Definition of Networking

Networking refers to the practice of connecting computers and other devices (like phones, printers, etc.) so they can **communicate and share resources** (data, files, internet, etc.).

Basic Components of a Network

1. **Devices:**
    - **Hosts**: Computers, smartphones, servers (end-users)
    - **Networking Devices**: Routers, switches, hubs, modems, firewalls
2. **Media (Transmission Medium):**
    - **Wired**: Ethernet cables (e.g., Cat5, Cat6)
    - **Wireless**: Wi-Fi, Bluetooth, cellular signals
3. **Protocols:**
    - Rules that define how data is transmitted. Examples:
        - **TCP/IP** (foundation of the internet)
        - **HTTP/HTTPS** (web browsing)
        - **FTP** (file transfer)
        - **DNS** (domain name resolution)

Types of Networks

1. **LAN (Local Area Network):**
    - Small geographic area (e.g., home, office)
    - Fast and relatively inexpensive
2. **WAN (Wide Area Network):**
    - Covers large areas (e.g., the internet)
    - Uses leased telecommunication lines
3. **MAN (Metropolitan Area Network):**

    - Covers a city or large campus
4. **PAN (Personal Area Network):**
    - Short-range (e.g., Bluetooth between phone and headphones)

🔀 Network Topologies

Describes the layout of a network:

- **Bus**: All devices connected to a single backbone
- **Star**: Devices connect to a central switch or hub
- **Ring**: Each device connects to two others, forming a loop
- **Mesh**: Devices are interconnected (used in large, fault-tolerant networks)

📦 Data Transmission & the OSI Model

The **OSI Model** explains how data moves through a network in **7 layers**:

1. **Physical** – Hardware (cables, connectors)
2. **Data Link** – MAC addressing, switches
3. **Network** – IP addressing, routers
4. **Transport** – Reliable data transfer (TCP/UDP)
5. **Session** – Manages connections between devices
6. **Presentation** – Data formatting, encryption
7. **Application** – Interfaces for the user (e.g., browsers)

🌍 IP Addressing & DNS

- **IP Address**: Unique identifier for devices on a network (e.g., 192.168.1.1)
- **DNS (Domain Name System)**: Converts human-friendly names (google.com) to IP addresses

🔐 Basic Network Security Concepts

- **Firewalls**: Control incoming/outgoing traffic

- **Encryption**: Protects data during transmission
- **Authentication**: Ensures only authorized users access the network (e.g., passwords, biometrics)
- **VPNs**: Create secure tunnels over public networks

📡 Internet and the Role of ISPs

- **Internet**: A global network of networks
- **ISP (Internet Service Provider)**: Gives users access to the internet
- **Identify key components of a network**

the **key components of a network**, grouped by their function:

💻 1. End Devices (Clients and Servers)

- **Clients**: Devices that request data (e.g., computers, smartphones, tablets)
- **Servers**: Devices that provide resources or services (e.g., web server, file server)

📡 2. Networking Devices

- **Router**:
    - Connects different networks (like your home network to the internet)
    - Routes data using IP addresses
- **Switch**:
    - Connects multiple devices within a local area network (LAN)
    - Uses MAC addresses to forward data to the correct device
- **Hub**:
    - Basic device that connects multiple devices in a LAN
    - Broadcasts data to all connected devices (less efficient than a switch)
- **Modem**:

    - Modulates and demodulates signals to connect to the internet (via ISP)
    - Often combined with a router in home networks
- **Access Point (AP)**:
    - Provides wireless access to a wired network (Wi-Fi)
    - Used in larger networks or to extend Wi-Fi range
- **Firewall**:
    - Filters traffic to protect the network from unauthorized access

🔗 3. Transmission Media

- **Wired**:
    - Ethernet cables (Cat5, Cat6, etc.)
    - Coaxial cables
    - Fiber optic cables
- **Wireless**:
    - Radio waves (Wi-Fi, cellular, Bluetooth)
    - Infrared (used in some remote controls)

🌐 4. Network Protocols

- **TCP/IP**: Core protocol suite for communication over the internet
- **HTTP/HTTPS**: Used for web communication
- **FTP/SFTP**: File transfers
- **DNS**: Resolves domain names to IP addresses
- **DHCP**: Automatically assigns IP addresses

🧠 5. Network Software

- **Operating Systems**: Windows, Linux, macOS (with networking support)

- **Network Management Tools**: Monitor, troubleshoot, and manage the network
- **Security Software**: Antivirus, intrusion detection systems (IDS), etc.

🧭 6. IP Addressing & Naming Services

- **IP Address**: Unique address assigned to each device
- **MAC Address**: Physical hardware address of a device
- **DNS Server**: Resolves human-friendly names (like example.com) to IP addresses
- **DHCP Server**: Assigns dynamic IP addresses to devices on the network

- **Describe the purpose of networking in distributed systems**

The purpose of **networking in distributed systems** is to **enable communication and coordination** between multiple independent computers (nodes) that work together to perform a task as if they were a single system.

🌐 Key Purposes of Networking in Distributed Systems

1. **Resource Sharing**

· **Goal**: Allow multiple nodes to share hardware (e.g., printers), software, and data.

· **Example**: A distributed database system where data is stored across multiple machines but accessed as one unified database.

2. **Communication**

· **Goal**: Facilitate message exchange between nodes.

· **Protocols**: Use TCP/IP, HTTP, gRPC, or custom protocols to transmit data reliably.

· **Example**: Microservices architecture where services communicate over the network using REST APIs.

3. **Coordination & Synchronization**

- **Goal**: Ensure consistency, ordering, and timing of operations across different nodes.
- **Mechanisms**: Clock synchronization (NTP), consensus algorithms (e.g., Raft, Paxos)
- **Example**: Distributed locking to prevent conflicts when multiple nodes access shared data.

4. **Fault Tolerance**

- **Goal**: Detect and recover from node or network failures.
- **How Networking Helps**: Heartbeat signals, health checks, replication updates
- **Example**: In a cluster, if one server goes down, another can take over, and updates are replicated across nodes.

5. **Scalability**

- **Goal**: Support growth in system size and workload.
- **How Networking Helps**: By adding more machines (horizontal scaling), each connected over a network, the system can handle more requests or data.

---

6. **Transparency**

Networking allows distributed systems to appear as a single, unified system to users by providing:

- **Location transparency** (users don't need to know where a resource is)
- **Access transparency** (accessing remote resources like local ones)
- **Failure transparency** (handling failures without user disruption)

✅ **Summary**

Networking in distributed systems is essential for:

- Connecting nodes
- Sharing resources

- Exchanging messages
- Coordinating actions
- Ensuring reliability
- Scaling the system

Without networking, a distributed system would just be isolated machines, unable to function as a cohesive whole.

1.2 Types of networks are illustrated

What Is a Computer Network?

A computer network is a connection between two or more network devices, like computers, routers, and switches, to share network resources.

The establishment of a computer network depends on the requirements of the communication channel, i.e., the network can be wired or wireless.

1. Local Area Network (LAN) - A network that connects devices within a limited area such as a home, office, or school.

2. Wide Area Network (WAN) - A network that covers a large geographical area and connects multiple LANs together, often using public or private telecommunications lines.

3. Metropolitan Area Network (MAN) - A network that covers a city or metropolitan area, connecting multiple LANs and WANs together.

4. Wireless Local Area Network (WLAN) - A type of LAN that uses wireless technology, such as Wi-Fi, to connect devices without the need for physical cables.

5. Virtual Private Network (VPN) - A network that creates a secure connection over the internet, allowing users to access resources on a private network from a remote location.

6. Intranet - A private network that is only accessible to users within a specific organization, often used for sharing resources and information within the organization.

7. Extranet - A network that allows external users, such as partners or customers, limited access to a company's internal network for specific purposes.

8. Peer-to-Peer Network - A network in which all devices have equal status and can communicate directly with one another without the need for a central server.

9. Client-Server Network - A network in which one or more central servers provide resources and services to client devices, such as accessing files, printers, or databases.

10. Internet - A global network of networks that allows devices all over the world to communicate and access information and services.

Types of Networks

According to the communication requirements, multiple types of network connections are available. The most basic type of network classification depends on the network's geographical coverage.

Below mentioned are different types of networks:

- PAN (Personal Area Network)
- LAN (Local Area Network)
- MAN (Metropolitan Area Network)

· WAN (Wide Area Network)

Let’s look into each of the network types in detail.

What Is Local Area Network (LAN)?

The Local Area Network (LAN) is designed to connect multiple network devices and systems within a limited geographical distance. The devices are connected using multiple protocols for properly and efficiently exchanging data and services.

Attributes of LAN Network:

· The data transmit speed in the LAN network is relatively higher than the other network types, MAN and WAN.

· LAN uses private network addresses for network connectivity for data and service exchange, and it uses cable for network connection, decreasing error and maintaining data security.

Advantages and Disadvantages of LAN Network

Advantages	Disadvantages
Transmission of data and services is relatively higher than other network connections.	Need constant administration of experienced engineers for functioning.
The Network Server acts as a central unit for the whole network.	Probability of leak of sensitive data by LAN administration.

Now let’s move on to the next network type, MAN Network.

What Is Metropolitan Area Network (MAN)?

The Metropolitan Area Network (MAN) is a network type that covers the network connection of an entire city or connection of a small area. The area covered by the network is connected using a wired network, like data cables.

Attributes of MAN Network:

· Network covers an entire town area or a portion of a city.

· Data transmission speed is relatively high due to the installation of optical cables and wired connections.

Advantages and Disadvantages of MAN Network:

Advantages	Disadvantages
Provides Full-Duplex data transmission in the network channel for devices.	High probability of attack from hackers and cybercriminals due to large networks.
The network connection area covers an entire city or some parts using the optic cables.	The need for good quality hardware and the installation cost is very high.

What Is Wide Area Network (WAN)?

The Wide Area Network (WAN) is designed to connect devices over large distances like states or between countries. The connection is wireless in most cases and uses radio towers for communication.

The WAN network can be made up of multiple LAN and MAN networks.

Attributes of WAN Network:

· The speed of the WAN data transfer is lower than in comparison to LAN and MAN networks due to the large distance covered.

· The WAN network uses a satellite medium to transmit data between multiple locations and network towers.

Advantages and Disadvantages of WAN Network:

Advantages	Disadvantages
This network covers a high geographical area and is used for large-distance connections.	High cost to set up the network and the Support of experienced technicians is needed to maintain the network.
They also use radio towers and connect channels for users.	It is difficult to prevent hacking and debug a large network.

Difference Between LAN, MAN, and WAN

Basis	**LAN**	**MAN**	**WAN**
Meaning	LAN is a network that enables the communication between many linked	Several computers can be connected to MAN in the	The WAN network extends to a much

	devices. It is in charge of establishing connections among neighborhood units, including universities and schools.	same city or separately. It encompasses a greater region, including minor towns and cities.	greater area. It can link multiple countries together.
Network Authority	LAN is a private and secured network. Hospitals, schools, offices, etc., can own it.	MAN can be either public or private. A lot of businesses and telephone companies could own them.	A single company may not own WAN. It can be private or public.
Speed	The Internet speed provided through LAN is fast.	MAN provides a modest Internet connection speed.	WAN provides a slow Internet connection.
Maintenance	LAN maintenance is very easy.	MAN's maintenance is easier compared to LAN.	WAN maintenance is very difficult.
Congestion	Congestion is less in the LAN network.	It is more in MAN.	Congestion is more in WAN when compared to LAN and MAN.
Bandwidth	The bandwidth in LAN is very high.	In MAN, bandwidth is less.	WAN bandwidth is quite limited.
Designing	It is very easy to design a LAN network.	It isn't easy to design a MAN network.	It is complicated to design WAN.

How to Set Up The Networks?

LAN

Ethernet is the foundation of all existing LANs, whether wired or wireless. Computers and servers can connect via cables or wirelessly. WiFi Access Points provide wireless connectivity in combination with a wired network. WAP-enabled devices serve as a link between PCs and networks. A WAP may connect a hundred or even a thousand wireless individuals to a network. Servers on a LAN are generally connected by wire.

MAN

A metropolitan area network combines many LANs with a fiber optic as the basis. It offers services akin to those offered by an internet service provider for broad area networks. MANs can use microwave or infrared lasers to connect Local Area Networks wirelessly. MANs are often

owned by just one significant organization and are mainly created for towns or cities to give a high data connection.

WAN

Users and computers in one area may interact with users and computers in other locations via a WAN, composed of two or more interconnected Local Area Networks or Metropolitan Area Networks. Computers in a Wide Area Network are linked by public networks such as phone lines, satellite connections, or leased lines. To extend the network's capabilities across locations, costly leased lines are usually used to build WANs. At each end of a leased line, a router is attached.

How Do These Networks Function?

LAN

A local area network is a collection of computers and other technology with a common communication line or wireless network and, in most cases, the facilities of an individual server or processor within a limited geographic region. Typically, the server houses shared data storage and applications for many computer users.

MAN

Multiple LANs are connected by metropolitan area networks using specialized wireless and wired foundations. A MAN may link to a network exchange point and a local exchange carrier to offer connections between LANs and instantaneous communication between the MAN and the open Internet.

WAN

A point to another service that can employ traditional dial-up lines or modems to link the device to the phone line. Point-to-point WAN service suppliers include both local mobile phone providers and long-distance operators.

Characteristics of These Networks

LAN

- LANs are simple to construct and maintain.
- To link the LAN networks, a centralized database is needed.
- A private owner owns the network.

MAN

· The geographical region covered exceeds that of LAN.

· Through this network, there is more than one computer connected.

WAN

· WAN covers the biggest region, comparable to a nation.

· WANs can be networked all over the world.

· Through phone lines or satellites, the networks are connected.

Benefits of These Networks

LAN

· Its main advantages are the local area network's rapid, simple setup and low cost.

· Keeping everything stored on the server safe and secure is done through data protection.

· LAN model and established ethernet cabling allow a system linked to a LAN to interact directly at a very high speed.

MAN

· MAN offers more security than WAN and is simpler to deploy.

· Due to MAN's lower resource requirements than WAN, MAN deployment costs are lower than WAN. It reduces the cost of implementation.

· MANs may be controlled centrally, making network traffic monitoring and control easier.

WAN

· WAN has a wide geographical coverage.

· The information connected to every device in the relevant network can be shared through the WAN network.

Disadvantages of the Networks

LAN

· Local area networks are only utilized in structures since they cannot be used in larger regions.

· Unauthorized users may access data if the server's equipment is not appropriately configured and there is a technology issue.

· There are restrictions on how many devices may be connected to LANs.

MAN

· Because of the huge size, it is difficult to safeguard the system from hackers.

· To link MAN from one location to another, extra cables are necessary. MAN necessitates the use of fiber optic connections, which are relatively costly.

· MAN takes up a lot of space, making managing a big network difficult.

WAN

· Because WAN networks combine more technologies, they have more security issues when compared to LAN and MAN networks.

· Because of their enormous geographical coverage, WANs are complex and convoluted.

· A lot of time must be spent troubleshooting the WAN network.

Wireless Local Area Network (WLAN)

WLAN or a wireless local area network functions like LAN as it transfers data in a small area. It is hardly compulsory for devices to have a wired connection that uses WLAN, and even though it is slightly weaker and less secure than other networks, a wireless local area network offers users the flexibility to use their devices in multiple locations. It is worth mentioning WLAN security can be strong if proper encryption methods like WPA3 are used.

How to Set Up?

Follow the steps mentioned below to set up a WLAN:

· Get a WLAN router.

· Visit the configuration page of your WLAN router.

· Open the browser and enter the web address.

· Now mention the provided username and password. These credentials come along with your router's documentation.

· Enter the information of your internet connection, including IP address and DNS, from your internet provider.

· Open the wireless settings section to change the network name or password, enable or disable the wireless connection and set the encryption.

· Ensure to click on save changes in your router's settings.

· Locate your WLAN router in a place like the central location that offers the best possible signal. Remember that obstacles such as doors or walls will disrupt your network.

· Once a wireless network gets broadcasted by a router, connect the network to any device, like a laptop, mobile phone or tablet, by mentioning the password, and your WLAN network is ready to use.

How Does a Wireless Local Area Network (WLAN) Function?

In the wireless local area, is the type of network that transfers data through radio signals, and the data is forwarded in the form of a packet. Each packet includes labels, instructions, and layers, with a specific MAC address appointed for each endpoint. This helps routing data packets to appropriate locations.

It has a very high data switch rate and uses a star topology, where each node is connected to a central point. Moreover, an access point connects to the internet by promoting the transmission of frequency signals to the connected stations.

Characteristics

Some key characteristics of WLAN are listed below:

· A wireless local area network is used to connect and interact with gadgets to the internet without using directed mediums, such as fiber or cables.

· WLAN offers versatility by letting wireless devices connect and disconnect, avoiding physical wiring.

· WLAN uses wireless connectivity to forward transmission, generating a more adaptable and dynamic network environment.

· It uses radio waves to transfer records among devices, making it a flexible and useful alternative in multiple situations.

Advantages and Disadvantages

WLAN offers numerous advantages. Some of them are:

· It is a reliable communication as it depends on reliable protocols.

· WLAN setup is a clean and brief network, followed by a wireless setup, as it does not include any physical connections and is easier to install.

· This network is advantageous for transforming physical layouts in dynamic workspaces. Businesses transferring and transforming offices do not affect network connectivity for longer

periods as the setup doesn't include heavy cable connections and can be reconnected quickly to new places.

WLAN network also comes with certain drawbacks, including:

· Security issues regarding wireless local area networks are the major drawbacks. These networks can be easily attacked by hackers, resulting in the loss of crucial records, and information might be misused.

· If multiple WLAN devices come with equal frequencies, together with cordless telephones or microwaves, there are chances of inflicting interference in this network. Hence, due to this network, the relationship might fail, resulting in connectivity issues.

· Reliability problems might also occur in WLAN. The connection might turn much less steady in case of rain, excessive boundaries or other barriers between the device and the community router.

Campus Area Network (CAN)

The campus area network is utilized in most educational environments, such as schools or universities. Even though every school department might use WLAN, all the WLANs across the school can be connected through a CAN. Campus area networks include multiple independent networks in one unit. For instance, the Engineering and English departments can connect via a campus area network to directly communicate with one another.

How to Set Up?

CAN is a single network of multiple interconnected LANs that are connected via switches and routers. In CAN, nodes are connected via optical fiber media and take advantage of 10 Gigabit ethernet technology and wifi hotspots to access the network.

How Does Campus Area Network (CAN) Function?

A campus area network is created using access points and switches to link the devices and let them communicate with one another. In a CAN, devices get connected via wireless and wired technologies, such as Wi-Fi and ethernet. The wire connections are faster and highly reliable, which is why the wireless connections provide amazing mobility and flexibility. The IT team monitors the network traffic, troubleshoots issues, and configures the network settings.

Characteristics

· CAN is a computer network usually located in places like big organizations or schools and colleges.

· It covers only specific geographical areas.

· CAN uses ethernet technology in a range of 1 to 5 km.

· It comes with a very high transmission speed and a moderate cost.

Advantages and Disadvantages

Some benefits of the CAN are:

· CANs offer reliable and fast connectivity for devices connected to the network.

· As compared to WAN, CAN is less expensive to set up and maintain.

· They can be scaled down or up easily when needed, making it a flexible option according to the fluctuating network requirements.

Drawbacks that are associated with the CAN include:

· CAN is created to cover only small geographical areas and is not suitable for widely spread organizations.

· They depend on physical infrastructure, such as access points, cables, or Wi-Fi, to connect devices. When any disruption occurs in the infrastructure, it affects the connectivity and performance of the CAN.

· The cost associated with setting up and maintaining CAN is higher for organizations with limited budgets.

Storage Area Network (SAN)

It is a type of network that teams to store huge amounts of crucial data. It offers users a process to centralize data on non-localized networks that are different from the major operating ones.

How to Set Up?

To set up the storage area network, you must follow the guidelines listed below:

· Assemble cable and other hardware components and install the software.

· Change the configuration settings according to the requirements.

· Test integrations, including the operational procedures for the SAN environment, along with failure mode, testing and backup, and normal production processing.

· Create a performance baseline for each component and the entire SAN.

· Document the SAN operational procedures and installation.

How Does the Storage Area Network (SAN) Function?

The storage area network aims to grab storage from an individual server and transport the storage where storage resources are centrally handled and protected. This centralization is performed by locating it into a storage subsystem. However, centralization can also be handled through software, which depends on virtualization to aggregate and manage the available storage.

In SAN, storage traffic performance is accelerated and optimized as the storage traffic doesn't need to compete with the LAN required by servers and workloads. Hence, enterprise workloads can receive faster access to use volumes of storage. SAN is perceived as having three different layers, including a storage layer, a fabric layer, and a host layer.

Characteristics

Key characteristics of SAN include:

· SAN is used to transfer data between the storage device and the server. It also promotes data transfer between storage systems.

· SAN is mainly utilized to access storage devices, such as disk-based devices and tape libraries, from the servers.

· It is a network which is not accessible via LAN. It includes switches, hosts, and storage devices that are interconnected through protocols, topologies, and technologies.

Advantages and Disadvantages

The major advantages of SAN are as follows:

· SAN supports large deployment, including thousands of storage devices and SAN hosts, servers or storage systems. New storage and hosts are also added to build the SAN to align with the specific requirements of the organization.

· A completely featured SAN deployment does not include any point of failure between a storage device and a host, and communications through the fiber always fetch an alternative path for storage availability to the workload.

· SAN supports multiple useful storage features, such as data deduplication, data encryption, storage replication and self-healing technologies to maximize the storage capacity, data resilience and security.

Despite the multiple benefits, SANs come with certain limitations; they are:

· SAN is effective only in complex and larger environments where there are multiple servers and enough storage. Moreover, the complexity and cost of SAN is hard to justify.

· SAN management is a significant challenge as configuring features is problematic for busy organizations.

· Setting up self-healing technologies and RAID is very time-consuming and cannot be avoided to maintain compliance with the organization.

Passive Optical Local Area Network (POLAN)

A passive optical local area network is a low-cost network linking multiple locations to a specific central network. It has the power to connect different entities to one information hub.

How to Set Up?

The passive optical local area network depends on single-mode fiber optic cables with few copper cables at the endpoints. It is created with multiple levels or layers of routers, ethernet cables, and active switches. The devices and core layer connect to distribution layer switches, which get linked to access layer switches in closets of communication. From these closets, copper cables run to the users' computers.

How Does a Passive Optical Local Area Network (POLAN) Function?

A passive optical network is a type of network that uses fiber or technology to transmit data from one source to several endpoints. This network is a point-to-multipoint indoor network structure, using optical splitters to allocate data from one source to multiple user endpoints. It also implements Wavelength Division Multiplexing technology to allow downstream and bi-directional upstream communication.

Characteristics

· A passive optical network uses fiber optic technology to distribute data from one source to many endpoints.

· The word ‘passive’ represents the usage of optical fiber cables that are linked to an unpowered splitter that forwards straighter from the service provider's network to different customers.

Advantages and Disadvantages

Some benefits of POLAN are as follows:

· In comparison with traditional LAN, POLAN minimizes the number of devices and cables required in a network. These are smaller, less susceptible to interference, and have lighter cables, allowing POLANs to cover long distances and offer enhanced space.

· POLAN centralizes management and intelligence and allows the delivery of all services through one infrastructure, reducing the requirement for several platforms.

Disadvantages of POLAN include:

· In passive optical local area networks, short-term adoption is complex because of substantial investment in present copper networks.

· Passive optical local area networks are not cost-effective network infrastructure for small organizations as they fail to utilize the entire capacity of this network.

Enterprise Private Network (EPN)

EPN, or Enterprise Private Network is an exclusive type of network created and operated by businesses to share company resources at rapid speeds. These are unique networks to a certain company, ensuring the security of the connection.

How to Set Up?

Setting up an EPN network includes installing switches, dedicated lines, security systems, routers, and potentially integrating cloud services.

How Does Enterprise Private Network (EPN) Function?

EPN includes connecting multiple components and devices within a specific organization, including branch offices, data centers and cloud services to promote business processes, data exchange, and network activity analysis. EPN starts with a local area network, connecting devices in a specific facility or location. Later, these local area networks are connected through wide area networks, enabling data transmission over longer distances. Hence, EPN is a complicated process that includes the connection of multiple components within a single organization to promote efficiency, data exchange, and other network activities, ensuring the reliability and security of the company's data.

Characteristics

· EPN is a private network and not open to the public.

· It is created to keep the communication and data of a company secure and confidential.

· It is a highly scalable network and hence accommodates the rising needs of an organization as it grows.

· These networks restrict connectivity to certain devices, users, and facilities. Moreover, they encrypt the data passing over them through virtual private networks or transport layer security encryption.

Advantages and Disadvantages

EPN offers the following advantages:

· EPN provides enhanced security to organizations from outside threats and data leakage. With advanced trade detection technologies, companies can protect their crucial data and prevent unauthorized access.

· Network optimization in EPN improves the enterprise network performance. A well-structured EPN promotes smooth data transfer, leading to better user satisfaction and increased productivity.

· With a well-crafted EPN, companies handle changing technologies and growth effectively.

Drawbacks of EPN include the following:

· EPN requires enough maintenance and set-up cost

· Organizations require IT experts to manage the EPN network

· EPN comes with the complexity of making sure every location is connected effectively.

Virtual Private Network (VPN)

A VPN is a kind of computer network, extending a private network across the Internet, and permitting the user to send and receive data like they were connected to a certain private network, even though they aren't. By using a virtual point-to-point connection, users access a private network. It protects users from malicious threats by existing as a medium, giving you a protected network connection.

How to Set Up?

To set up a VPN connection:

· Download a VPN app from the Internet.

· Then open settings, click on network and select VPN.

· Click on Add a VPN and mention the files for VPN type and server name, along with the account information provided to you by the VPN provider.

How Does Virtual Private Network (VPN) Function?

A VPN creates a digital connection between the remote server provided by a VPN provider and the computer, generating a point-to-point tunnel encrypting your data, masking your IP address, and allowing you to sidestep websites and firewalls on the Internet.

Characteristics

· A virtual private network routes traffic via a remote server and encrypts it in the process.

· When a VPN is connected to your network, it redirects the traffic of your Internet through a remote server before forwarding it to your destination.

· VPN secures your data from malicious attackers, helps you protect your Internet traffic, and reduces your online footprint.

Advantages and Disadvantages

Using VPN offers multiple benefits:

· Businesses get to secure their network through VPN. By using a VPN, your network is protected from software, people, and web browsers from getting access to your connection.

· VPN lets you hide your private crucial information from hackers. Hence, with a VPN, you access high-level security, making all your online communications appear like garbled characters and text to hackers willing to access your data.

VPN has certain drawbacks. They are:

· A VPN encounters an encryption process to secure your data, which takes excess time and can affect your online experience and reduce the Internet speed.

· With little exposure to networking terminology, it can be challenging to understand and configure a VPN without a VPN provider.

System-Area Network (SAN)

A system area network is a local network that offers connections in groups. Multiple devices are connected to a system area network and operate in a single system. These are newly developed networks operating at higher speeds.

How to Set Up?

You can set up a system area network by assembling the cable and other components and installing the software. Now, set up the configurations according to your requirements and test integrations. After creating a performance baseline for the system area network and completing its installation, your network is ready to use.

How Does System-area Network (SAN) Function?

A system area network backs up data safely and keeps the data separate from the major server. However, the server acts as a transmission line, connecting the data stored on the system area network with the user on the other end.

Characteristics

· The System Area Network is a separate network focusing on storing backups of shared data and resources.

· It lets the registered users gain complete liberty of accessing the backup files.

· This kind of network is preferred among organizations due to its ability to store data and resources with extreme security and end-to-end encryption.

Advantages and Disadvantages

The advantages of system media networks are as follows:

· Data is not stored on the major network server, which is of great benefit as the user receives additional storage which can be utilized for other requirements.

· SAN is capable of backing up data, especially over the system area network's storing channels, which prevents resources from getting jam-packed within the LAN.

SAN comes with certain drawbacks, such as:

· Firstly, system area networks are very costly and come with additional costs of continuous management and maintenance.

· Functioning system media networks are very complex and can only be maintained and managed by specialists.

Conclusion

In this article on 'Types of Networks,' we looked into the types of computer networks. Also, we learned some information about the features of each network, along with the advantages and disadvantages of the networks.

To further gain information on the topic of computer networks and apply them practically to design communication channels, you can refer to Simplilearn's Advanced Executive Program in Cyber Security. With the completion of this professional course, you'll be proficient with terms related to computer networks. Additionally, consider exploring cyber security certifications online and participating in a CISSP®- Certified Information Systems Security Professional to deepen your understanding and practical skills in the cybersecurity domain.

If you have any questions about this article on ‘Types of Networks.’ Feel free to mention them in the comment section at the bottom of this page. Our expert team will help you solve your queries at the earliest.

FAQs

1. What is the importance of a LAN?

Allow sharing of resources, including printers, applications, and other shared services. Permit many computers on a LAN to utilize a single internet connection.

2. What is the importance of a WAN?

Through a WAN provider, WANs can make it easier for devices worldwide to communicate, share information, and do much more.

3. What is the function of LAN cable in networking?

The LAN cable allows several devices to communicate with one another.

Network Topologies	By the end of the session the trainee should be able to: 1. Illustrate common network topologies (star, ring, bus, mesh) 2. Discuss advantages and disadvantages of each topology 3. Determine appropriate topologies for different network needs

Network Topologies

1. Illustrate common network topologies (star, ring, bus, mesh)

Geometric representation of how the computers are connected to each other is known as topology. There are eight types of topology – Mesh, Star, Bus, Ring, Hybrid, Tree, P2P and Daisy chain.

Types of Topology

There are mainly eight types of topology in computer networks:

1. Mesh Topology
2. Star Topology
3. Bus Topology
4. Ring Topology
5. Hybrid Topology
6. Tree Topology
7. P2P Topology
8. Daisy Chain Topology

Mesh Topology

In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated it means that the link only carries data for the two connected devices only. Lets say we have n devices in the network then each device must be connected with (n-1) devices of the network. Number of links in a mesh topology of n devices would be n(n-1)/2.

There are two types of Mesh topology:

1. **Full Mesh Topology:** In this topology each device is connected to all the devices available on the network.

2. **Partial Mesh Topology:** In partial mesh topology, each device is connected to only those devices, to which they communicate frequently. This reduces redundant links and saves the setup cost.

Advantages of Mesh topology

1. **No data loss:** No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.
2. **Reliable:** Mesh topology is reliable and robust as failure of one link doesn't affect other links and the communication between other devices on the network.

3. **Secure:** Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.
4. **Easy to troubleshoot:** Fault detection is easy as there is a separate connection between each devices.
5. **Fast communication:** As there is a dedication connection between two devices on a network, the communication is fast.

Disadvantages of Mesh topology

1. Amount of wires required to connected each system is tedious and headache.
2. Since each device needs to be connected with other devices, number of I/O ports required must be huge.
3. Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link.

Star Topology

In star topology each device in the network is connected to a central device called **hub**. Unlike Mesh topology, star topology doesn't allow direct communication between devices, a device must have to communicate through hub.

If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.

The **central device is known as hub** and **other devices connected to hub are called clients**. Generally Coaxial cable or RJ-45 cables are used to connect the clients to the hub.

Advantages of Star topology

· **Less expensive:** Less expensive because each device only need one I/O port and needs to be connected with hub with one link.

· **Easier to install**

· **Cost effective:** Less amount of cables required because each device needs to be connected with the hub only.

· **Robust:** If one link fails, other links will work just fine.

· **Easy to troubleshoot:** Easy fault detection because the link can be easily identified.

· **Reliable:** Each device is separately connected to the hub, so a connection failure between a device and hub doesn't affect the connection of the other devices.

Disadvantages of Star topology

· If hub goes down everything goes down, none of the devices can work without hub.

· Hub requires more resources and regular maintenance because it is the central system of star topology.

· **Not Scalable:** There is a limit to add new devices as each device increase the load on the central unit (hub or switch). This is why it is not suitable for the large networks.

Bus Topology

In bus topology there is a main cable and all the devices are connected to this main cable through drop lines. There is a device called tap that connects the drop line to the main cable. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

· The main cable that is connected to the devices on the network using drop line is called **backbone cable**.

· The main cable **broadcast the message** to all the devices connected to it.

· When a device wants to sends a message, it **transmits the message to the backbone cable**. All the other devices connected to the backbone cable receives the message whether they are intended to receive the message or not.

· The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access). This method is used to prevent the collision of data as two or more devices can send the data to main cable at the same time.

CSMA: This method is developed to decrease the chance of collisions when two or more devices starts sending the signal at the same time.

CSMA CD (Carrier Sense Multiple Access with Collision Detection): In this method, a device monitors the transmission medium after it sends the data to see if the transmission was successful. If successful, the device marks the communication successful else it sends the data again.

CSMA CA (Carrier Sense Multiple Access with Collision Avoidance): This method tries to

prevent the collision from happening. In this method, before sending the data, the device checks the transmission medium to see if it is busy or not. If busy, then the sender device waits until the transmission medium becomes idle.

Advantages of bus topology

- **Easy installation**, each cable needs to be connected with backbone cable.
- **Less Expensive: Less cables** are required than Mesh and star topology
- **Limited failure:** The connection failure of one device doesn't affect the connections of other devices on network.

Disadvantages of bus topology

- Difficultly in fault detection.
- **Not scalable** as there is a limit of how many nodes you can connect with backbone cable.
- **Difficult to troubleshoot:** It is difficult to identify the cause of failure.
- **Data collision:** When two or more devices send the data simultaneously then there is a chance of data collision. However this can be solved by implementing CSMA techniques that we discussed above.

Ring Topology

In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it. This structure forms a ring thus it is known as **ring topology**.

If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

· Data flow is **unidirectional** in ring topology.

· This topology doesn't have any end points as nodes are connected in circular fashion.

· The data transfers in ring topology in clockwise direction.

· The popular access method used in ring topology is **token passing method.** The word token describes segment of data send through the network. There are multiple tokens available on the network, the device that successfully acquires the token attaches the data to the token. The device that successfully decodes the token, receives the data.

Advantages of Ring Topology

· Easy to install.

· Managing is easier as to add or remove a device from the topology only two links are required to be changed.

· **Less expensive:** Generally Twisted pair cabling is used in ring topology which is inexpensive and easily available.

· **Easy maintenance:** The network in ring topology is easy to maintain as a system failure doesn't affect other systems on network, the failed system can be easily removed and installed again after fixing the issue.

Disadvantages of Ring Topology

· A link failure can fail the entire network as the signal will not travel forward due to failure.

· Data traffic issues, since all the data is circulating in a ring.

Hybrid topology

A combination of two or more topology is known as hybrid topology. For example a combination of star and bus topology is known as star bus hybrid topology, this topology is shown in the above diagram.

Advantages of Hybrid topology

· We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.

· Scalable as we can further connect other computer networks with the existing networks with different topologies.

Disadvantages of Hybrid topology

· Fault detection is difficult.

· Installation is difficult.

· Design is complex so maintenance is high thus expensive.

Tree topology

· Tree topology is an **example of hybrid topology** as it is a combination of **star topology** and **bus topology** that forms a tree like structure.

· The devices are connected to each other in hierarchical manner. Each node has arbitrary number of child nodes. The device at the top of the hierarchy is known as root node and other devices that are lower in hierarchy known as descendants of the root node.

· There is a single path between two devices and this is the path of the communication between devices.

· Tree topology is also called **star-bus topology**.

Advantages of Tree topology

· Easy error detection.

· **Expendable:** It is easy to add new devices to the network in tree topology.

· **Easy maintenance:** Devices are grouped in small star networks and these star networks are connected to each other using bus topology. It is easy to manage a device in small star network.

· **Reliable:** One system failure doesn't bring the whole network down. The failed system can be easily managed.

· **Supports broadband transmissions:** It supports broadband transmission that is reason this topology is frequently used in corporate networks.

Disadvantages of Tree topology

· **Cost:** Cost of broadband transmission is high.

· **Dependant on backbone cable of bus topology:** All the devices connected in star networks are connected with other devices using backbone cable of bus topology. Failure in this main cable can affect the whole network.

P2P (Peer to Peer) Topology

In Peer to Peer topology, two devices are connected to each other directly. There is no client and server in P2P topology as both the devices serve the purpose of client and server both. **Torrent is an example of P2P topology** as one computer can download the data as well as upload the data to another computer.

In P2P, these two devices can be two computers, routers, switches etc. The client is the computer that requests the data and server is the computer that serves the request by sending data. In P2P, both the devices can request as well as send the data.

Con: The biggest disadvantage of P2P network is the security. A computer connected to another computer using P2P can read and write the data on the computer.

Daisy Chain Topology

In Daisy Chain Topology, all devices are connected in a linear fashion. Consider it as a ring topology where the last device is not connected to the first device. Every device in the daisy chain network is connected to **immediate left and right** neighbour devices, **except the first and last device**.

The intermediate device helps in propagating the signal by relaying it until it reaches the destination. Consider ring topology as an advanced version of this topology, by joining first and last devices in this topology a ring topology can be formed.

The advantages ring topology has over daisy chain are:

· If there is a failure in ring network, it can send the data through alternate path. For example, if the signal is transmitting clockwise and there is a failure, the signal can still reach destination by sending the signal in reverse direction.

· Since signal flows in a loop, there is less need of transmitters and receivers so their count can be reduced to lessen the cost.

2. Discuss advantages and disadvantages of each topology

Network topologies define the structure or layout of a network, specifying how different devices and nodes are connected. The main types of network topologies are:

1. **Bus Topology**
2. **Star Topology**
3. **Ring Topology**
4. **Mesh Topology**
5. **Tree Topology**
6. **Hybrid Topology**

Breakdown of the **advantages and disadvantages** of each:

1. Bus Topology

Description: All devices are connected to a single central cable (the bus).

Advantages:

- Easy to implement and extend.
- Requires less cable than other topologies.
- Cost-effective for small networks.

Disadvantages:

- Poor scalability – performance decreases as more devices are added.
- A failure in the central cable (bus) can bring down the entire network.
- Difficult to troubleshoot and isolate issues.

2. Star Topology

Description: All devices are connected to a central hub or switch.

Advantages:

- Easy to install and manage.
- Failure in one device does not affect the rest of the network.

- Easy to add new devices.

Disadvantages:

- Failure of the central hub/switch brings down the entire network.
- Requires more cabling than bus topology.
- More expensive due to the hub/switch cost.

3. Ring Topology

Description: Each device is connected to two other devices, forming a circular data path.

Advantages:

- Data flows in a single direction (or both in a dual ring), reducing collisions.
- Good performance under light loads.

Disadvantages:

- A failure in any cable or device breaks the loop and can disrupt the entire network.
- Troubleshooting is more difficult.
- Adding or removing devices can be complex.

4. Mesh Topology

Description: Devices are interconnected, with multiple paths between them.

Advantages:

- High fault tolerance – one connection failure doesn't disrupt the network.
- Excellent redundancy and reliability.
- Supports high traffic loads.

Disadvantages:

- Expensive due to the large number of cables and ports required.
- Complex setup and maintenance.
- Not practical for large-scale networks due to cost and complexity.

5. Tree Topology

Description: A hierarchical combination of star and bus topologies.

Advantages:

- Scalable – easy to add more nodes.
- Fault isolation is easier than in a pure bus.
- Ideal for large networks with branching groups.

Disadvantages:

- Dependent on the main bus – failure in backbone affects the entire network.
- More cable required than bus or ring.
- Maintenance can be difficult.

6. Hybrid Topology

Description: Combines two or more different topologies (e.g., star-bus, star-ring).

Advantages:

- Flexible – can be designed to meet specific needs.
- Scalable and efficient.
- Offers the strengths of multiple topologies.

Disadvantages:

- Complex design and implementation.
- Expensive to set up and maintain.
- Difficult to manage due to varied structure.

3. **Determine appropriate topologies for different network needs**

Selecting the appropriate network topology depends on the specific requirements of your network, including scalability, performance, cost, reliability, and ease of troubleshooting. Here's a breakdown of common topologies and scenarios where each is most appropriate:

1. **Bus Topology**

Description: All devices are connected to a single central cable (the bus).
Best for: Small, temporary, or cost-sensitive networks.

- **Pros:**
  - Inexpensive to implement
  - Easy to extend (to a point)
- **Cons:**
  - Not scalable
  - Difficult to troubleshoot
  - A single cable failure can bring down the entire network

Use case:

- Small office or lab setups where simplicity and cost matter more than speed or fault tolerance.

2. **Star Topology**

Description: All devices connect to a central hub or switch.
Best for: Most modern LANs, including home and office networks.

- **Pros:**
  - Easy to install and manage
  - Failure of one device doesn't affect the rest of the network
- **Cons:**
  - Central hub/switch is a single point of failure
  - Requires more cabling than bus topology

Use case:

- Medium-sized offices, educational institutions, or anywhere moderate scalability and stability are needed.

3. **Ring Topology**

Description: Each device is connected to two others, forming a circular data path.
Best for: Networks where data must travel in one direction or where deterministic performance is needed.

- **Pros:**
  - Better performance than bus under heavy load
  - Predictable data transmission
- **Cons:**
  - A failure in one device or cable can affect the entire network
  - Harder to troubleshoot

Use case:

- Some legacy systems, older MANs, or specialized networks like token ring (less common now).

4. **Mesh Topology**

Description: Devices are interconnected; every node may connect to every other node.
Best for: Highly reliable networks where fault tolerance is critical.

- **Pros:**
  - Redundant paths increase reliability
  - Fault isolation is easier
- **Cons:**
  - Very expensive due to cabling and ports
  - Complex setup and maintenance

Use case:

- Military, aerospace, or mission-critical systems like data centers or large-scale enterprise WANs.

5. **Tree Topology (Hierarchical)**

Description: A variation of star topology with a hierarchy of devices.
Best for: Large networks with different departments or branches.

- **Pros:**
  - Scalable and organized
  - Easier management of large segments
- **Cons:**
  - If the backbone fails, entire segments may go down
  - Requires proper planning

Use case:

- University campuses, large corporations with multiple departments.

6. **Hybrid Topology**

Description: A combination of two or more topologies.
Best for: Complex networks with varying needs.

- **Pros:**
  - Flexible and scalable
  - Can be optimized for specific performance and fault tolerance needs
- **Cons:**
  - High complexity
  - Expensive and hard to design and manage

Use case:

- Large enterprises, service providers, or institutions with diverse network requirements.

Summary Table:

Topology	Cost	Scalability	Reliability	Use Case Examples
Bus	Low	Low	Low	Small labs, temporary setups
Star	Medium	Medium	Medium-High	Homes, offices, schools
Ring	Medium	Medium	Medium	Legacy networks, specific industrial uses
Mesh	High	High	Very High	Data centers, military
Tree	Medium	High	Medium	Campuses, enterprises
Hybrid	High	Very High	High	Large organizations, service providers

Transmission Media	By the end of the session the trainee should be able to: 1. Outline types of transmission media (wired and wireless) 2. Compare performance characteristics of different media 3. Select appropriate media for specific networking environments

Transmission Media

1. Outline types of transmission media (wired and wireless)

Transmission media is the medium used to transmit data between devices in a network. It forms the communication channel that connects the sender and receiver, ensuring that data is delivered accurately and efficiently.

Key Characteristics of Transmission Media:

- **Bandwidth:** Determines the capacity to carry data.
- **Transmission Speed:** Defines how fast data can be sent.
- **Noise Resistance:** Measures the ability to resist interference.
- **Cost and Installation:** Influences the feasibility of deployment.

Applications of Transmission Media in Computer Networks

- **Corporate Networks:** Use fiber optics for high-speed data transfer between offices.
- **Home Networking:** Relies on twisted pair cables or Wi-Fi for internet connectivity.

- **Telecommunication Systems:** Employ coaxial cables and microwaves for signal transmission.
- **Military Communication:** Uses secure satellite and microwave links.

Types of Transmission Media

Transmission media is broadly categorized into two types:

1. Guided Transmission Media

Guided media, also known as **wired transmission media**, use physical paths to transmit data. These paths are tangible and include cables like twisted pair, coaxial, and fiber optics.

Examples of Guided Transmission Media:

1. **Twisted Pair Cable:**
    - Two insulated copper wires twisted together.
    - Commonly used in telephones and LANs.
2. **Coaxial Cable:**
    - Central conductor surrounded by an insulating layer and metallic shield.
    - Ideal for cable TV and broadband internet.
3. **Fiber Optic Cable:**
    - Transmits data using light signals through glass or plastic fibers.
    - Used for high-speed, long-distance communication.

2. Unguided Transmission Media

Unguided media, or **wireless transmission media**, use electromagnetic waves to transmit data through the air without physical connectors.

Examples of Unguided Transmission Media:

1. **Radio Waves:** Ideal for short to medium-range communication like Wi-Fi and AM/FM radios.
2. **Microwaves:** Used in satellite communication and long-distance point-to-point links.
3. **Infrared Waves:** Suitable for short-range communication in devices like TV remotes.

4. **Satellite Communication:** Facilitates global communication by transmitting signals via satellites.

Guided Transmission Media: Overview

Guided media is the backbone of many computer networks. Let's dive deeper into its key types:

Twisted Pair Cable

- **Features:** Cheap, flexible, and widely available.
- **Applications:** LANs, telecommunication networks.
- **Advantages:** Easy to install, suitable for short-distance communication.
- **Disadvantages:** Susceptible to interference and noise.

Coaxial Cable

Coaxial cables have four main parts, each with a specific function: the center conductor, dielectric insulator, outer conductor (shield), and outer jacket. The center conductor carries the signal, the dielectric insulator provides spacing and insulation, the outer conductor (shield) protects the signal from interference, and the outer jacket provides physical protection.

- **Features:** High bandwidth, excellent noise immunity.
- **Applications:** Cable TV, broadband internet.

- **Advantages:** Durable, supports longer distances than twisted pair.
- **Disadvantages:** Bulky and expensive compared to twisted pair.

Coax cable is defined as any cable with the following properties:

- A center conductor
- Insulation covering the center conductor, called a "dielectric"
- An optional foil shield
- A braided shield surrounding the dieletric
- An outer jacket

Each of these components plays a specific role. Let's take a look atwhat a coaxial cable is used for:

- **Center Conductor:** At the heart of a coaxial cable is a center conductor. The center conductor is responsible for transmitting the cable's signal.
- **Dielectric Insulator:** The dielectric insulator's purpose is two-fold; first, it acts as an insulator between the center conductor and the outer braided / foil shielding. Second, it helps physically hold the center conductor in the center of the cable.
- **Braided Shield:** Long copper cables have a tendency to act like antennas, picking up stray signals from the environment. These unwanted signals, known as

"interference". **Foil Shield:** Although not always present on coaxial cables, the foil shield serves to protect from RFI interference.

- **Outer Jacket:** The outer jacket is generally made out of flexible PVC (polyvinyl chloride) and serves primarily to hold the cable together and protect it from the elements.

Fiber Optic Cable

A fiber optic cable consists of several key parts, each with a specific function in transmitting data via light signals: the core, cladding, coating, strength members, and cable jacket. The core is the central part that carries the light signal. The cladding surrounds the core, reflecting the light back into the core to prevent signal loss. The coating protects the fiber from damage. The strength members provide tensile strength and protect the core from stress, and the cable jacket shields the entire cable from environmental factors.

Here's a more detailed breakdown:

· **Core:**

The heart of the fiber optic cable, the core is a thin strand of glass or plastic, typically made of silica, where light signals travel.

· **Cladding:**

Surrounding the core, the cladding is another layer of glass or plastic with a lower refractive index than the core. This difference in refractive index is crucial for total internal reflection, ensuring light stays confined within the core and propagates efficiently.

· **Coating:**

Applied over the cladding, the coating is a protective layer of plastic or acrylate. It shields the fiber from physical damage, moisture, and environmental factors, preventing scratches or breakage.

· **Strength Members:**

These are typically made of aramid yarn or fiberglass and are embedded within the cable's structure. Their purpose is to provide tensile strength, enabling the cable to withstand pulling and tension during installation and operation.

· **Cable Jacket:**

The outermost layer of the cable, the jacket, is made of a durable material like PVC or polyethylene. It protects the entire cable from environmental hazards, such as moisture, abrasion, and extreme temperatures, ensuring long-term reliability.

· Basic Components of a Fiber Optic Cable - trueCABLE

Conclusion. In summary, the core, cladding, coating, strength member Aramid yarn, and cable jacket are the five fiber optic compon...

trueCABLE

- High-speed data transmission using light.
- **Applications:** Long-distance telecommunication, data centers.
- **Advantages:** Immune to electromagnetic interference, high bandwidth.
- **Disadvantages:** Expensive, fragile, and requires specialized installation.

Unguided Transmission Media: Overview

Wireless communication has revolutionized modern networking. Here are its main types:

Radio Waves

- **Applications:** AM/FM radios, Wi-Fi networks.
- **Advantages:** Covers large areas, no physical infrastructure needed.
- **Disadvantages:** Prone to interference from other signals.

Microwaves

- **Applications:** Satellite communication, cellular networks.
- **Advantages:** High data rates over long distances.
- **Disadvantages:** Requires line-of-sight transmission.

Infrared Waves

- **Applications:** Remote controls, short-range communication.
- **Advantages:** Secure and interference-free.

- **Disadvantages:** Limited range and requires direct alignment.

Transmission Media Examples

Below are examples that illustrate the practical use of transmission media:

1. **LANs in Offices:**
    - Use twisted pair cables for connecting computers to a central router.
2. **Cable TV:**
    - Relies on coaxial cables for delivering video signals.
3. **Fiber Optic Internet:**
    - Delivers high-speed internet through fiber optic cables.
4. **Wi-Fi Networks:**
    - Use radio waves to provide wireless internet access.
5. **Satellite Communication:**
    - Uses microwaves for global telecommunication services.

Transmission Media Diagram

Below is a conceptual representation of how transmission media operates in a network:

[Sender] ---> [Guided Media: Twisted Pair / Coaxial / Fiber Optic] ---> [Receiver]
[Sender] ---> [Unguided Media: Radio Waves / Microwaves / Infrared] ---> [Receiver]

This diagram illustrates the pathways data can travel depending on the chosen transmission media.

Advantages and Disadvantages of Transmission Media

Advantages of Transmission Media	Description
Flexibility	Multiple media types, such as twisted pair, coaxial, fiber optics, and wireless, suit diverse needs.
Scalability	Supports networks of various sizes, from small local setups to extensive global networks.

Advantages of Transmission Media	Description
Cost-Effectiveness	Offers a range of options from affordable (e.g., twisted pair) to high-performance (e.g., fiber optics).
Mobility	Wireless media provide enhanced user mobility and flexibility in device placement.

Disadvantages of Transmission Media	Description
Noise and Interference	Both wired and wireless media are prone to disruptions caused by electromagnetic interference and noise.
Distance Limitations	Wired media, such as twisted pair and coaxial cables, have limited reach without the use of boosters.
Installation Challenges	Fiber optics require precise installation, and wireless setups demand careful planning and configuration.

Conclusion

Transmission media plays a critical role in enabling seamless communication in computer networks. From wired options like twisted pair and fiber optics to wireless solutions like radio waves and microwaves, each type has its own set of features, advantages, and use cases. Understanding these media helps design networks that are efficient, scalable, and suited to specific requirements.

As technology evolves, so too does the sophistication of transmission media, paving the way for faster, more reliable, and ubiquitous connectivity.

Q6. How do you choose the right transmission media?

Consider factors like distance, bandwidth requirements, cost, and environmental conditions when selecting transmission media.

Transmission media are the physical pathways that connect computers, devices, and other components in a network. These media can be **wired (guided)** or **wireless (unguided)**. Each type has different characteristics in terms of speed, reliability, cost, and application.

🔌 Wired (Guided) Transmission Media

Wired media use physical cables to transmit data signals between devices.

1. **Twisted Pair Cable**

Description: Consists of pairs of insulated copper wires twisted together to reduce electromagnetic interference.

- **Types:**
  - **UTP (Unshielded Twisted Pair):** Common in LANs (e.g., Cat5e, Cat6).
  - **STP (Shielded Twisted Pair):** Has shielding to further reduce interference.
- **Pros:**
  - Inexpensive and easy to install
  - Widely used in Ethernet networks
- **Cons:**
  - Limited distance and data rate
  - Prone to EMI (for UTP)
- **Typical Use:**
  - Office LANs, telephone lines

2. **Coaxial Cable**

Description: A single copper conductor at the center, surrounded by a plastic layer, metal shield, and outer insulating layer.

- **Pros:**
  - Better shielding and higher bandwidth than twisted pair
  - More resistant to interference
- **Cons:**
  - Bulkier and more expensive than twisted pair
  - Not commonly used in new installations
- **Typical Use:**
  - Cable TV, legacy Ethernet networks, broadband internet

3. **Fiber Optic Cable**

Description: Uses light to transmit data through strands of glass or plastic fibers.

- **Types:**
  - **Single-mode:** Long distances, higher cost (e.g., WAN backbones)
  - **Multi-mode:** Shorter distances, cheaper (e.g., LANs)
- **Pros:**
  - Extremely high speed and bandwidth
  - Immune to electromagnetic interference
  - Supports long-distance transmission
- **Cons:**
  - Expensive to install and maintain
  - Requires specialized equipment and skills
- **Typical Use:**
  - Internet backbone, large enterprise networks, data centers

📡 Wireless (Unguided) Transmission Media

Wireless media transmit signals through the air using electromagnetic waves.

1. **Radio Waves**

Description: Low-frequency waves that travel in all directions.

- **Pros:**
  - Can cover long distances (especially with low frequencies)
  - Suitable for both indoor and outdoor use
- **Cons:**
  - Susceptible to interference
  - Less secure without encryption
- **Typical Use:**

- Wi-Fi, Bluetooth, AM/FM radio, mobile phones

2. **Microwaves**

Description: Higher frequency radio waves, often line-of-sight.

- **Pros:**
  - Suitable for point-to-point communication
  - High bandwidth
- **Cons:**
  - Affected by weather (rain fade)
  - Requires line-of-sight alignment
- **Typical Use:**
  - Satellite communication, long-distance telephone, cellular networks

3. **Infrared (IR)**

Description: Short-range wireless communication using infrared light.

- **Pros:**
  - Immune to radio interference
  - Secure in closed environments
- **Cons:**
  - Requires direct line of sight
  - Limited range
- **Typical Use:**
  - Remote controls, some short-range data transfers

4. **Satellite Communication**

Description: Uses satellites in orbit to relay signals across the globe.

- **Pros:**
  - Covers vast geographic areas
  - Useful for remote locations
- **Cons:**
  - High latency
  - Expensive equipment and bandwidth
- **Typical Use:**
  - Global television, GPS, rural internet

5. **Wi-Fi and Cellular**

- **Wi-Fi (802.11):** Local area wireless network for homes and businesses.
- **Cellular (e.g., 4G, 5G):** Wide-area network for mobile devices.
- **Pros:**
  - Mobility and convenience
  - Increasing speeds with new technologies
- **Cons:**
  - Vulnerable to interference and security threats
  - Coverage depends on infrastructure
- **Typical Use:**
  - Internet access, mobile data, smart devices

📋 Summary Table

Medium	Type	Speed	Range	Common Use
Twisted Pair	Wired	Up to 10 Gbps	100 meters	LANs, telephone lines
Coaxial Cable	Wired	Hundreds of Mbps	500 meters	Cable TV, broadband internet

Medium	Type	Speed	Range	Common Use
Fiber Optic	Wired	100 Gbps+	Kilometers	Backbone networks, data centers
Radio Waves	Wireless	Varies (Wi-Fi: Gbps)	100+ meters	Wi-Fi, Bluetooth, mobile phones
Microwaves	Wireless	Hundreds of Mbps+	Long distance	Cell towers, point-to-point links
Infrared	Wireless	Mbps	A few meters	Remote controls, short-range comms
Satellite	Wireless	Mbps to Gbps	Global	GPS, global TV, rural connectivity
Cellular (4G/5G)	Wireless	100 Mbps – Gbps	Wide-area	Mobile internet, smart devices

2. Compare performance characteristics of different media

comparison of **performance characteristics** of different transmission media, both **wired** and **wireless**, based on key criteria:

📊 Comparison Table: Performance Characteristics

Medium	Bandwidth / Speed	Latency	Interference Susceptibility	Distance / Range	Security	Cost	Reliability
Twisted Pair (UTP/STP)	Up to 10 Gbps (Cat6/7)	Low	Medium (esp. UTP)	~100 meters	Medium	Low	Medium
Coaxial Cable	Up to 1 Gbps (some DOCSIS)	Low	Low	Up to 500 meters	Medium	Medium	High
Fiber Optic (SM/MM)	100 Gbps+	Very Low	Very Low (immune to EMI)	Several kilometers	High	High	Very High
Radio Waves (Wi-Fi, Bluetooth)	Up to several Gbps (Wi-Fi 6/7)	Medium	High	~10–100 meters	Low without encryption	Low-Medium	Medium (varies by setup)

Medium	Bandwidth / Speed	Latency	Interference Susceptibility	Distance / Range	Security	Cost	Reliability
Microwaves	Hundreds of Mbps–Gbps	Medium–High (esp. long links)	Medium–High	Up to 50 km (line-of-sight)	Medium	Medium–High	Medium (weather sensitive)
Infrared	Low–Moderate (few Mbps)	Very Low	Low	A few meters (line-of-sight)	High (contained)	Low	Medium
Satellite	Mbps–Gbps	High (due to distance)	Medium	Global	Medium	Very High	Medium (weather, latency)
Cellular (4G/5G)	100 Mbps – 10 Gbps+	Medium (5G = Low)	Medium	Up to several kilometers	Medium	Medium	High (with dense coverage)

📌 **Performance Analysis by Characteristic**

✅ **1. Bandwidth / Speed**

- **Best:** *Fiber Optic, 5G, High-end Wi-Fi*
- **Moderate:** *Coaxial, Twisted Pair (Cat5e/6)*
- **Low:** *Infrared, older cellular (3G)*

✅ **2. Latency**

- **Lowest:** *Fiber Optic, Infrared, Ethernet (twisted pair)*
- **Highest:** *Satellite (due to long signal travel time)*

✅ **3. Interference Susceptibility**

- **Least susceptible:** *Fiber Optic (immune to EMI), Infrared (in closed spaces)*
- **Most susceptible:** *Radio, Microwave (weather), Unshielded Twisted Pair*

✅ **4. Range**

- **Best for short range:** *Wi-Fi, Bluetooth, Twisted Pair*

- **Best for long range:** *Fiber Optic, Satellite, Microwave, Cellular*

✅ **5. Security**

- **Most secure:** *Fiber Optic, Infrared (closed line-of-sight)*
- **Less secure (needs encryption):** *Wi-Fi, Radio, Satellite*

✅ **6. Cost**

- **Lowest:** *Twisted Pair, Infrared*
- **Highest:** *Fiber Optic (initial cost), Satellite*

✅ **7. Reliability**

- **Most reliable:** *Fiber Optic, Coaxial*
- **Less reliable:** *Wi-Fi (in crowded areas), Satellite (weather dependent)*

🧠 **Recommendation Summary**

Use Case	Recommended Medium	Why
High-speed, secure backbone	Fiber Optic	Highest bandwidth, immune to EMI
Home/Office LAN	Twisted Pair (Cat6)	Cost-effective, easy to install
Long-distance urban link	Microwave or Fiber	Suitable for building-to-building links
Rural or remote internet	Satellite or Cellular	Wide coverage, no physical cables needed
Mobile communication	4G/5G Cellular	High mobility and range
Device interconnect (short-range)	Bluetooth, Infrared	Low power, short-range communications

3. **Select appropriate media for specific networking environments**

Selecting the **appropriate transmission media** for a specific networking environment involves balancing factors like bandwidth needs, distance, environment (indoor/outdoor), cost, and security. Below is a list of **common networking environments** along with the **most suitable transmission media** and the reasons why:

🌐 1. Local Area Network (LAN) – Office or Home

- **Recommended Media:**
  - **Twisted Pair (Cat6 or Cat6a)**
  - **Wi-Fi (802.11ac/ax/6/6E/7)**
- **Why:**
  - Twisted pair (Cat6) supports up to 10 Gbps at short distances—perfect for desktops and servers.
  - Wi-Fi allows wireless access for mobile devices, reducing cabling needs.
- **Hybrid Approach:** Use Ethernet for high-demand devices (e.g., servers, PCs) and Wi-Fi for mobility (phones, laptops).

🏢 2. Campus Network (University or Corporate HQ with Multiple Buildings)

- **Recommended Media:**
  - **Fiber Optic (Single-mode for backbone)**
  - **Twisted Pair (Cat6/7 within buildings)**
  - **Wi-Fi (for user access)**
- **Why:**
  - Fiber optic is essential for long-distance, high-speed links between buildings.
  - Twisted pair supports office workstations inside buildings.
  - Wi-Fi covers general mobility needs on campus.

🏙️ 3. Metropolitan Area Network (MAN) – Citywide ISP or Municipal Network

- **Recommended Media:**
    - **Fiber Optic**
    - **Microwave Links (point-to-point)**
    - **Coaxial (where legacy systems are used)**
- **Why:**
    - Fiber provides the necessary bandwidth and distance.
    - Microwave bridges can link areas where laying cables is impractical.

🌍 4. Wide Area Network (WAN) – ISP Backbone or Multi-Branch Organization

- **Recommended Media:**
    - **Fiber Optic (main backbone)**
    - **Satellite (for remote or inaccessible areas)**
    - **Cellular (for backup or mobile offices)**
- **Why:**
    - Fiber offers low latency and high throughput over long distances.
    - Satellite provides global reach, albeit with higher latency.
    - 4G/5G can offer rapid deployment in temporary or mobile setups.

🏠 5. Smart Home or IoT Network

- **Recommended Media:**
    - **Wi-Fi 6 or Wi-Fi 6E**
    - **Bluetooth Low Energy (BLE)**
    - **Zigbee / Z-Wave / Thread (for IoT devices)**
- **Why:**
    - Wi-Fi supports high-speed needs for media and home automation.

- BLE and Zigbee provide low-power, short-range communication ideal for sensors and smart devices.

🏗️ 6. Industrial/Factory Environment (Industrial IoT)

- **Recommended Media:**
  - **Fiber Optic (for EMI-heavy environments)**
  - **Shielded Twisted Pair (STP)**
  - **5G/Private LTE (for mobile robots, AGVs)**
- **Why:**
  - Fiber is immune to electrical noise (EMI).
  - STP withstands industrial interference better than UTP.
  - Private wireless ensures flexibility and real-time responsiveness.

🚜 7. Remote or Rural Locations

- **Recommended Media:**
  - **Satellite (e.g., Starlink)**
  - **4G/5G Cellular Networks**
  - **Fixed Wireless (radio or microwave)**
- **Why:**
  - These areas often lack fiber or cable infrastructure.
  - Satellite and wireless options provide broadband access with minimal setup.

1.5 Distributed system is explained

Distributed System Explained

A distributed system in networking is a collection of independent computers, or nodes, that work together as a single, coherent system to achieve a common goal. These nodes communicate and coordinate their activities over a network, sharing resources and tasks to

solve problems that a single computer might struggle with due to limitations in processing power, storage, or fault tolerance

A group of separate computers that provide a sense of being a single, cohesive system to its users is known as a distributed system. These computers, also known as nodes, collaborate, exchange information via a network, and plan their actions to accomplish a shared objective by sharing resources, tasks, and data. Characteristics of Distributed Systems include:

A **Distributed System** is a model in which components located on networked computers communicate and coordinate their actions by passing messages. These components interact with each other to achieve a common goal, and the system appears to the user as a single coherent system.

Key Features of Distributed Systems:

1. **Multiple Components**:

o The system is made up of several independent computers (nodes or hosts).

o Each node performs part of the computation or data storage.

2. **Concurrency**:

o Tasks are executed simultaneously across different nodes, increasing efficiency and performance.

3. **Scalability**:

o Systems can easily scale horizontally by adding more nodes to manage increased load.

4. **Resource Sharing**:

o Resources such as files, printers, and processing power are shared across the system.

5. **Fault Tolerance**:

o The system continues to function even if some components fail.

6. **Transparency**:

o The complexity of the distributed nature is hidden from users. They experience it as a single system.

Examples of Distributed Systems:

- **Internet**: A massive global distributed system.
- **Cloud Computing Platforms** (e.g., AWS, Azure): Offer storage, computing, and networking services.
- **Distributed Databases** (e.g., Cassandra, MongoDB).
- **Blockchain Networks**: A decentralized distributed ledger system.

Types of Distributed Systems:

1. **Client-Server**: Clients request services, and servers provide them.
2. **Peer-to-Peer (P2P)**: All nodes are equal and share resources directly.
3. **Three-Tier Architecture**: Includes presentation, logic, and data storage layers.

Advantages:

- Improved reliability and availability
- Scalability and flexibility
- Better resource utilization
- Geographic distribution

Challenges:

- Network issues and latency
- Data consistency and synchronization
- Security and privacy concerns
- Complex debugging and monitoring

Advantages of Distributed Systems

1. **Scalability**
   - Easily scaled by adding more nodes (horizontal scaling).
   - Can handle growing workloads effectively.
2. **Reliability and Fault Tolerance**

- If one node fails, others can take over the workload.
- System continues to function even during partial failures.

3. **Resource Sharing**

- Resources like data, files, printers, and services can be shared across the system.

4. **Concurrency**

- Multiple processes can be executed simultaneously across different machines, improving performance.

5. **Flexibility and Modularity**

- Systems can be maintained or upgraded node by node.
- Easier to isolate and fix problems without shutting down the entire system.

6. **Cost Efficiency**

- Uses commodity hardware rather than expensive mainframes.
- Reduces cost by using distributed processing.

7. **Geographical Distribution**

- Nodes can be located in different geographical areas, useful for global services and disaster recovery.

❌ Disadvantages of Distributed Systems

1. **Complexity**

- Designing, implementing, and maintaining distributed systems is more complex than centralized ones.

2. **Security Challenges**

- More entry points increase vulnerability.
- Requires complex authentication, encryption, and monitoring.

3. **Network Dependency**

- System performance and reliability depend on network stability.
- Latency or network failures can disrupt communication between nodes.

4. **Data Consistency Issues**

- Keeping data synchronized across all nodes is difficult.
- Can lead to conflicts or outdated data in some nodes.

5. **Debugging and Troubleshooting**

- Difficult to trace errors due to distributed nature.
- Monitoring and logging across many nodes can be challenging.

6. **Software Compatibility and Version Control**

- Ensuring all nodes run compatible versions of software can be hard to manage.

7. **Higher Initial Setup Cost**

- While hardware may be cheaper, the setup, configuration, and skilled personnel needed can be costly.

Summary Table

Advantages	**Disadvantages**
Scalable	Complex to design and maintain
Fault-tolerant	Security risks
Efficient resource utilization	Depends on network reliability
Concurrent processing	Data consistency problems
Modular and flexible	Harder to debug and manage
Cost-effective hardware	Software version control issues

1.6 ***Types of distributed systems*** are illustrated

Distributed systems can be broadly categorized into client-server, peer-to-peer, and middleware-based systems, with further distinctions like three-tier and N-tier architectures. These systems leverage multiple computers to achieve a common goal, offering advantages in scalability, resource utilization, and fault tolerance.

Types of Distributed System

Pre-requisites: Distributed System

A Distributed System is a Network of Machines that can exchange information with each other through Message-passing. It can be very useful as it helps in resource sharing. It enables computers to coordinate their activities and to share the resources of the system so that users perceive the system as a single, integrated computing facility.

Types of Distributed Systems

1. Client/Server Systems
2. Peer-to-Peer Systems
3. Middleware
4. Three-tier
5. N-tier

1. Client/Server Systems: Client-Server System is the most basic communication method where the client sends input to the server and the server replies to the client with an output. The client requests the server for resources or a task to do, the server allocates the resource or performs the task and sends the result in the form of a response to the request of the client. Client Server System can be applied with multiple servers.

2. Peer-to-Peer Systems: Peer-to-Peer System communication model works as a decentralized model in which the system works like both Client and Server. Nodes are an important part of a system. In this, each node performs its task on its local memory and shares data through the supporting medium, this node can work as a server or as a client for a system. Programs in the peer-to-peer system can communicate at the same level without any hierarchy.

3. Middleware: Middleware can be thought of as an application that sits between two separate applications and provides service to both. It works as a base for different interoperability applications running on different operating systems. Data can be transferred to other between others by using this service.

4. Three-tier: Three-tier system uses a separate layer and server for each function of a program. In this data of the client is stored in the middle tier rather than sorted into the client system or on their server through which development can be done easily. It includes an Application Layer, Data Layer, and Presentation Layer. This is mostly used in web or online applications.

5. N-tier: N-tier is also called a multitier distributed system. The N-tier system can contain any number of functions in the network. N-tier systems contain similar structures to three-tier

architecture. When interoperability sends the request to another application to perform a task or to provide a service. N-tier is commonly used in web applications and data systems.

Distributed System

Characteristics of Distributed System

· **Resource Sharing:** It is the ability to use any Hardware, Software, or Data anywhere in the System.

· **Concurrency:** It is naturally present in Distributed Systems, that deal with the same activity or functionality that can be performed by separate users who are in remote locations. Every local system has its independent Operating Systems and Resources.

· **Scalability:** It increases the scale of the system as several processors communicate with more users by accommodating to improve the responsiveness of the system.

· **Transparency:** It hides the complexity of the Distributed Systems from the Users and Application programs as there should be privacy in every system.

Challenges of Distributed Systems

· **Network latency:** The communication network in a distributed system can introduce latency, which can affect the performance of the system.

· **Distributed coordination:** Distributed systems require coordination among the nodes, which can be challenging because of the distributed nature of the system.

· **Data consistency:** Maintaining data consistency across multiple nodes in a distributed system can be challenging.