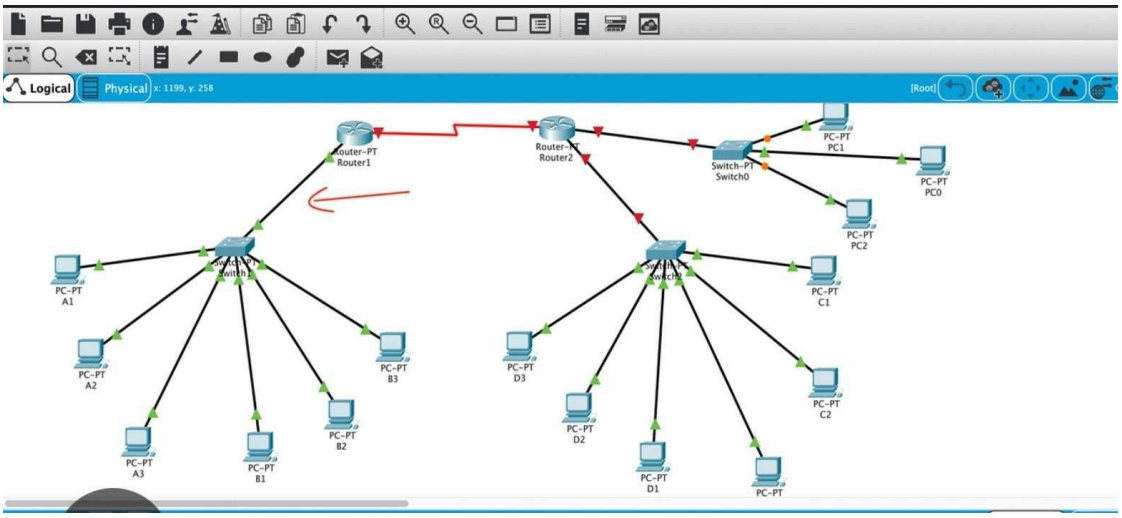
```
Router(config)# interface GigabitEthernet0/0.1
Router(config-subif)# encapsulation dot1Q 1
Router(config-subif)# ip address 192.168.1.1 255.255.255.192

Router(config)# interface GigabitEthernet0/0.2
Router(config-subif)# encapsulation dot1Q 2
Router(config-subif)# ip address 192.168.1.65 255.255.255.192
```

- **Repeat for All Subnets**: Configure additional sub-interfaces for each subnet on the router.

Step 5: Test Connectivity

- **Ping Devices Across Subnets**: In Packet Tracer, use the **ping** command on PCs to test connectivity to other PCs in different subnets.
- **Verify Routing**: Use the `show ip route` command on the router to verify that it has routes to each subnet.



Task 11 : Practical implementation of basic network command and Network configuration commands like ping, ipconfig, netstat, tracert etc. for troubleshooting network related problems.

Tracert : This command is used to diagnose path-related problems. On an IP network, routers exchange IP packets between the source and the destination. They take IP packets from the source host and forward them in a sequence until they reach the destination host. The sequence of routers between the source and destination is known as the path. A path consists of all routers in a sequence that IP packets sent from the source host traverse to reach the destination host.

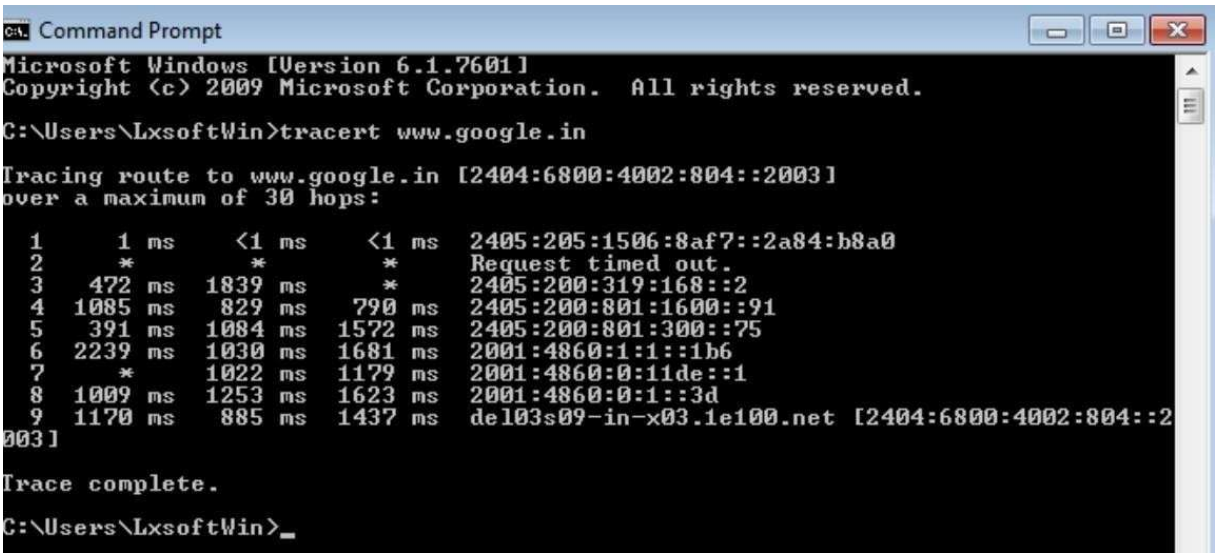
The tracert command prints the path. If all routers on the path are functional, this command prints the full path. If a router is down on the path, this command prints the path up to the last operational router

The tracert command uses the following syntax.

tracert Destination *Name or IP address*

The following command traces the path to the host named www.google.co.in.

tracert www.google.co.in



Option	Description
-d	Do not resolve the IP addresses of intermediate routers to their names.
-h	Specifies the maximum number of hops (routers) to search on the path. The default is 30 hops.
-w	Specifies the amount of time in milliseconds to wait for a reply message from the router. If not receiveddefault time-out is 4000 (4 seconds).

The following table lists some important options of the **tracert** command.

Ping : The ping command is used to test connectivity between two hosts. It sends ICMP echo request messages to the destination. The destination host replies with ICMP replies messages. If the ping command gets a reply from the destination host, it displays the reply along with round-trip times.

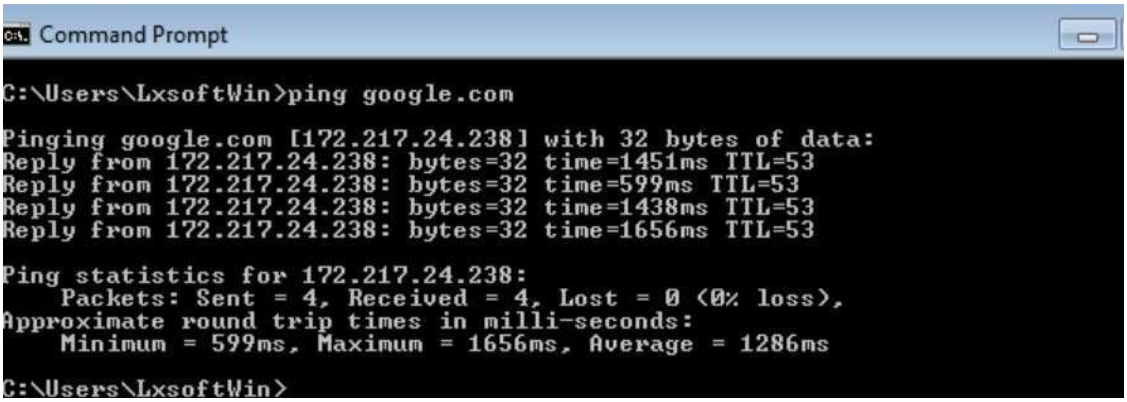
The **ping** command uses the following syntax.

ping *destination host IP or name*

The following command tests connectivity between the host computer and Google's server.

ping **google.com**

The following image shows the output of this command.



If you specify the hostname as an argument, the ping command uses the configured DNS client service to automatically translate the hostname into the IP address.

Arp : To send IP packets, a computer needs two addresses. These addresses are the MAC address and the IP address. A MAC address is the physical or hardware address of the NIC. An IP address is the logical or software address of NIC. If a computer knows the IP address of the destination computer but it does not know the MAC address of the destination computer, it uses the ARP protocol to know the MAC address of the destination computer.

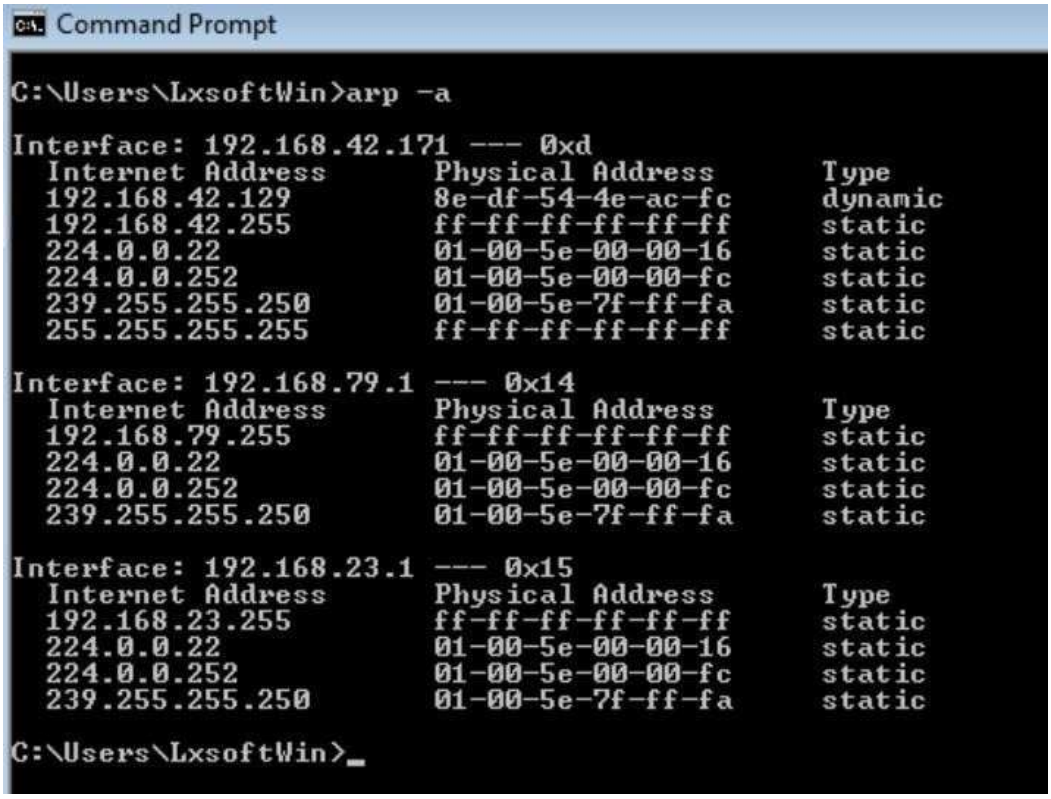
The ARP protocol broadcasts a given IP address over a local network. The corresponding host responds to the broadcast with its MAC address. To avoid repetition, ARP stores the answer in a table known as **ARP table**. ARP maintains a separate ARP table for each NIC.

To view the ARP table, you can use the following command.

```
arp
```

By default, this command displays the ARP table of the active NIC. If multiple NICs are installed on the computer, you can use the **-a** option with this command. If the -a option is used, the ARP command displays all ARP tables.

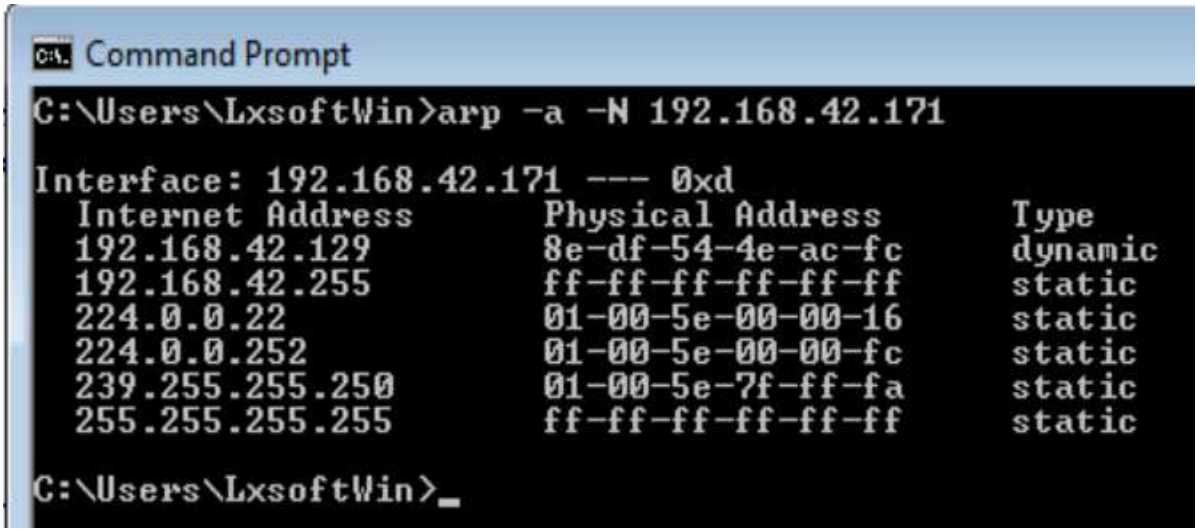
The following image shows the output of the arp command when used with the **-a** option.



To display the ARP cache entry for a specific IP address, specify the IP address with the **-N** option. For example, the following command displays the ARP cache table for the interface that is assigned the IP address 192.168.42.171.

```
Arp -a -N 192.168.42.171
```

The following image shows the output of the above command.



Netstat : This command displays active connections, ports on which the computer is listening, Ethernet statistics,the IP routing table, and IP statistics.

The output of this command is organised in rows and columns. Each row represents a new connection or an entry in the output. It contains four columns. These columns provide the following information about the row.

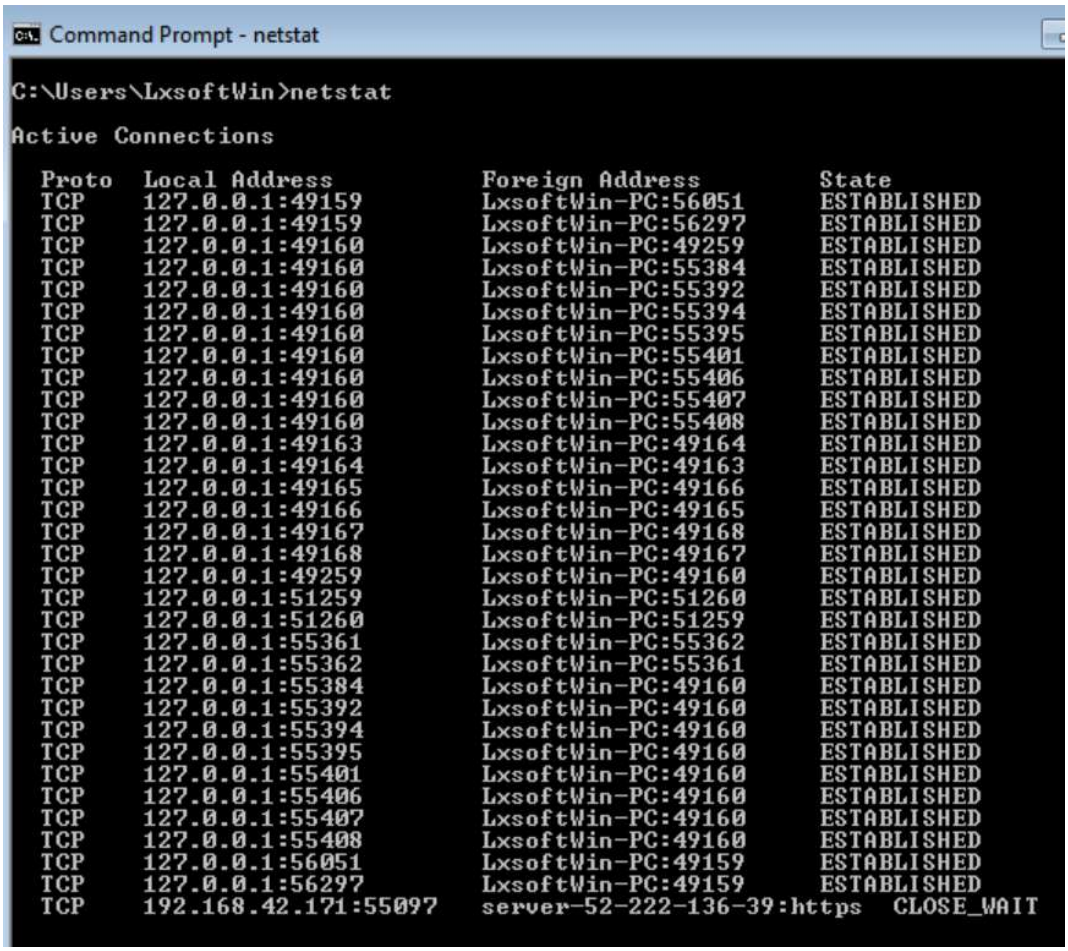
Proto: - This column displays the name of the protocol (TCP or UDP).

Local Address: - This column displays the IP address of the local computer and the port number being used. If the port is not yet established, the port number is shown as an asterisk (*).

Foreign Address: - This column displays the IP address and port number of the remote computer towhich the port is connected.

State: - This column displays the status of the connection.

The following image shows the sample output of this command.



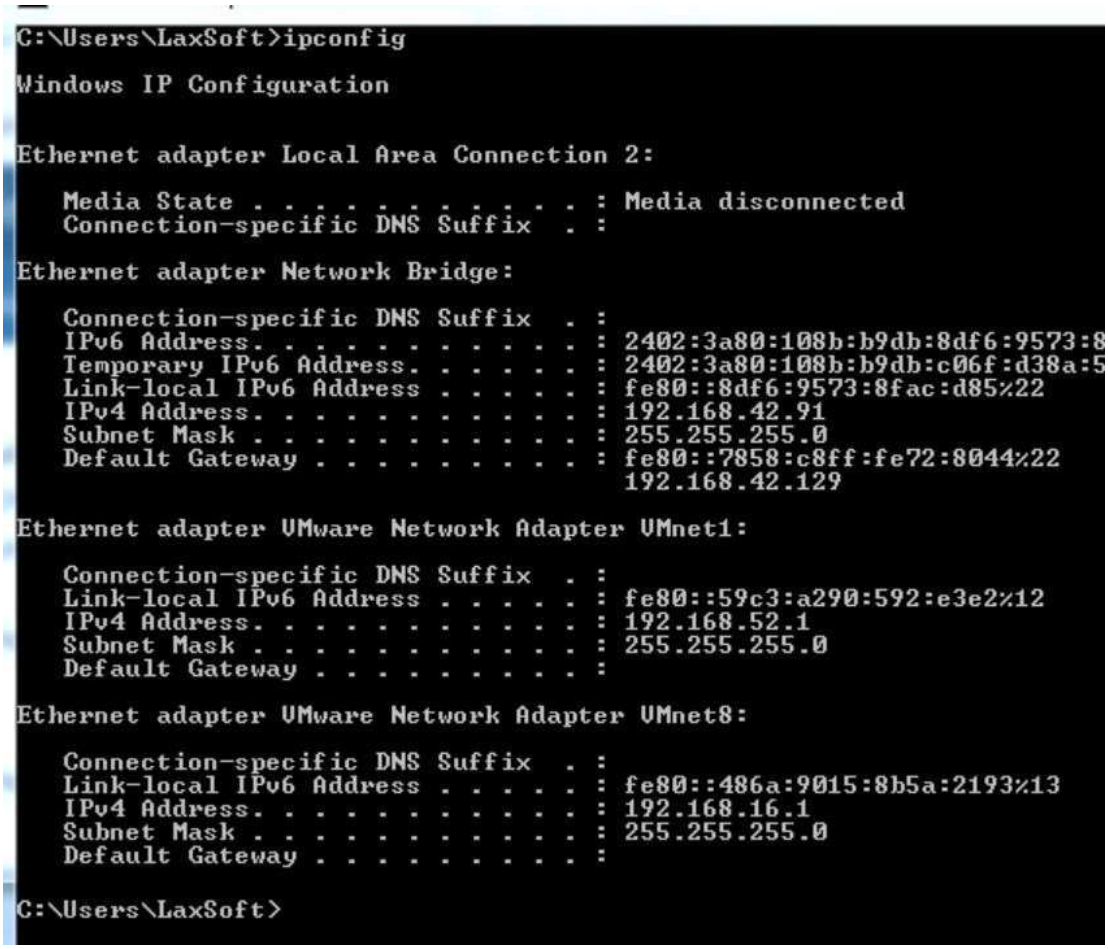
Options and parameters

Option	Description
-a	Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
-e	Displays Ethernet statistics, such as the number of bytes and packets sent and received.
-n	Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.
-o	Displays active TCP connections and includes the process ID (PID) for each connection.
-p	Shows connections for the protocol specified by Protocol. In this case, the Protocol can be TCP, UDP, tcpv6, or udpv6.
-s	Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols.
-r	Displays the contents of the IP routing table.

The following table lists some common options of the netstat command.

Ipconfig : This command displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. This command is mainly used to view the IP addresses on the computers that are configured to obtain their IP address automatically.

The following image shows the sample output of this command.



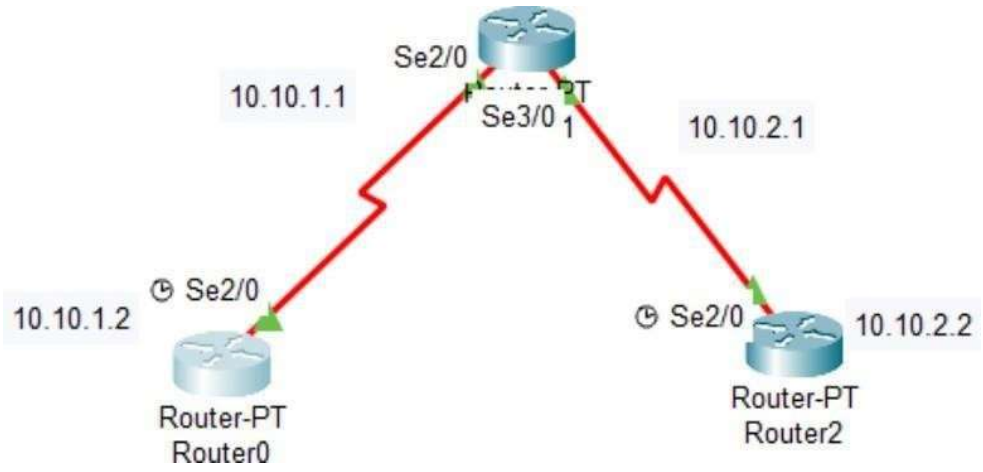
Used without parameters	Displays the IP address, subnet mask, and default gateway for all adapters.
/all	Displays the full TCP/IP configuration for all adapters.
/renew [Adapter]	Renews DHCP configuration for all adapters (if an adapter is not specified) or for a specific
/release [Adapter]	Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configurall adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter i
/flushdns	Flushes and resets the contents of the DNS client resolver cache.

The following table lists some important options of the **ipconfig** command.

Task 12 : Configuration of networks using static and default routes.

Steps :

- Go to Toolbox and select any three routers. Here Router-PT
- Go to the Toolbox and select the cables and attach the routers in a linear order
- Click on Router0 and open its config, there in se/2 give the IP address and subnet mask as 10.10.1.2 and 255.255.255.0 respectively
- Click on Router1 and open its config, there in se/2 give the IP address and subnet mask as 10.10.1.1 and 255.255.255.0 respectively
- For the same router configure the interface se/3 and give the IP address as 10.10.2.1 and subnetmask as 255.255.255.0
- Click on Router2 and open its config, there in se/2 interface give the IP and subnet mask as
  10.10.2.2 and 255.255.255.0 respectively
- Now try send message from Router0 to Router1 (successful), Router1 to Router2 (successful) andRouter0 to Router2 (FAILED)
- The message from Router0 to Router2 failed because there is no path from Router0 to Router2 asshown from using ‘show ip route’ command




```
%SYS-5-CONFIG_I: Configured from console by console
show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.0.0/24 is directly connected, Serial2/0
```

- Now to enable messaging from Router0 to Router2 set a static route from Router0 to Router2
- Click on Router0 and open config then in settings > static fill the fields of IP address, subnet maskand Next hop as 10.10.2.0, 255.255.255.0, 10.10.1.1 respectively.
- Now again try sending now it will be successful
- Do similar for Router2 so it can also send messages to Router0