DATA COMMUNICATION AND NETWORKING

UNIT-1

Evolution of Computer Networks:

The evolution of computer networks can be traced back to the 1960s when the first wide area network (WAN) was developed. Since then, computer networks have undergone several transformations to become the complex systems that we rely on today. Here is a brief overview of the evolution of computer networks:

1. **The ARPANET (1969):** The ARPANET was the first wide-area packet-switching network and was developed by the US Department of Defense's Advanced Research Projects Agency (ARPA). It was the precursor to the internet and was designed to allow scientists and researchers to share resources and communicate with each other.
2. **Ethernet (1973):** Ethernet was developed by Xerox PARC as a local area network (LAN) technology. It allowed computers to be connected to each other within a building or campus and was much faster than previous technologies.
3. **TCP/IP (1983):** The Transmission Control Protocol/Internet Protocol (TCP/IP) was developed to connect networks together into a single global internet. This was the beginning of the internet as we know it today.
4. **World Wide Web (1990):** The World Wide Web was developed by Tim Berners-Lee as a way to easily access and share information over the internet. It quickly became the most popular way to access the internet and has transformed the way we communicate and share information.
5. **Wireless Networks (late 1990s):** Wireless networks were developed, which allowed devices to connect to the internet without cables. This made it possible to access the internet from anywhere and transformed the way we use computers and mobile devices.
6. **Cloud Computing (2000s):** Cloud computing made it possible to store and access data and applications over the internet, rather than on local devices. This made it easier and more cost-effective for individuals and businesses to store and share data.
7. **Internet of Things (IoT) (2010s):** The IoT refers to the growing number of devices and objects that are connected to the internet, such as smart home devices, wearables, and industrial sensors. This has the potential to transform industries and our daily lives.

CODECHAMP
CREATED WITH ARBOK

Network architecture:

Network architecture refers to the design and layout of a computer network. It includes the hardware, software, protocols, and policies that govern the network's operation. A well-designed network architecture can enhance performance, security, and scalability. A network architecture diagram visually represents the components and relationships between them.

Here are some key components of a network architecture diagram:

1. **Network Topology:** The physical or logical layout of the network is the topology. The topology determines how devices are connected and how data flows through the network.
2. **Network Devices:** The devices used in a network can include routers, switches, firewalls, servers, and storage devices. These devices work together to provide services and support communication.
3. **Network Protocols:** These are the rules and standards that define how data is transmitted, received, and processed in a network. Common protocols include TCP/IP, HTTP, and SMTP.
4. **Network Security:** This is the process of protecting the network from unauthorized access, theft, or damage. Network security can include firewalls, intrusion detection systems, and encryption.
5. **Network Services:** These are the applications or services that run on the network, such as email, file sharing, and web browsing. These services depend on the network's hardware, software, and protocols.

Configuring Network:

Configuring a network involves several steps that are necessary to set up a reliable and efficient communication system between devices. Here are some detailed notes on how to configure a network:

CODECHAMP
CREATED WITH ARBOK

1. **Identify the network requirements -** Before configuring the network, it is essential to determine the network requirements, such as the number of devices that need to be connected, the type of data that will be transmitted, and the distance between the devices. This information helps in selecting the appropriate network topology, devices, and protocols.
2. **Choose the network topology -** Network topology is the physical or logical arrangement of devices in a network. There are several network topologies available, including bus, star, ring, mesh, and hybrid. The topology chosen should be based on the network requirements and the physical layout of the devices.
3. **Choose the networking devices -** A network requires several devices to function, including routers, switches, modems, access points, and hubs. The devices chosen should be based on the network topology, the number of devices to be connected, and the distance between them.
4. **Configure the network devices -** Once the devices are selected, they need to be configured to enable communication between the devices. The configuration includes assigning IP addresses, setting up DHCP, configuring NAT, enabling firewalls, and setting up VLANs.
5. **Set up the network protocols -** Network protocols are the rules and procedures that govern communication between devices in a network. Some of the common protocols used in networking include TCP/IP, HTTP, FTP, SMTP, and DNS. These protocols need to be configured to enable the devices to communicate effectively.

6. **Configure security settings -** Network security is critical to protect the network from unauthorized access and data breaches. The security settings should include setting up passwords, encrypting data, and setting up firewalls.
7. **Test the network -** Once the network is set up, it is essential to test it to ensure that it is functioning correctly. The testing should include checking connectivity between devices, checking the speed of data transfer, and checking the security settings.

Network Strategies:

Network strategies refer to a set of tactics or plans implemented by organizations to optimize the performance and security of their network. Network strategies help organizations meet their goals by reducing network downtime, enhancing network security, improving network accessibility and reliability, and optimizing network speed and efficiency. The following are some network strategies:

1. Network design strategy:

This strategy involves designing a network infrastructure that aligns with the organization's objectives, needs, and budget. It includes determining the type of network, devices, and connectivity options that are most suitable for the organization. The network design strategy should also take into consideration future growth, scalability, and disaster recovery plans.

CODECHAMP
CREATED WITH ARBOK

2. Network security strategy:

This strategy focuses on ensuring the confidentiality, integrity, and availability of network resources. It includes implementing firewalls, intrusion detection systems, encryption, and access control mechanisms to protect the network from external and internal threats. A network security strategy should be regularly reviewed and updated to counter new and evolving security threats.

3. Network performance strategy:

This strategy aims to optimize network performance by minimizing downtime, enhancing speed and efficiency, and ensuring data availability. It includes deploying technologies such as load balancing, Quality of Service (QoS), bandwidth management, and network monitoring tools to identify and address performance issues.

4. Network accessibility strategy:

This strategy aims to ensure that the network is accessible to authorized users from anywhere and at any time. It includes implementing virtual private networks (VPNs), remote access technologies, and mobile device management (MDM) tools to facilitate secure and convenient access to the network.

5. Network backup and disaster recovery strategy:

This strategy focuses on minimizing the impact of network downtime caused by disasters such as power outages, natural disasters, or cyber-attacks. It includes backing up critical data and systems, establishing redundant network connections, and implementing disaster recovery plans to minimize downtime and data loss.

Network Types:

There are several types of networks, each with its own unique features and characteristics. Some of the most common types of networks include:

1. Local Area Network (LAN):

A LAN is a network that connects devices within a small geographical area such as an office, home or school. This network is used to share resources like printers, scanners, files and internet connection.

2. Wide Area Network (WAN):

A WAN is a network that connects devices over a large geographical area like a city, state or even a country. The internet is the most common example of a WAN, which enables the connection of devices and computers all over the world.

3. Metropolitan Area Network (MAN):

A MAN is a network that connects devices within a metropolitan area like a city or town. This network is used to share resources like data, video and voice communication between different organizations and businesses.

CODECHAMP
CREATED WITH ARBOK

4. Wireless Local Area Network (WLAN):

A WLAN is a wireless network that connects devices within a small geographical area like an office, home or school. This network uses wireless technologies like Wi-Fi to connect devices to the network.

5. Personal Area Network (PAN):

A PAN is a network that connects devices within a person's personal space like their mobile phone, laptop or wearable devices. This network is used to share data and files between devices.

6. Virtual Private Network (VPN):

A VPN is a secure network that connects devices over the internet. This network is used to access data and resources from remote locations and to maintain privacy and security.

Line configuration:

Line configuration is the arrangement of communication lines between two devices or network nodes. It is the physical layout of the communication path, and it determines the type of signals that can be transmitted between devices. The following are the different types of line configurations:

1. Point-to-Point:

In point-to-point line configuration, two devices are connected using a single communication line. It is a simple and straightforward connection that is used for communication between two devices over short distances. Point-to-point connections are widely used in telecommunications networks, and they provide reliable and fast communication.

2. Multipoint:

In a multipoint line configuration, more than two devices are connected using a single communication line. The line is shared by all devices, and any device can communicate with any other device on the line. Multipoint connections are commonly used in local area networks (LANs) and wide area networks (WANs), where multiple devices need to communicate with each other.

Network Topology:

Network topology refers to the physical or logical layout of the components of a computer network. There are several types of network topologies, each with its advantages and disadvantages. The following are some of the most common network topologies:

CODECHAMP
CREATED WITH ARBOK

1. Bus Topology:

In a bus topology, all devices in the network are connected to a single cable called a backbone. The backbone acts as a communication channel, and devices communicate by sending data signals along the cable. The bus topology is simple, inexpensive, and easy to implement, but it is prone to signal interference and difficult to troubleshoot.

2. Star Topology:

In a star topology, all devices in the network are connected to a central device called a hub or a switch. The hub acts as a central point of communication, and devices communicate by sending data signals to the hub. The star topology is reliable, easy to troubleshoot, and scalable, but it is more expensive than a bus topology.

3. Ring Topology:

In a ring topology, all devices in the network are connected in a circular ring, with each device connected to its neighboring devices. Data signals are transmitted from one device to the next until they reach the destination device. The ring topology is reliable, easy to troubleshoot, and has good performance, but it is expensive to implement and difficult to scale.

4. Mesh Topology:

In a mesh topology, each device in the network is connected to every other device, creating a mesh of interconnected devices. Data signals are transmitted through multiple paths, providing redundancy and fault tolerance. The mesh topology is highly reliable, scalable, and has excellent performance, but it is expensive to implement and difficult to manage.

5. Hybrid Topology:

A hybrid topology is a combination of two or more of the above topologies. For example, a network may have a star topology with each star connected to other stars in a mesh topology. The hybrid topology combines the advantages of the individual topologies while minimizing their disadvantages.

Transmission mode:

Transmission mode refers to the way data is transmitted from one device to another. It defines the way in which information is encoded and transmitted over a communication channel, such as a wired or wireless network. There are several different transmission modes, including simplex, half-duplex, and full duplex.

CODECHAMP
CREATED WITH ARBOK

1. Simplex transmission

Simplex transmission is the simplest form of data transmission, where data is transmitted in only one direction. In this mode, data can only be sent from the sender to the receiver, and there is no feedback or response from the receiver. Examples of simplex transmission include broadcast radio or television, where the sender broadcasts information to many receivers, but no feedback is received.

2. Half-duplex transmission

Half-duplex transmission is a mode of transmission where data can be sent in both directions, but only one direction at a time. In half-duplex transmission, data is transmitted from the sender to the receiver, and then the receiver can respond by transmitting data back to the sender. This type of transmission is commonly used in two-way radios and walkie-talkies, where users take turns speaking and listening.

3. Full-duplex transmission

Full-duplex transmission is a mode of transmission where data can be sent in both directions simultaneously. In full-duplex transmission, data is transmitted from the sender to the receiver, and the receiver can respond at the same time with their own data. This type of transmission is commonly used in telephone conversations and video conferencing, where both parties can speak and listen at the same time.

key components of network:

A network is a group of devices, such as computers, printers, routers, and switches, that are connected to share information and resources. There are several key components that make up a network, including:

1. **Network Interface Cards (NICs):** NICs are the hardware components that enable devices to connect to the network. They are responsible for sending and receiving data packets across the network.
2. **Cables:** Cables are the physical components that connect devices to the network. There are several types of cables, including Ethernet, fiber optic, and coaxial cables.
3. **Switches:** Switches are networking devices that connect devices on a network. They manage traffic on the network and direct data packets to the appropriate device.
4. **Routers:** Routers are networking devices that connect multiple networks together. They manage traffic between networks and direct data packets to the appropriate destination.
5. **Firewalls:** Firewalls are software or hardware devices that protect the network from unauthorized access. They monitor incoming and outgoing traffic and prevent unauthorized access to the network.
6. **Network Operating Systems (NOS):** NOS is the software that manages and controls the network. It provides services such as file sharing, printing, and security.
7. **Servers**: Servers are computers that provide services to the network. They can provide file sharing, printing, email, web hosting, and other services.
8. **Clients:** Clients are devices that access services provided by servers. They can be desktop computers, laptops, smartphones, or tablets.
9. **Protocols:** Protocols are the rules and standards that govern communication on the network. They define how data is transmitted, received, and interpreted by devices on the network.
10. **IP Addressing:** IP addressing is the system used to identify and locate devices on the network. It assigns a unique address to each device on the network, which enables data packets to be sent and received between devices.

CODECHAMP
CREATED WITH ARBOK

Categories of network:

Networks can be categorized based on various factors such as their size, topology, protocol, and application. Let's look at each of these categories in more detail:

A. Size of Network:

1. **LAN (Local Area Network):** A LAN is a small network that covers a small area such as a building, a floor, or a room. It is used for sharing resources and data within the organization.

2. **MAN (Metropolitan Area Network):** A MAN is a network that covers a city or a metropolitan area. It is used for connecting multiple LANs and sharing resources over a larger area.
3. **WAN (Wide Area Network):** A WAN is a network that covers a wide geographical area, such as a country or the world. It is used for connecting multiple MANs and LANs, and sharing resources over a large area.

B. Topology of Network:

1. **Bus Topology:** In a bus topology, all devices are connected to a single cable or backbone. This topology is simple and inexpensive but can have issues with congestion and security.
2. **Ring Topology:** In a ring topology, devices are connected in a circular loop. Data travels in one direction around the loop, and each device is connected to the next. This topology is reliable but can have issues with scalability.
3. **Star Topology:** In a star topology, all devices are connected to a central hub or switch. This topology is easy to manage and troubleshoot but can have issues with a single point of failure.

C. Protocol of Network:

1. TCP/IP (Transmission Control Protocol/Internet Protocol): TCP/IP is the standard protocol used for the internet and most networks. It is a set of rules for communication between devices.
2. Ethernet: Ethernet is a protocol for local area networks. It is used for communication between devices and for sharing resources such as printers and files.
3. Wi-Fi: Wi-Fi is a wireless protocol for connecting devices to a network. It is commonly used for connecting mobile devices and laptops to the internet.

CODECHAMP
CREATED WITH ARBOK

D. Application of Network:

1. **Client-Server:** In a client-server network, one or more servers provide resources and services to clients. This type of network is commonly used in businesses and organizations.
2. **Peer-to-Peer:** In a peer-to-peer network, all devices have equal status and can share resources and services. This type of network is commonly used for sharing files and printers in a small group of devices.
3. **Cloud:** A cloud network is a type of network that is hosted on the internet. It allows users to access resources and services from anywhere with an internet connection. This type of network is commonly used for online storage and web applications.

Differentiating between LAN, MAN, WANS and Internet:

The main differences between LAN, MAN, WAN, and the Internet are:

1. Geographical Coverage:

LANs cover a small geographical area, typically a single building or campus. MANs cover a larger geographical area, typically a city or town. WANs cover a wide geographical area, such as a country or the entire world. The Internet covers the entire world.

2. Ownership and Control:

LANs are owned and controlled by a single organization, such as a company or school. MANs may be owned and controlled by a single organization or a group of organizations. WANs are typically owned and controlled by multiple organizations, such as internet service providers. The Internet is owned and controlled by a wide range of organizations and individuals.

3. Speed and Capacity:

LANs typically offer high-speed communication and data sharing among connected devices. MANs and WANs may offer lower speeds due to the longer distances involved, and their capacity may be limited by the number of devices connected to the network. The Internet offers high-speed communication but its capacity may be limited by the number of users accessing it at the same time.

4. Purpose:

LANs are primarily used for local communication and data sharing within a single organization. MANs are used to connect multiple LANs within a metropolitan area. WANs are used to connect LANs and MANs over long distances. The Internet is used for global communication and data sharing between individuals and organizations around the world.

CODECHAMP
CREATED WITH ARBOK