Computer Networks Notes for Interview

PLACEMENT PREPARATION [EXCLUSIVE NOTES]

SAVE AND SHARE WITH YOUR CONNECTION TO HELP THEM

Network:

A network is a collection of devices that are interconnected through physical media links. It allows multiple nodes (devices) to share data either within a local group or by connecting different networks together.

Network Topology:

Network topology refers to the arrangement or layout of a computer network, showing how devices and cables are interconnected.

Types of Network Topology:

1) Star Topology:

In a star topology, all nodes are connected to a central device. This central device acts as a hub, and each node communicates directly with it.

Advantages of Star Topology:

- If a cable between a node and the central device fails, only that particular node is affected, leaving the rest of the network functional.

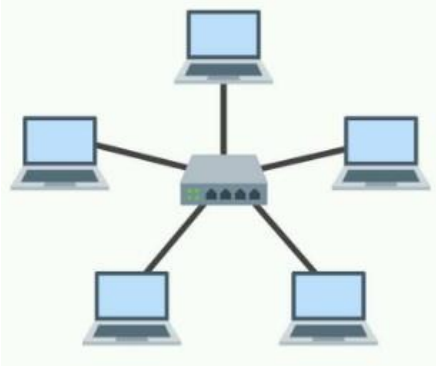
- Installation, management, and troubleshooting of a star topology are relatively simple.

Disadvantage of Star Topology:

- The entire network will fail if the central device itself is damaged.

Usage of Star Topology:

Star topology is commonly employed in both office and home networks. It provides a good balance between simplicity and robustness.



2) Ring Topology:

Ring topology is a type of network configuration where each node is precisely connected to two or more neighboring nodes, creating a continuous circular path for data transmission.

Advantages of Ring Topology:

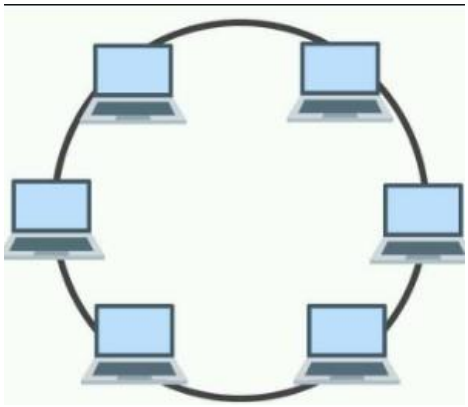
- Ring topology does not require a central server to manage connectivity among the nodes.

Disadvantages of Ring Topology:

- The entire network will fail if a single node in the ring is damaged or malfunctions.
- Ring topology is rarely used due to its high cost, complexity in installation, and management difficulties.

Examples of Ring Topology:

Some examples of networks that use ring topology are SONET (Synchronous Optical Networking) and SDH (Synchronous Digital Hierarchy) networks. However, these examples are not common in everyday networks due to the limitations and challenges of ring topology. forming a single continuous path for the transmission.



3) Bus Topology:

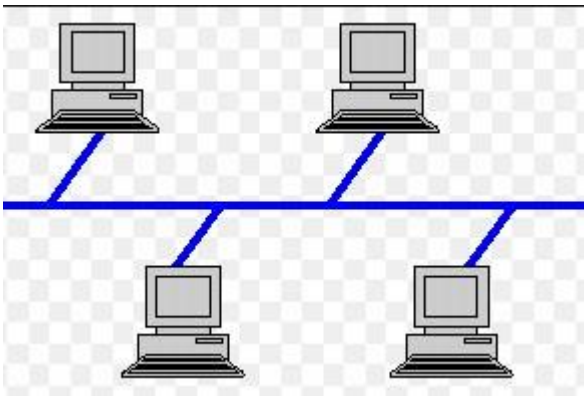
Bus topology is a network configuration where all nodes are connected to a single cable, referred to as the central cable or bus.

How it Works:

In bus topology, the central cable acts as a shared communication medium. When a device needs to send data to other devices, it transmits the data over the bus, which then distributes the data to all connected devices.

Suitability:
Bus topology is suitable for small networks with a limited number of devices.

Disadvantage:
One significant drawback of bus topology is that if the central bus is damaged or experiences a failure, the entire network will be affected, resulting in network failure.

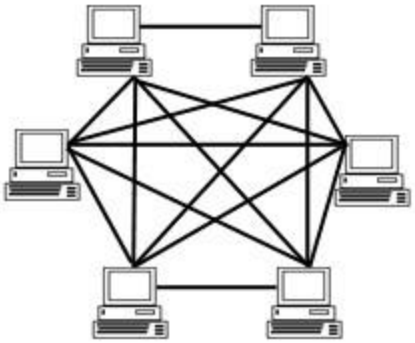


4) Mesh Topology:
Mesh topology is a network configuration where each node is directly connected to every other node in the network.

Advantages of Mesh Topology:
- Mesh topology does not rely on a central switch or hub for managing connectivity among the nodes.
- It offers high resilience as a failure in one cable will only affect the specific nodes connected to that cable.

Types of Mesh Topology:
1. Fully Connected Mesh Topology: In this type, all nodes are directly connected to every other node in the network.
2. Partially Connected Mesh Topology: In this type, not all nodes have direct connections to each other; some nodes have limited connections.

Disadvantages of Mesh Topology:
- Mesh topology is rarely used due to the complexity involved in installation and configuration, especially as the number of connections increases.
- The cabling cost is significantly high, as it requires a substantial amount of wiring to create direct links between nodes.



5) Tree Topology:

Tree topology is a network configuration that combines aspects of both the star and bus topologies, often referred to as the "expanded star."

How it Works:

In tree topology, multiple star networks are interconnected by a single bus, creating a hierarchical structure.

Ethernet Protocol:

The Ethernet protocol is commonly used in tree topology networks to facilitate communication.

Segmentation and Maintenance:

The network is divided into segments, each forming a star network. These segments can be managed and maintained individually. If one segment is damaged, it does not affect the operation of other segments.

Vulnerability:

However, tree topology heavily relies on the "main bus" connecting all the segments. If this main bus experiences a failure or breaks down, the entire network will be affected. This vulnerability is a crucial consideration when designing a tree topology network.

6) Hybrid Topology:

Hybrid topology is a network configuration that combines multiple different topologies to create a unique and flexible network structure.

Combining Topologies:
When two or more star topologies are connected, the resulting configuration remains a star topology. However, if a star topology is connected with a different topology, it transforms into a hybrid topology.

Flexibility and Implementation:
One of the key advantages of a hybrid topology is its flexibility. It can be implemented in various network environments, allowing network designers to tailor the configuration to suit specific requirements and constraints. This adaptability makes hybrid topology a popular choice in complex networking scenarios.

Different Types of Networks : (Imp) - Networks can be divided on the basis of area of distribution. For example:

- **PAN (Personal Area Network)**: Its range limit is up to 10 meters. It is created for personal use. Generally, personal devices are connected to this network. For example computers, telephones, fax, printers, etc.
- **LAN (Local Area Network)**: It is used for a small geographical location like office, hospital, school, etc.
- **HAN (House Area Network)**: It is actually a LAN that is used within a house and used to connect homely devices like personal computers, phones, printers, etc.
- **CAN (Campus Area Network)**: It is a connection of devices within a campus area which links to other departments of the organization within the same campus.
- **MAN (Metropolitan Area Network)**: It is used to connect the devices which span to large cities like metropolitan cities over a wide geographical area.
- **WAN (Wide Area Network)**: It is used over a wide geographical location that may range to connect cities and countries.
- **GAN (Global Area Network)**: It uses satellites to connect devices over the global area.

- **VPN (Virtual Private Network)** : VPN or the Virtual Private Network is a private WAN (Wide Area Network) built on the internet. It allows the creation of a secured tunnel (protected network) between different networks using the internet (public network). By using the VPN, a client can connect to the organization's network remotely.
- **Advantages of VPN** :
    1. VPN is used to connect offices in different geographical locations remotely and is cheaper when compared to WAN connections.

2. VPN is used for secure transactions and confidential data transfer between multiple offices located in different geographical locations.
3. VPN keeps an organization's information secured against any potential threats or intrusions by using virtualization.
4. VPN encrypts the internet traffic and disguises the online identity.

Types of VPN

1. Access VPN:
Access VPN is designed to provide connectivity to remote mobile users and telecommuters. It serves as a cost-effective alternative to traditional dial-up or ISDN connections, offering a broad range of connectivity options.

2. Site-to-Site VPN:
Site-to-Site VPN, also known as Router-to-Router VPN, is commonly employed by large companies with multiple branches in different locations. It enables the connection of one office's network to another office in a separate geographical area. This type of VPN has two sub-categories:

a. Intranet VPN:
Intranet VPN facilitates the connection of remote offices located in different geographical areas through a shared infrastructure, such as internet connectivity and servers. It allows these offices to have the same accessibility policies as a private WAN (wide area network).

b. Extranet VPN:
Extranet VPN utilizes shared infrastructure over an intranet to connect suppliers, customers, partners, and other external entities using dedicated connections. It enables secure communication and collaboration between these external parties and the organization's internal network.

IPv4 Address : An IP address is a 32-bit dynamic address of a node in the network. An IPv4 address has 4 octets of 8-bit each with each number with a value up to 255. IPv4 classes are differentiated based on the number of hosts it supports on the network. There are five types of IPv4 classes and are based on the first octet of IP addresses which are classified as Class A, B, C, D, or E.

IPv4 Class	IPv4 Start Address	IPv4 End Address	Usage
A	0.0.0.0	127.255.255.255	Used for Large Network
B	128.0.0.0	191.255.255.255	Used for Medium Size Network
C	192.0.0.0	223.255.255.255	Used for Local Area Network
D	224.0.0.0	239.255.255.255	Reserved for Multicasting
E	240.0.0.0	255.255.255.254	Study and R&D

OSI (Open Systems Interconnection) Model (Important):

The OSI model is a network architecture model based on ISO (International Organization for Standardization) standards. Its name, Open Systems Interconnection, reflects its purpose of facilitating communication between systems that are open for interaction with other systems. The OSI model is organized into seven layers.

Principles of the OSI Model:

1. Create a New Layer When Needed:
The OSI model follows a modular approach. If a different level of abstraction is required to handle specific tasks, a new layer is added to address those functions independently.

2. Well-Defined Functions for Each Layer:
Each layer of the OSI model has a specific, clearly defined function. These functions are designed to address specific aspects of data communication, ensuring a systematic and organized approach to networking.

3. Use Internationally Standardized Protocols:
The functions of each layer in the OSI model are based on internationally standardized protocols. This ensures that network devices and systems from different manufacturers can interoperate seamlessly.

The OSI model serves as a conceptual framework that aids in understanding the various processes involved in data communication across networks, making it a fundamental tool in network architecture and design.

The OSI model consists of seven layers, each serving a specific purpose in data communication:

1. Physical Layer:

The Physical layer is the lowest layer and deals with the physical transmission of raw bit streams over the network medium. It manages the physical connection between devices, utilizing cables or wireless media like twisted-pair cables or fiber optics.

2. Data Link Layer:

The Data Link layer is responsible for transferring data frames between nodes in the network. It takes data from the Network layer, converts it into data frames, and adds physical addresses to them. The Data Link layer ensures error-free transmission, frame synchronization, and handles flow control.

3. Network Layer:

The Network layer is involved in routing, where it determines the best route for data packets to travel from the source to the destination. It converts logical addresses into physical addresses and performs packetizing to segment data into packets. The Network layer also facilitates internetworking by connecting different networks to form a larger network.

4. Transport Layer:

The Transport layer is responsible for delivering messages through the network and ensures error checking to prevent data errors during transmission. It provides two types of services: connection-oriented transmission, where acknowledgments are sent to confirm successful data delivery, and connectionless transmission, where acknowledgments are not sent.

5. Session Layer:

The Session layer manages the establishment, maintenance, and termination of communication between devices. It reports errors from upper layers and establishes sessions between users for effective communication.

6. Presentation Layer:

The Presentation layer, also called the Translation layer, translates data from one format to another format. It handles character code translation, data conversion, data compression, and data encryption. At the sender's

end, it translates data from the application layer format to a common format, and at the receiver's end, it translates the common format back to the application layer format.

TCP/IP Reference Model:

The TCP/IP reference model is a simplified version of the OSI model, consisting of four layers. It was developed by the US Department of Defense (DoD) in the 1960s. The name is derived from two key protocols used in the model: TCP (Transmission Control Protocol) and IP (Internet Protocol).

1. Link Layer:
The Link layer determines the physical links, such as serial lines or classic Ethernet, to be used to fulfill the requirements of the connectionless internet layer. Protocols like SONET and Ethernet operate at this layer.

2. Internet Layer:
The Internet layer is crucial in holding the entire architecture together. It is responsible for delivering IP packets to their intended destinations. IP (Internet Protocol) and ICMP (Internet Control Message Protocol) are examples of protocols used in the Internet layer.

3. Transport Layer:
The Transport layer serves a function similar to the OSI Transport layer. It enables peer entities on the network to establish and maintain communication. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are examples of protocols operating at this layer.

4. Application Layer:
The Application layer contains higher-level protocols that facilitate user-level communication. Protocols like HTTP, SMTP, RTP, and DNS operate in this layer.

HTTP and HTTPS:

- HTTP (HyperText Transfer Protocol) defines the rules and standards for transmitting information on the World Wide Web (WWW). It facilitates communication between web browsers and web servers. It is a stateless

protocol, where each command is independent of previous commands. HTTP operates at the application layer, built upon TCP, and typically uses port 80 for communication.

- HTTPS (HyperText Transfer Protocol Secure) is a secure and advanced version of HTTP. It uses SSL/TLS protocols on top of HTTP to provide security and encrypt communication. It enables secure transactions and uses port 443 by default.

DNS (Domain Name System) (Important):

DNS is a naming system used to identify resources over the internet, including physical nodes and applications. It translates domain names into their associated IP addresses, making it easier to locate resources on the network. Without DNS, users would have to know the IP address of the websites they want to access. DNS was introduced in 1983 by Paul Mockapetris and Jon Postel.

DNS works by translating human-readable domain names (like "www.shaurya.com") into machine-readable IP addresses (like "192.168.1.1"). DNS forwarders are used when a DNS server receives queries that it cannot resolve quickly; it forwards those requests to external DNS servers for resolution.

SMTP Protocol:

SMTP (Simple Mail Transfer Protocol) is responsible for communication between email servers and setting rules for email transmission over the internet. It supports both End-to-End and Store-and-Forward methods and listens on port 25.

Difference Between TCP and UDP:

- TCP (Transmission Control Protocol) is connection-oriented, while UDP (User Datagram Protocol) is connectionless.
- TCP is comparatively slower than UDP, but it provides extensive error checking mechanisms, flow control, and acknowledgment of data, making it more reliable.

- UDP is faster, simpler, and more efficient, but it lacks error correction mechanisms. It is commonly used in scenarios where real-time data transfer is essential, and occasional data loss is acceptable (e.g., video streaming, online gaming).

Important Protocols:

1. DHCP (Dynamic Host Configuration Protocol):

DHCP is an application layer protocol that enables automatic configuration of devices on IP networks. It assigns IP addresses and other network configurations to devices, allowing them to communicate over the network. DHCP uses port 67 by default.

2. FTP (File Transfer Protocol):

FTP is an application layer protocol used for reliable and efficient file transfer between hosts. It allows users to upload and download files from remote servers. FTP uses port 21 by default.

3. ICMP (Internet Control Message Protocol):

ICMP is a network layer protocol used for error handling and network diagnostics. It is primarily utilized by routers to diagnose network connection issues and report errors. ICMP uses port 7 by default.

4. ARP (Address Resolution Protocol):

ARP is a network-level protocol used to map IP addresses to MAC addresses. It resolves the MAC address of devices on the local network, facilitating communication.

5. RIP (Routing Information Protocol):

RIP is a dynamic protocol used by routers to find the best route from source to destination over a network using the hop count algorithm. Routers exchange network topology information using RIP. It is commonly used in small or medium-sized networks.

MAC Address and IP Address (Important):

MAC Address (Media Access Control) and IP Address both uniquely identify devices on the internet. The MAC Address is assigned by the NIC (Network Interface Card) manufacturer and is used to identify devices on a network at the physical level. On the other hand, IP Addresses are provided by Internet Service Providers (ISPs) and are used to uniquely identify the connection of a device to a network.

Ipconfig and Ifconfig:

- Ipconfig (Internet Protocol Configuration): It is a command used in Microsoft operating systems to view and configure network interfaces.

- Ifconfig (Interface Configuration): It is a command used in MAC, Linux, and UNIX operating systems to view and configure network interfaces.

Firewall:

A firewall is a network security system that monitors incoming and outgoing network traffic and blocks unauthorized or potentially harmful traffic based on predefined security policies. It acts as a barrier between the public internet (external network) and the private network of networking devices, adding an extra layer of security to the network. Firewalls can be implemented as hardware devices, software programs, or a combination of both. They play a critical role in safeguarding networks from potential threats and attacks.

Important Key Points

Important Key Points:

1. **What happens when you enter google.com in the web browser? (Most Imp)**
   - The browser checks the cache for the content and displays it if available.
   - If not in cache, it checks the IP of the URL in the cache and OS.
   - If not in cache, the browser requests the OS to perform a DNS lookup to get the IP address from the DNS server using UDP.
   - A new TCP connection is established between the browser and server.
   - An HTTP request is sent to the server via the TCP connection.

- The web server handles the request and sends an HTTP response.
- The browser processes the response, renders the content, and may close or reuse the TCP connection.
- Cacheable responses are stored in the browser's cache.

2. Hub vs. Switch:

- Hub transmits the signal to all ports (except the one it received from), while a switch establishes connections based on need.
- Hub operates at the Physical layer, while a switch operates at the Data Link layer.
- Hub lacks packet filtering, whereas a switch provides packet filtering, making it more efficient.

3. Subnet:

- A subnet is a network within a network achieved through subnetting.
- It enhances routing efficiency and network security.
- Subnetting reduces the time to extract the host address from the routing table.

4. Reliability of a network is measured by downtime, failure frequency, and handling unexpected events like catastrophes.

5. Factors making a network effective and efficient:

- Performance (transmit time, response time)
- Reliability (frequency of failure)
- Robustness (strong and in good condition)
- Security (protecting data from unauthorized access and viruses)

6. Node and Link:

- A network consists of two or more computers (nodes) connected by physical mediums (links).

7. Gateway and Router:

- A gateway is a node connected to two or more networks, used for forwarding messages between networks.
- Router and gateway are often used interchangeably, but a router typically connects similar networks, while a gateway connects dissimilar networks.

8. NIC (Network Interface Card):

- NIC is a peripheral card attached to a PC to connect to a network.
- It has a unique MAC address that identifies the PC on the network.

9. POP3 (Post Office Protocol version 3):

- POP3 is responsible for accessing mail services on a client machine.
- It works in Delete mode and Keep mode.

10. Private and Public IP Address:

- Private IP addresses are reserved for local networks and not valid for the internet.
- Public IP addresses are assigned by ISPs and facilitate communication on the internet.

11. RAID (Redundant Array of Inexpensive/Independent Disks):

- RAID is a method to provide fault tolerance using multiple hard disk drives.

12. Netstat:

- Netstat is a command-line utility that provides information about current TCP/IP settings of a connection.

13. Ping:

- Ping is a utility program that checks connectivity between network devices using IP address or name.

14. Peer-peer processes:

- Processes on each machine that communicate at a given layer are called peer-peer processes (P2P).

15. Unicasting, Anycasting, Multicasting, and Broadcasting:

- Unicasting: Sending a message to a single node.
- Anycasting: Sending a message to any of the nodes.
- Multicasting: Sending a message to a subset of nodes.
- Broadcasting: Sending a message to all nodes in a network