******

Computer network

Lab work

* **Study of Interconnection Device**
* **Explain Computer Networks**

Computer networks are systems of interconnected computers and devices that enable communication and data sharing among them. These networks can be established using various technologies, including wired (such as Ethernet cables) and wireless (such as Wi-Fi) connections. The primary purpose of computer networks is to facilitate the exchange of information and resources among users, devices, and applications.

Key components and concepts of computer networks include:

* Nodes: These are the individual devices connected to the network, such as computers, servers, printers, and smartphones.
* Links: Links are the communication channels that connect nodes. They can be physical cables (wired) or radio waves (wireless).
* Topology: Topology refers to the arrangement of nodes and links in a network. Common topologies include star, bus, ring, and mesh.
* Protocols: Protocols are rules and standards that govern data exchange and communication between devices. They ensure that devices can understand and interpret each other's signals and messages.
* LAN (Local Area Network): A LAN connects devices within a limited geographic area, like a home, office, or campus. LANs are commonly used for resource sharing and local communication.
* WAN (Wide Area Network): A WAN spans a larger geographic area, often connecting LANs across cities, countries, or continents. The internet itself is a massive example of a WAN.
* Internet: The internet is a global network of networks that enables worldwide communication and information exchange. It uses a variety of protocols, including TCP/IP, for data transmission.
* Intranet: An intranet is a private network within an organization that uses internet technologies to facilitate internal communication, collaboration, and information sharing.
* Extranet: An extranet is an extension of an intranet that allows controlled access to authorized external users, such as partners, suppliers, or clients.
* Client-Server Model: In this model, some devices (clients) request resources or services from other devices (servers). Servers fulfill these requests and provide the necessary resources.
* Peer-to-Peer (P2P) Model: In this model, devices communicate and share resources directly with each other without a central server. This is often used for file sharing.
* **Explain Interconnecting Devices**

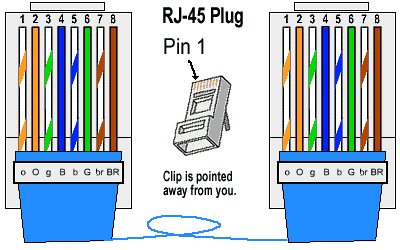
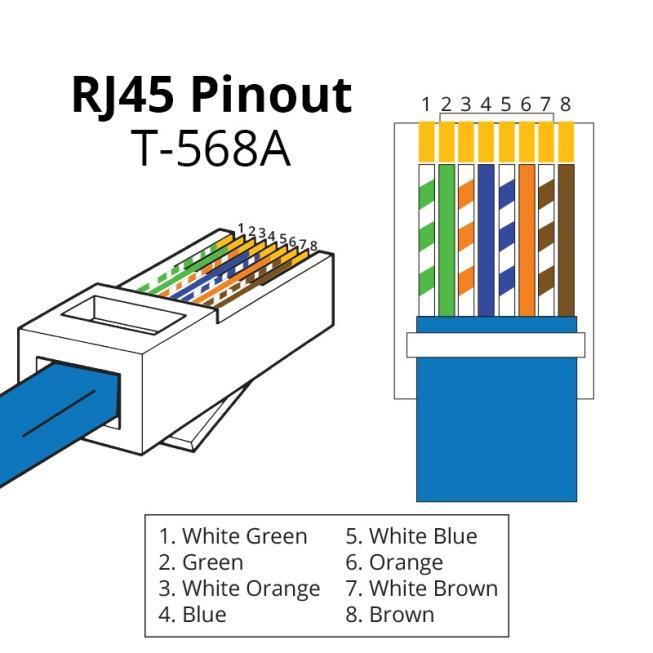
Interconnecting devices, within the context of computer networks, are hardware components that facilitate communication and data exchange between various devices within a network. They enable the efficient transfer of data, allowing devices to communicate, share resources, and access the internet. These devices play a vital role in the functioning of computer networks by managing the flow of data and ensuring that information reaches its intended destination accurately and in a timely manner.

Here are some common types of interconnecting devices used in computer networks:

* Routers: Routers are devices that connect different networks together and determine the best path for data to travel from the source to the destination. They use routing tables to make decisions about how to forward data packets.
* Switches: Switches are used to connect devices within the same network. They operate at the data link layer and forward data only to the specific device it's intended for, improving network efficiency.
* Hubs: Hubs are older and simpler devices that operate at the physical layer. They broadcast data to all devices connected to them, which can lead to network congestion and reduced efficiency. Hubs are less commonly used today
* Access Points: Access points are used in wireless networks to connect wireless devices to a wired network. They enable devices like laptops, smartphones, and tablets to access the network without the need for physical cables.
* Modems: Modems convert digital data from a computer into analog signals that can be transmitted over telephone lines or cable systems. They also perform the reverse operation, converting incoming analog signals back into digital data
* **Description:-**

RJ45, short for "Registered Jack 45," refers to a standard connector used primarily for Ethernet networking. It's a common type of connector used to terminate twisted pair cables, which are commonly used for both wired local area networks (LANs) and internet connections.

The RJ45 connector looks like a larger and wider version of a telephone jack (RJ11), but with eight pins instead of four. These pins correspond to the individual wires within an Ethernet cable. The connector is used to establish a physical connection between network devices, such as computers, switches, routers, and modems, allowing them to communicate with each other over a network.

** **

* Study of **t**ransmission media & tools : -

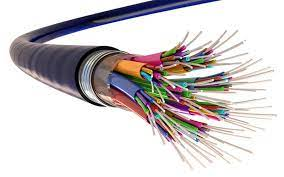
1.Coaxial cable-

Coaxial cable is an electrical cable consisting of a central conductor, insulating layer, metallic shield, and outer insulating layer. It's used to transmit high-frequency signals like those for cable TV, internet, and data networking. The central conductor carries signals while the metallic shield protects against interference and signal loss. The insulating layers isolate components and enhance durability. Coaxial cable is essential for reliable data transmission, offering efficient signal transmission while reducing external interference. Various types exist for specific applications, such as RG-6 for cable TV and broadband, making it a crucial technology for modern communication and broadcasting systems.



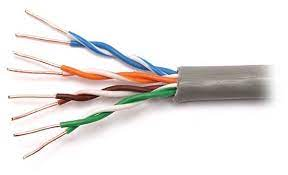
2.Fiber optic cable-

Fiber optic cable is a high-speed data transmission technology that uses thin strands of glass or plastic fibers to transmit data as pulses of light. These optical fibers carry information over long distances at incredibly high speeds, making them ideal for telecommunications and internet infrastructure. Light signals are reflected within the fiber, reducing signal loss and electromagnetic interference. Fiber optics offer enormous bandwidth and are immune to electrical interference, making them suitable for high-speed internet, long-distance communication, and data networking. They play a crucial role in modern telecommunications, enabling faster and more reliable data transmission compared to traditional copper cables.



3.Twisted cable-

Twisted pair cable is a common type of electrical cable used for transmitting data particularly in telecommunications and computer networking. It consists of pairs of insulated copper wires twisted together in a helical pattern to reduce electromagnetic interference and crosstalk. The twisting of wires helps cancel out external electromagnetic interference, enhancing signal quality. Twisted pair cables come in two main categories: unshielded twisted pair (UTP), which is commonly used for Ethernet networks, and shielded twisted pair (STP), which adds an extra layer of shielding to protect against interference. Twisted pair cables are versatile and cost-effective, making them widely used in phone lines, LANs, and other data transmission applications.



4.Crimping cable-

Crimping a cable involves attaching a connector, such as an RJ-45 connector for Ethernet cables or an RJ-11 connector for telephone cables, to the ends of bare wires within the cable. This process is crucial for creating reliable and functional connections in networking and telecommunications. To crimp a cable, the cable's insulation is stripped to expose the inner wires. These wires are then carefully arranged and inserted into the connector's pins. A crimping tool is used to securely press and deform the connector, ensuring that the wires make proper electrical contact. This technique is essential for creating custom-length cables and maintaining data transmission quality.



5.Connectors-

Connectors are devices used to join two or more electrical or electronic components, cables, or devices together, facilitating the transfer of signals, power, or data between them. They come in various forms, including plugs, jacks, sockets, and terminals, and are designed to match specific types of cables or ports. Connectors are essential components in electronics, telecommunications, and various industries, ensuring secure and reliable connections. They can be found in everyday technology, from USB connectors for data transfer to audio jacks for headphones and power connectors for charging devices. Connectors play a crucial role in enabling devices and systems to work together seamlessly.



6.RJ45 , RJ11-

RJ45 and RJ11 are standardized connectors used in telecommunications and networking. RJ45 connectors have eight pins and are commonly used for Ethernet cables, enabling high-speed data transmission in local area networks (LANs). They have become the standard for connecting computers, routers, and other networked devices.

On the other hand, RJ11 connectors have six pins and are typically used for telephone lines. They are prevalent in telephone systems, allowing the connection of telephones, fax machines, and modems to the telephone network. RJ11 connectors are smaller than RJ45 connectors and are primarily used for voice communication, though they can carry low-speed data as well.



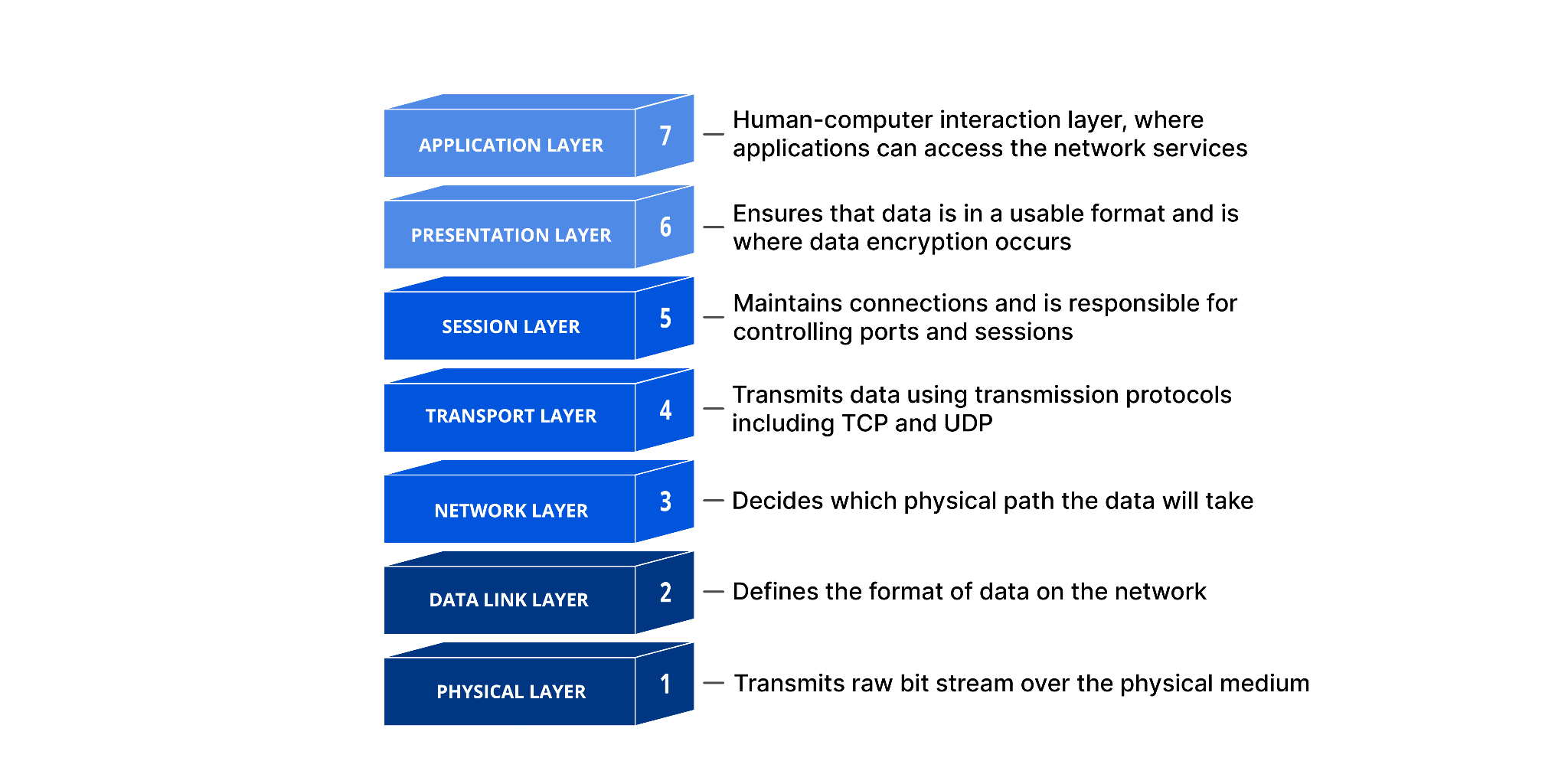
Q. Study of different networking models OSI & TCP?

“OSI Model (Open Systems Interconnection Model)”

The OSI model is a conceptual framework that standardizes the functions of a telecommunications or networking system into seven distinct layers. Each layer has a specific role and interacts with adjacent layers through defined protocols. The OSI model is a theoretical model and not directly implemented in networking hardware or software. It serves as a reference for understanding network communication.

The seven layers of the OSI model, from the lowest (Physical Layer) to the highest (Application Layer), are as follows: -

1. Physical Layer: This layer deals with the physical connection between devices and includes specifications for cables, connectors, and transmission of raw binary data over the network medium.
2. Data Link Layer: Responsible for data framing, error detection, and addressing at the link level. It includes protocols like Ethernet and MAC addresses.
3. Network Layer: Manages routing, addressing, and forwarding of data packets. The Internet Protocol (IP) operates at this layer.
4. Transport Layer: Ensures end-to-end communication, error correction, and data flow control. TCP and UDP are transport layer protocols.
5. Session Layer: Establishes, maintains, and terminates sessions or connections between applications. It manages dialog control and synchronization.
6. Presentation Layer: Translates data between application format and network format, handling data encryption and compression.
7. Application Layer: This is the topmost layer where application-specific protocols and interfaces reside, allowing user applications to interact with the network. Examples include HTTP, FTP, and SMTP.

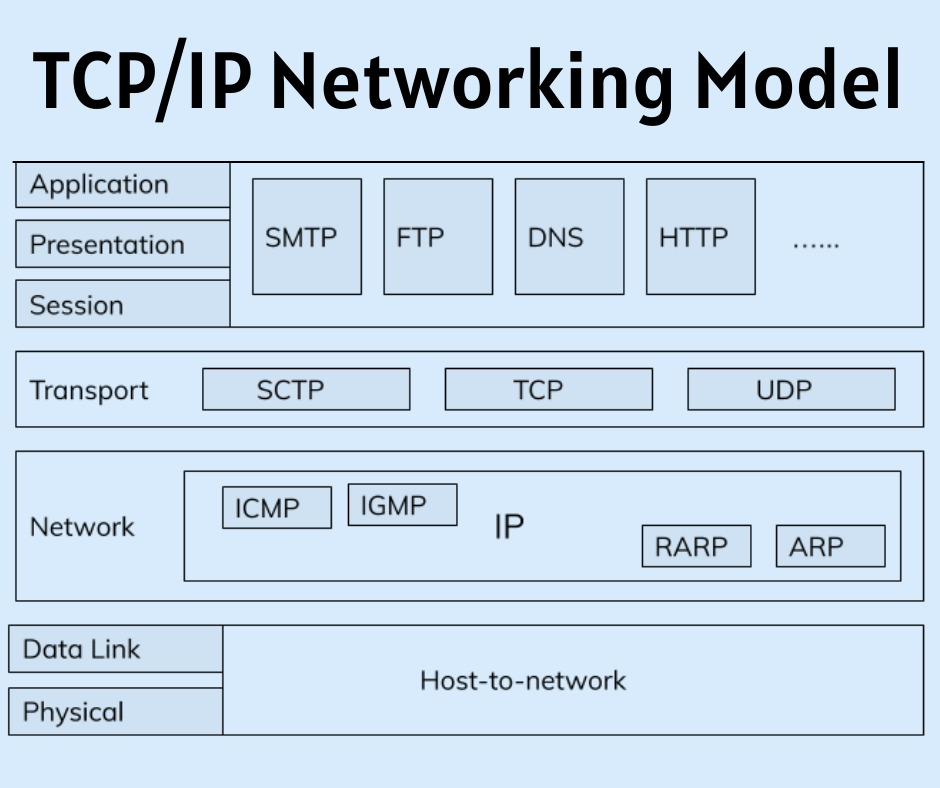


“ TCP/IP Model (Transmission Control Protocol/Internet Protocol Model)”

The TCP/IP model, also known as the Internet protocol suite, is a practical networking model used as the foundation for the modern Internet. It consists of four layers, which are often compared to the OSI model: -

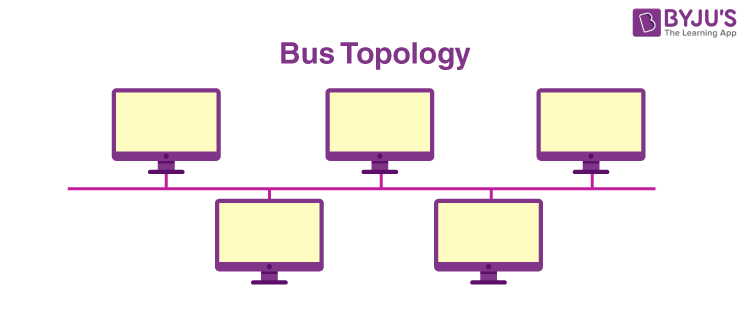
1. Network Interface Layer: This layer corresponds to the combined functions of the OSI Physical and Data Link layers. It deals with hardware-specific protocols and interfaces, such as Ethernet, Wi-Fi, and PPP.
2. Internet Layer: Corresponds to the OSI Network Layer. It primarily involves the Internet Protocol (IP) for routing packets between different networks.
3. Transport Layer: Similar to the OSI Transport Layer, it provides end-to-end communication and includes both TCP and UDP.
4. Application Layer: Unlike the OSI model, the TCP/IP model combines the Session, Presentation, and Application Layers into a single Application Layer. It includes all application-specific protocols like HTTP, FTP, DNS, and SMTP

DIAGRAM: -



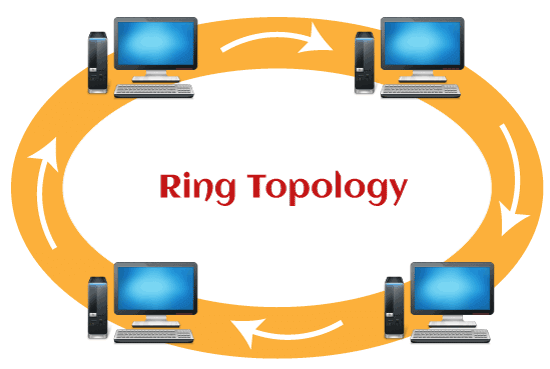
Q. Study of various LAN topologies & their application?

BUS topology: -



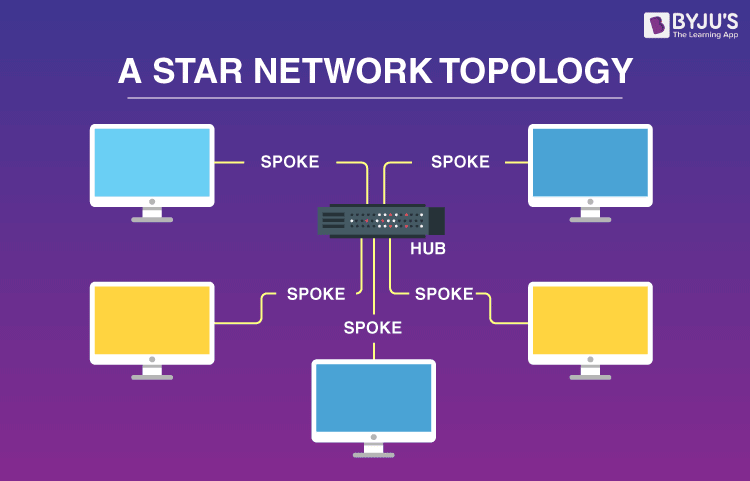
* The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
* Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
* When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
* The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
* The configuration of a bus topology is quite simpler as compared to other topologies.
* The backbone cable is considered as a "single lane" through which the message is broadcast to all the stations.
* The most common access method of the bus topologies is CSMA (Carrier Sense Multiple Access)

## Ring Topology: -



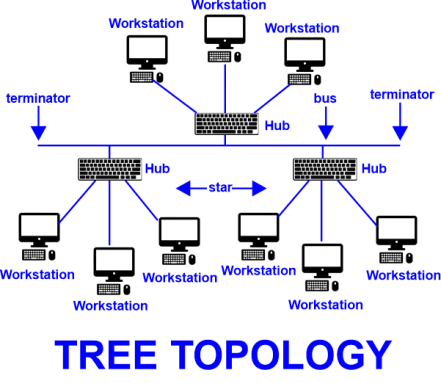
* Ring topology is like a bus topology, but with connected ends.
* The node that receives the message from the previous computer will retransmit to the next node.
* The data flows in one direction, i.e., it is unidirectional.
* The data flows in a single loop continuously known as an endless loop.
* It has no terminated ends, i.e., each node is connected to other node and having no termination point.
* The data in a ring topology flow in a clockwise direction.
* The most common access method of the ring topology is token passing.
  + Token passing: It is a network access method in which token is passed from one node to another node.
  + Token: It is a frame that circulates around the network.

Star topology: -



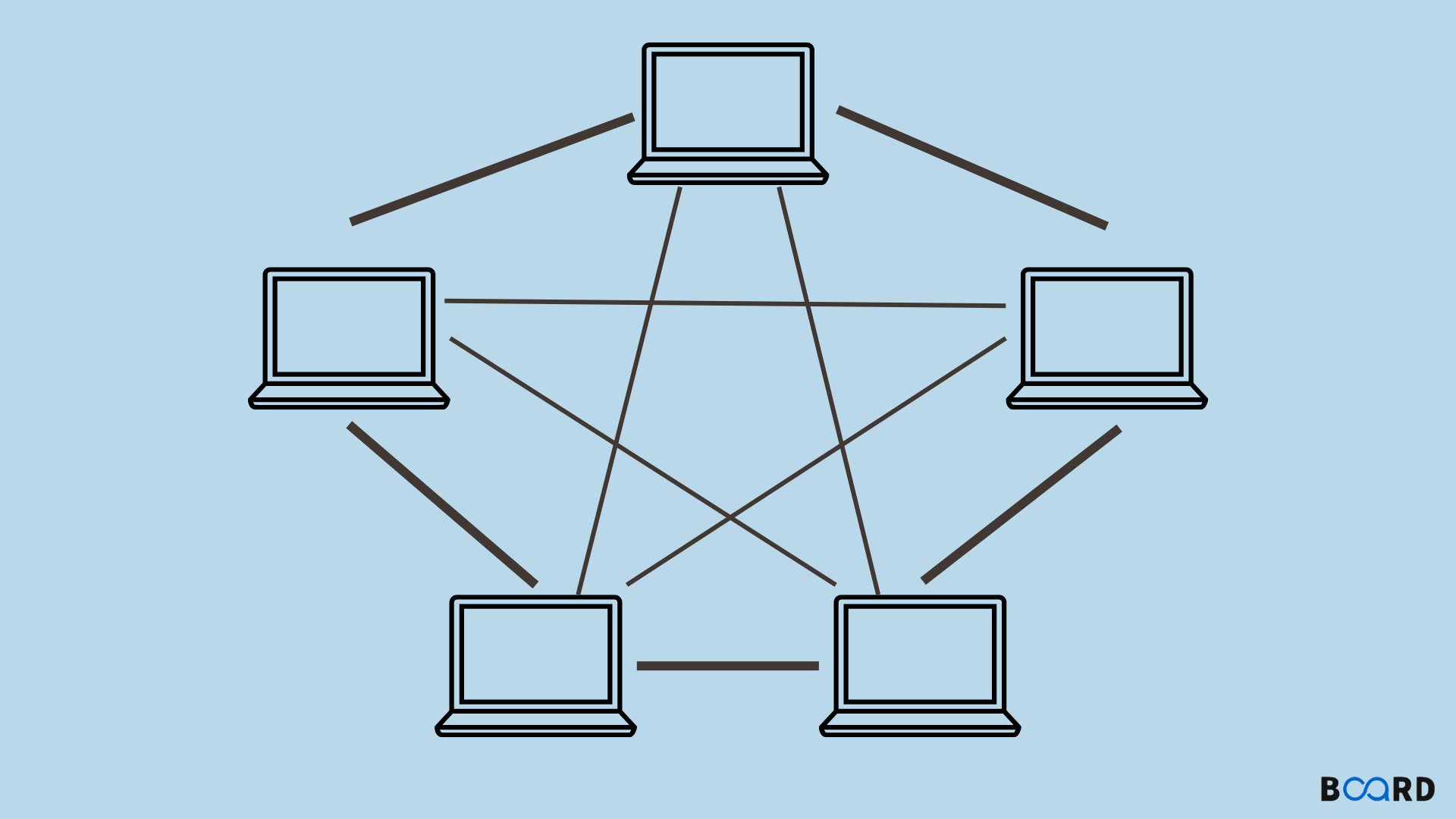
* Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
* The central computer is known as a server, and the peripheral devices attached to the server are known as clients.
* Coaxial cable or RJ-45 cables are used to connect the computers.
* Hubs or Switches are mainly used as connection devices in a physical star topology.
* Star topology is the most popular topology in network implementation.

Tree topology: -



* Tree topology combines the characteristics of bus topology and star topology.
* A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
* The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
* There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

Mesh topology: -



* Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
* There are multiple paths from one computer to another computer.
* It does not contain the switch, hub or any central computer which acts as a central point of communication.
* The Internet is an example of the mesh topology.
* Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
* Mesh topology is mainly used for wireless networks.

Mesh topology can be formed by using the formula:

Number of cables = (n\*(n-1))/2.

Q. Study of basic network & network configuration command?

Studying basic networking and network configuration commands is essential for understanding and managing computer networks. Below, I'll provide an overview of some fundamental networking concepts and common commands used for network configuration on Unix/Linux systems.

1. IP Addressing:

* ifconfig (or ip addr): Displays or configures network interfaces and their IP addresses.
* ping: Tests network connectivity by sending ICMP echo requests to a host.
* netstat (or ss): Shows network statistics, including open ports and routing tables.

2. Network Configuration:

* ifconfig or ip: Used to configure network interfaces, set IP addresses, and configure network parameters.
* route or ip route: Sets up static routes or displays the routing table.
* hostname: Sets or displays the system's hostname.

3. DNS Configuration:

* /etc/hosts: A local file for mapping hostnames to IP addresses.
* /etc/resolv.conf: Contains DNS server configurations.

4. Firewall Configuration:

* iptables: Used to configure the Linux firewall (netfilter) rules.
* ufw (Uncomplicated Firewall): A user-friendly interface for managing iptables rules.

5. Network Services:

* systemctl: Used to manage system services, including network-related services.
* netstat, ss, or lsof: Helpful for listing open ports and associated processes.

6. Network Diagnostics:

* traceroute or mtr: Traces the route packets take to reach a destination.
* tcpdump or wireshark: Packet sniffing tools for network troubleshooting and analysis.

7. SSH and Remote Access:

* ssh: Secure Shell for remote access to other systems securely.
* scp: Securely copy files between systems using SSH.

8. Network File Sharing:

* nfs: Network File System for sharing files between Unix/Linux systems.
* samba: Allows Unix/Linux systems to share files with Windows systems using the SMB/CIFS protocol.

9. DHCP Configuration:

* dhclient or systemctl: Used to obtain or configure dynamic IP addresses.

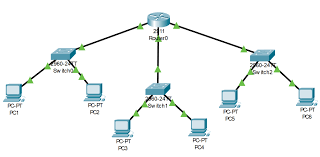
10. Network Testing and Tools: - curl and wget:

* Download files from the internet. - nc (netcat): A versatile networking utility for reading/writing data across network connections.

Q.Study of Standard Network Simulator:

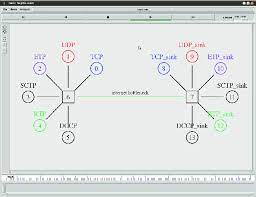
1.Cisco Packet Tracer-

Cisco Packet Tracer is a network simulation and visualization tool developed by Cisco Systems. It allows users to create, configure, and simulate network topologies, making it a valuable tool for networking students and professionals to practice and experiment with various networking scenarios, protocols, and configurations in a virtual environment.



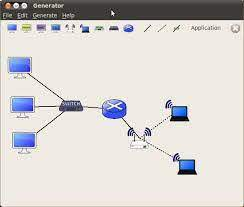
2.NS2-

NS2, or Network Simulator 2, is an open-source software tool used for simulating and analyzing computer networks. It is widely used in academic and research environments to model and study network protocols, performance, and behavior. NS2 allows researchers to evaluate and experiment with network designs, making it a valuable tool in the field of computer networking.



3.NS3-

NS3, or Network Simulator 3, is an open-source network simulation framework used for modeling and simulating computer networks. It is a powerful tool for researchers, developers, and educators in the field of networking. NS3 provides a platform to design, test, and evaluate network protocols, algorithms, and applications, aiding in the development and optimization of network technologies.



4.Opnet-

OPNET (Optimized Network Engineering Tools) was a software suite used for network modeling and simulation, especially in the field of network performance analysis and optimization. It allowed users to simulate and analyze complex computer networks, aiding in the design, evaluation, and troubleshooting of network systems. Note that as of my last knowledge update in September 2021, OPNET had been acquired by Riverbed Technology and integrated into their product offerings. There may have been further developments or changes since then.



Q.Installation of Cisco Packet Tracer

As of my last knowledge update in September 2021, I can provide general guidance on how to install Cisco Packet Tracer. Please note that there may have been updates or changes since then, so it's a good idea to visit the official Cisco Networking Academy website for the most current installation instructions. Here are the general steps for installing Cisco Packet Tracer:

* 1.Obtain Packet Tracer:
  + Cisco Packet Tracer is often available through the Cisco Networking Academy program. You may need to register for a Cisco Networking Academy account to access the download.
* 2.Check System Requirements:
  + Ensure your computer meets the minimum system requirements for Packet Tracer. These requirements may vary depending on the version of Packet Tracer you're installing.
* 3.Download Packet Tracer:
  + Visit the Cisco Networking Academy website or the Cisco Packet Tracer download page.
  + Sign in with your Cisco Networking Academy account if required.
  + Locate the Packet Tracer download for your operating system (Windows or Linux).
  + Click on the download link to start the download.
* 4.Install Packet Tracer:
  + Once the download is complete, locate the installer file and run it.
  + Follow the on-screen instructions to install Packet Tracer.
  + Accept the license agreement and choose the installation directory when prompted.
* 5.Launch Packet Tracer:
  + After the installation is complete, you can typically find Packet Tracer in your computer's applications or programs menu.
  + Launch the application.
* 6.Log In:
  + Depending on the version and licensing, you may be prompted to log in with your Cisco Networking Academy credentials. Follow the login instructions provided.
* 7.Start Using Packet Tracer:
  + You can now start using Cisco Packet Tracer to create, configure, and simulate network topologies for learning and practicing networking concepts.

Q.Demonstration of Simple Network Configuration using Cisco Packet Tracer

Here's a demonstration of a simple network configuration using Cisco Packet Tracer. In this example, we'll set up a basic network with two PCs connected through a switch.

Step 1: Open Cisco Packet Tracer

* Launch Cisco Packet Tracer from your computer's applications or programs menu.

Step 2: Create a Network Topology

* Click on the "Add a Simple PDU" icon in the bottom-left corner to enable automatic IP assignment for PCs.

Step 3: Add Devices

* Drag and drop two PCs (End Devices) from the left sidebar onto the workspace.
* Drag and drop a Switch (Switches and Hubs) onto the workspace.

Step 4: Connect Devices

* Click on the "Copper Straight-Through" cable type in the left sidebar.
* Click on one of the PCs and then click on one of the switch ports to connect them. Repeat this for the other PC.

Step 5: Configure IP Addresses

* Click on one of the PCs to select it.
* Click on the "Config" tab in the right sidebar.
* Enter an IP address (e.g., 192.168.1.1) and subnet mask (e.g., 255.255.255.0).
* Repeat the same process for the other PC with a different IP address (e.g., 192.168.1.2).

Step 6: Test Connectivity

* Click on one of the PCs to select it.
* Click on the "Desktop" tab in the right sidebar.
* Open a web browser (e.g., HTTP) and enter the IP address of the other PC (e.g., [http://192.168.1.2](http://192.168.1.2/)).
* You should see a successful connection.

Step 7: Save Your Project

* Go to "File" > "Save" to save your network configuration project.

Q.Case Study of DHCP , DNS Protocols

Case Study: Network Management for XYZ Corporation

Scenario: XYZ Corporation is a large multinational company with offices worldwide. They are looking to optimize their network infrastructure to improve efficiency and user experience.

DHCP Implementation:

Problem: Manually configuring IP addresses for each device in the organization's vast network is time-consuming, error-prone, and lacks flexibility.

Solution: Implement DHCP for automatic IP address assignment.

Implementation Steps:

* DHCP Server Deployment: Set up DHCP servers in the data center and branch offices. Configure scopes for each subnet, defining IP address ranges, subnet masks, and lease durations.
* Client Configuration: Configure all devices (computers, printers, phones) to obtain IP addresses automatically through DHCP.
* Scope Management: Continuously monitor and manage DHCP scopes to ensure they have enough available addresses and suitable lease times.
* Redundancy: Implement DHCP failover for fault tolerance to ensure uninterrupted IP address assignment even if one DHCP server fails.

DNS Implementation:

Problem: Users are struggling to remember IP addresses, and the organization wants to enable user-friendly domain names.

Solution: Implement DNS for name-to-IP address resolution.

Implementation Steps:

* DNS Server Deployment: Set up DNS servers, both primary and secondary, in the organization's data centers for redundancy. Configure forward and reverse lookup zones.
* Domain Name Registration: Register a domain name (e.g., xyzcorp.com) with a domain registrar.
* DNS Records: Create DNS records (A records, CNAME records, MX records) to map domain names to IP addresses and manage mail routing.
* Client Configuration: Configure all devices to use the organization's DNS servers for name resolution.
* DNS Security: Implement DNSSEC (DNS Security Extensions) to enhance DNS security and prevent DNS spoofing attacks.

Results:

* With DHCP, XYZ Corporation experiences simplified network management, reduced human errors, and improved IP address allocation efficiency.
* DNS allows users to access resources using user-friendly domain names, enhancing the overall user experience.
* DNSSEC ensures data integrity and authenticity, enhancing DNS security.
* Together, DHCP and DNS improve network efficiency and user satisfaction, enabling the organization to focus on its core operations.