Shastri 3rd Semester

Computer Science

Unit: 1st

Internet Technology and Protocol

Characteristics of Local Area Network & Wide Area Network:

Local Area Network (LAN):

LANs typically cover a small geographic area, such as a single building or campus.

LANs are typically owned and operated by a single organization.

LANs use high-speed technologies such as Ethernet or Token Ring to connect devices.

LANs have a relatively small number of devices connected to them (compared to WANs).

LANs are typically used for sharing resources such as printers and files, and for communication between devices within the same organization.

Wide Area Network (WAN):

WANs cover a large geographic area, such as a city, state, or even multiple countries.

WANs may be owned and operated by multiple organizations, or by a single organization with multiple locations.

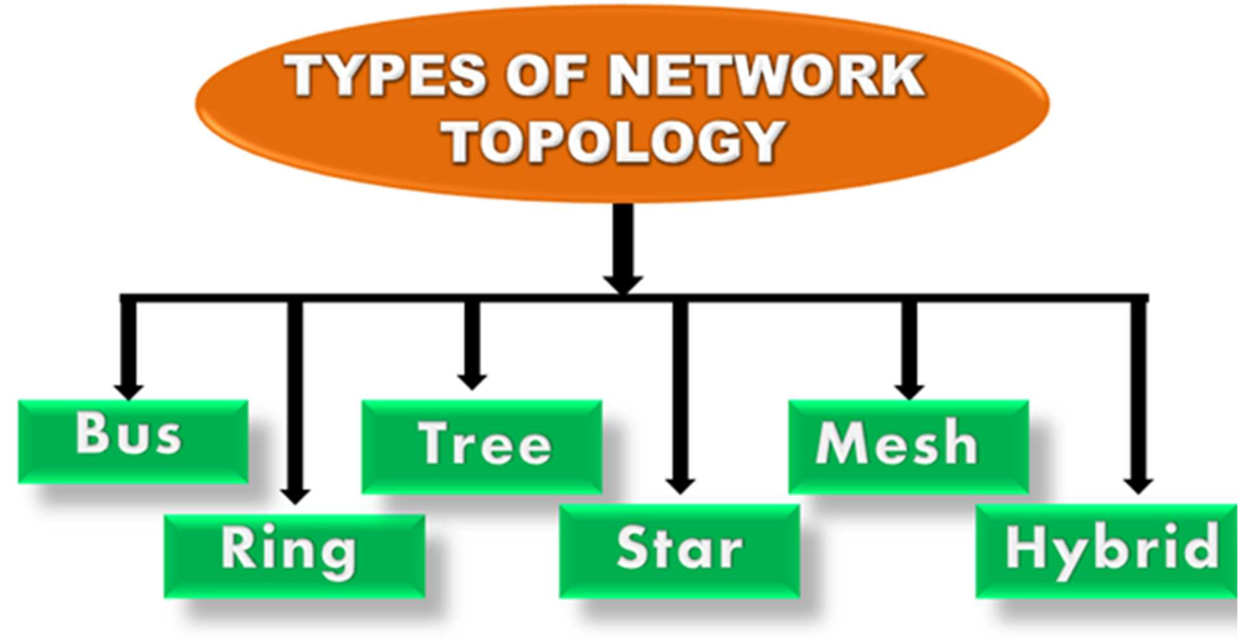
WANs use technologies such as T1, T3, or SONET to connect devices.

WANs have a relatively large number of devices connected to them (compared to LANs).

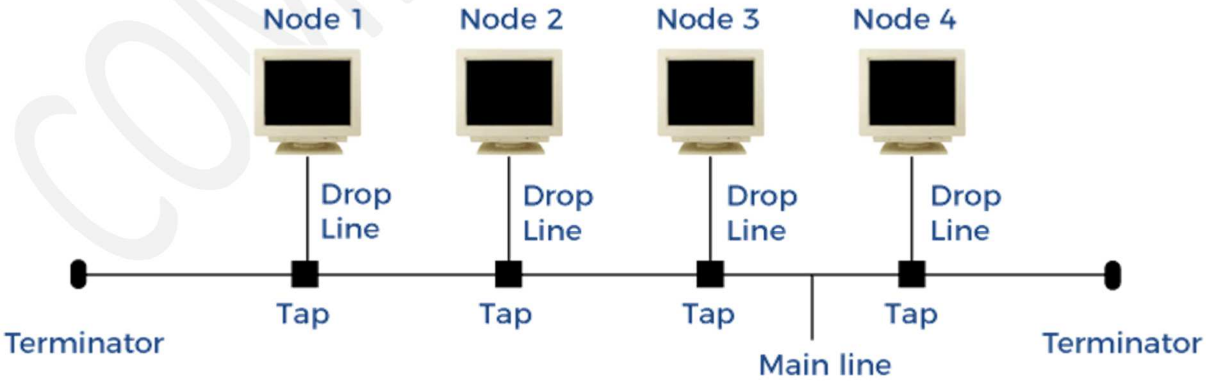
WANs are typically used for connecting multiple LANs together, allowing devices in different locations to communicate with each other.

Local Area Network (LAN): topology

The topology of a Local Area Network (LAN) refers to the physical and logical layout of the network. There are several common LAN topologies, including:

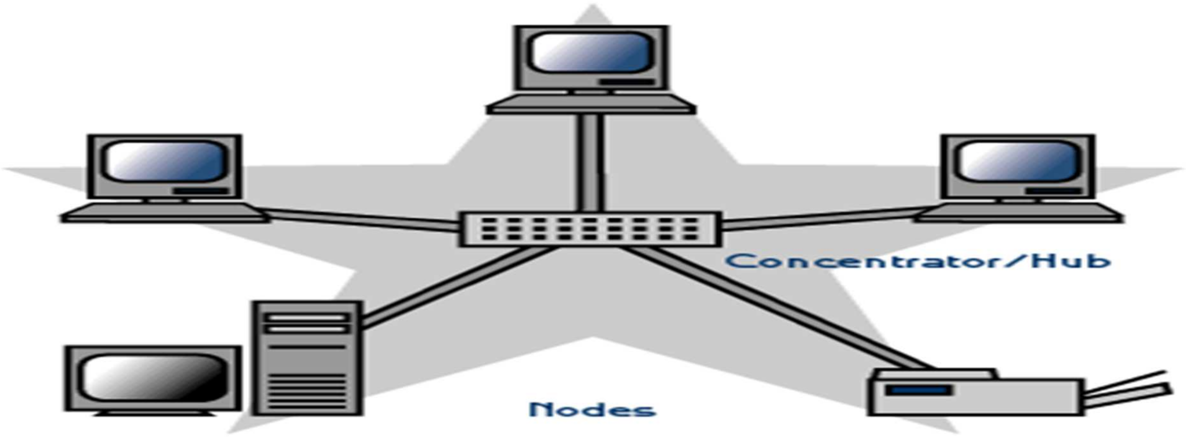


Bus topology: In a bus topology, all devices are connected to a single cable, known as the bus. This cable acts as a backbone for the network, and all data transmitted on the network travels along the bus. The main advantage of this topology is its simplicity and low cost, however, if the bus is damaged or disconnected the entire network will be affected.

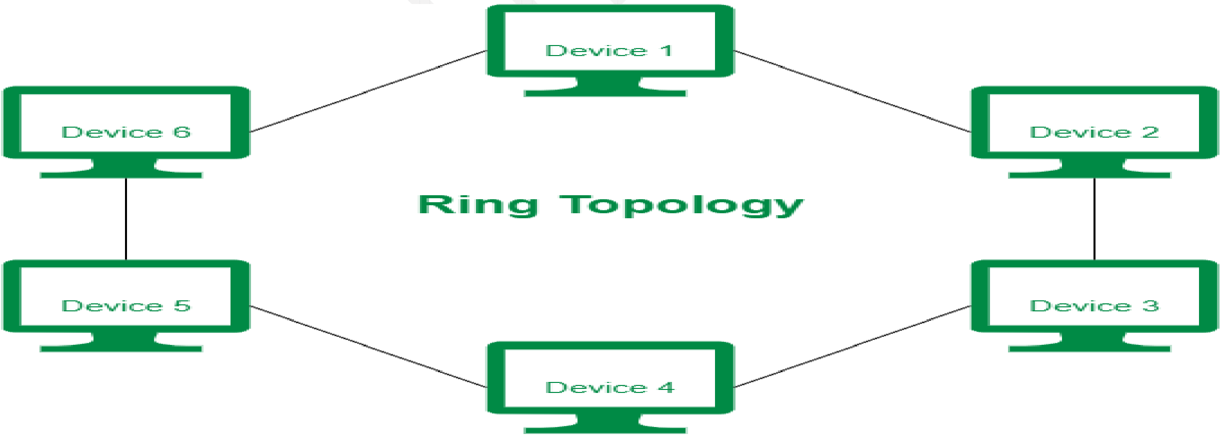


Bus Topology

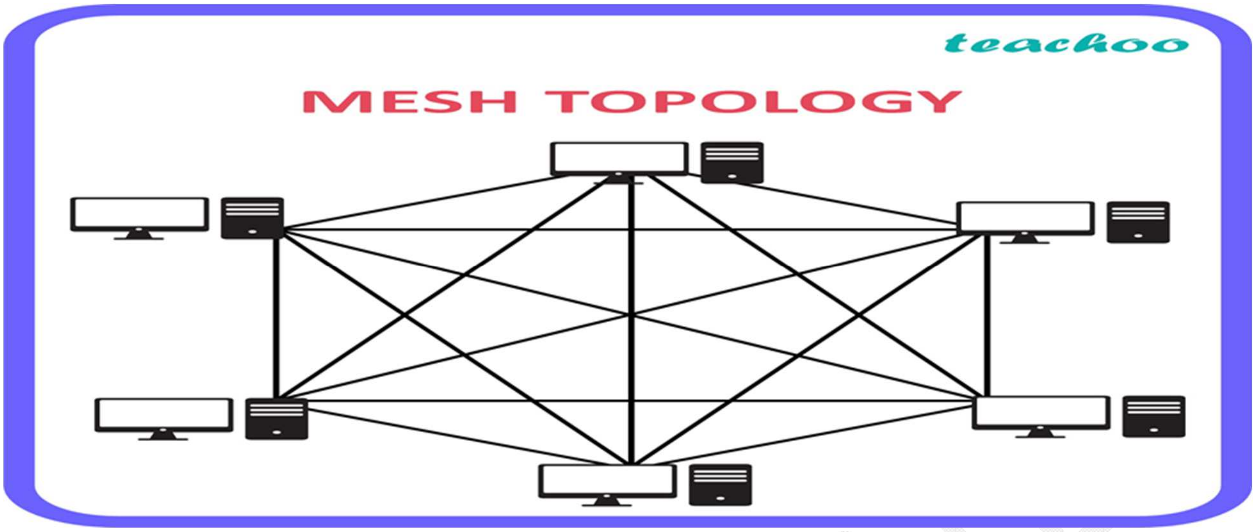
Star topology: In a star topology, all devices are connected to a central hub or switch. Each device has its own cable connecting it to the central hub, which acts as a central point of connection for the network. The main advantage of this topology is that if one device or cable fails, it only affects that device and not the entire network.



Ring topology: In a ring topology, all devices are connected to each other in a circular fashion. Data travels around the ring in one direction, with each device acting as a repeater to boost the signal. The main advantage of this topology is that it can be more reliable than other topologies, but if one device or cable fails it can affect the entire network.

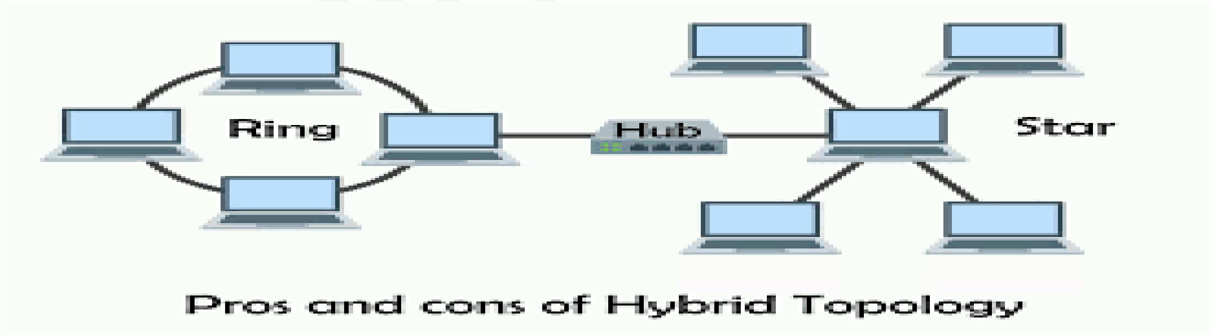


Mesh topology: In a mesh topology, each device is connected to every other device. This topology provides the most reliable and resilient network but is also the most expensive to install and maintain.

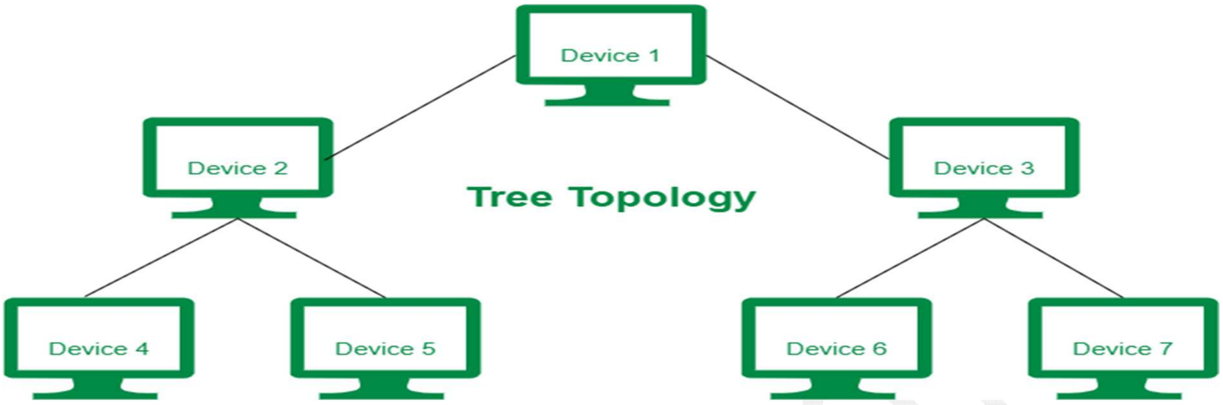


LANs can also use a combination of these topologies

Hybrid Topology: A **hybrid topology** is a combination of two or more different network topologies. It is used to take advantage of the strengths of different topologies while minimizing their weaknesses. For example, a hybrid topology may combine the high fault-tolerance of a ring topology with the high data transfer rates of a bus topology. A common example of a hybrid topology is the star-bus topology, which combines the centralization of a star topology with the broadcast capabilities of a bus topology. Other examples include star-ring, star-mesh, and mesh-bus topologies.



Tree Topology: A tree topology is a type of network topology that is structured like an inverted tree, with a central "root" node (or "root hub") and multiple levels of "branch" nodes branching out from it. The root node typically serves as the central hub of the network, connecting all of the other nodes in the network. Each level of branch nodes typically connects to one or more other levels of branch nodes, forming a hierarchical structure. This topology is commonly used in wide area networks (WANs) and enterprise networks, it is also used in wireless networks. It allows the network to expand and contract easily, it can easily handle the addition of new devices and it is easy to troubleshoot. The disadvantage is that the failure of the root node or a connection to it can cause a large part of the network to fail.



Protocols and Media

Protocols:

A protocol is a set of rules and guidelines that govern the communication between devices on a network. Some common protocols used in Local Area Networks (LANs) include:

Ethernet: A widely used LAN protocol that uses a bus or star topology and supports data transfer rates of 10, 100, and 1000 Mbps.

TCP/IP: The standard protocol suite for the internet, includes the Transmission Control Protocol (TCP) and Internet Protocol (IP).

IPX/SPX: A protocol suite developed by Novell for use in its NetWare operating system.

AppleTalk: A protocol suite developed by Apple for use in Macintosh networks.

Media:

The media refers to the physical means by which data is transmitted between devices on a network. Some common types of media used in LANs include:

Copper cables: Ethernet networks typically use unshielded twisted pair (UTP) or shielded twisted pair (STP) cables to transmit data.

Fiber-optic cables: Fiber-optic cables can be used to transmit data over longer distances and at higher speeds than copper cables.

Wireless: Wireless LANs (WLANs) use radio waves to transmit data between devices, eliminating the need for physical cables.

It's important to note that different protocols and media can be used together to create hybrid networks and can also be used in different combinations depending on the requirements of the network.

Implementing a Local Area Network (LAN) involves several steps, including:

Planning: Before implementing a LAN, it is important to plan out the network's design, including the number of devices that will be connected to the network, the topology that will be used, and the protocols and media that will be employed.

Hardware and software procurement: Once the plan is in place, the necessary hardware and software must be procured. This includes devices such as switches, routers, and servers, as well as network interface cards (NICs) for each device that will be connected to the network.

Installation: The next step is to physically install the hardware, including running cables and connecting devices. This includes configuring the network interface cards (NICs) on each device, connecting devices to switches and routers, and setting up servers.

Configuration: After the installation, the devices and protocols need to be configured. This includes setting IP addresses, configuring routing tables, and setting up security measures such as firewalls and access controls.

Testing: After the configuration, it's important to test the network to ensure that it is functioning properly. This includes testing connectivity between devices, checking for errors and issues, and verifying that data is being transmitted correctly.

Maintenance: Once the LAN is up and running, it is important to maintain it properly. This includes monitoring the network for issues, troubleshooting problems, and performing regular updates and backups.

It's important to note that while these are the general steps involved in implementing a LAN, the specific details may vary depending on the network's size, complexity, and requirements.

Transmission

Transmission refers to the process of sending data from one device to another over a network. In computer networking, data is typically transmitted in the form of packets, which are small units of data that are sent over the network.

There are several different types of transmission methods used in computer networks, including:

Simplex: In simplex transmission, data is transmitted in only one direction. This type of transmission is typically used in devices such as televisions and radios, where the device only needs to receive data and not transmit it.

Half-duplex: In half-duplex transmission, data can be transmitted in both directions, but not at the same time. This type of transmission is typically used in walkie-talkies, where the device can both transmit and receive data, but not simultaneously.

Full-duplex: In a full-duplex transmission, data can be transmitted in both directions simultaneously. This type of transmission is typically used in Ethernet networks, where devices can both transmit and receive data at the same time.

Broadcast: In a broadcast transmission, a single packet of data is sent to all devices on a network. This type of transmission is typically used for network management protocols such as DHCP and ARP.

Different types of transmission methods are better suited for different types of networks and applications. For example, full-duplex transmission is more efficient for high-bandwidth applications such as streaming video, while the simplex transmission is better suited for low-bandwidth applications such as sensor networks.

Access method and Technologies

Access method refers to the method by which devices on a network gain access to the network's resources, such as data and hardware.

There are several different types of access methods used in computer networks, including:

Circuit switching: In circuit switching, a dedicated physical connection, or circuit, is established between the sender and the receiver for the duration of the communication session. This type of access method is typically used in telephone networks.

Packet switching: In packet switching, data is divided into small units called packets, which are sent independently over the network. Each packet is routed to its destination based on its destination address. This type of access method is typically used in data networks such as the internet.

Message switching: In message switching, data is sent in the form of messages, which are stored temporarily at intermediate nodes before being forwarded to their destination. This type of access method is typically used in older data networks.

Token passing: In token passing, a special packet called a token is passed around the network, giving each device the opportunity to transmit data when it holds the token. This type of access method is typically used in Token Ring networks.

Carrier sense multiple access (CSMA): In CSMA, devices on a network listen for a carrier signal before transmitting, to avoid collisions with other devices trying to transmit at the same time. This type of access method is typically used in Ethernet networks.

There are also many technologies that are used in conjunction with these access methods to provide efficient and secure communication across networks, such as:

Transmission Control Protocol/Internet Protocol (TCP/IP)

Special consideration for the Blinds

There are certain special considerations that need to be taken into account when designing and implementing computer networks for the blind. These include:

1. **Accessibility:** Network interfaces and applications need to be designed with accessibility in mind so that they can be easily navigated and used by people who are blind or have low vision. This may include providing keyboard shortcuts, high-contrast displays, and text-to-speech functionality.
2. **Audio feedback:** Audio feedback is an important feature for people who are blind, as it allows them to hear what is happening on the network and navigate it accordingly. This may include providing audio cues for incoming messages and notifications, as well as spoken error messages.

3. **Text-to-speech:** Text-to-speech software is an important tool for people who are blind, as it allows them to hear the contents of text-based documents and websites. This should be integrated into network interfaces and applications to make it easy for users to access and read the information they need.
4. **Touchscreen support:** Some users who are blind may rely on touchscreens to navigate through the network, therefore the network interfaces and applications need to be designed to support touch screens.
5. **Support for screen readers:** Some users who are blind use screen readers, which are software programs that read the contents of the screen aloud. These programs need to be compatible with network interfaces and applications to make them accessible to users who are blind.
6. **Training:** It is important to provide training for people who are blind or have low vision on how to use the network, its interfaces, and applications so that they can make the most of the resources available to them.

It's important to note that these considerations are not only for the blind but also for people with other disabilities and for the Elderly.

Addressing the Internet: DNS

DNS (Domain Name System) is a system used to translate human-friendly domain names, such as "www.example.com", into machine-friendly IP addresses, such as "192.0.2.1". DNS is a critical component of the internet, as it allows users to access websites and other resources using domain names instead of having to remember the IP addresses of each resource.

DNS operates on a hierarchical system, with the top-level domain (TLD) at the root of the hierarchy. TLDs are the last part of a domain name, such as ".com", ".org", or ".gov". Below the TLD, there can be multiple levels of subdomains, such as "www" or "mail" in the domain name "www.example.com".

The process of resolving a domain name to an IP address involves several steps:

1. The user's device sends a query to the local DNS resolver, which is typically provided by the user's Internet Service Provider (ISP).
2. If the local DNS resolver has the IP address for the requested domain name in its cache, it returns the IP address to the user's device.
3. If the local DNS resolver does not have the IP address in its cache, it sends a query to a DNS server that is authoritative for the TLD of the domain name.

4. The authoritative DNS server returns the IP address for the domain name to the local DNS resolver, which in turn returns it to the user's device.

DNS also provides other important functions, such as providing email routing information, and security through DNSSEC, and also allows for load balancing and failover.

The domain name and their organization

A domain name is a unique string of characters that identifies a specific website or resource on the internet. The organization responsible for managing and registering domain names is ICANN (Internet Corporation for Assigned Names and Numbers). ICANN is a non-profit organization that was created in 1998 to oversee the management of IP addresses and domain names on the internet.

ICANN coordinates the assignment of IP addresses and domain names through a system of registries and registrars. Registries are organizations that manage the databases of domain names for specific top-level domains (TLDs), such as .com, .org, and .net. Registrars are companies that are accredited by ICANN to sell domain names to the public.

When a user wants to register a domain name, they would typically go through a registrar, which would then communicate with the appropriate registry to reserve the domain name.

It's important to note that ICANN is not the only organization responsible for managing domain names. There are also country code top-level domains (ccTLDs) that are managed by organizations in different countries, such as .cn (China) and .us (United States). These organizations may have their own policies and procedures for registering domain names within their respective TLDs.

understanding the internet protocols Address

An Internet Protocol (IP) address is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two main functions: identifying the host or network interface and providing the location of the host in the network.

There are two main versions of IP addresses in use today: IPv4 and IPv6.

1. IPv4: IPv4 stands for Internet Protocol version 4. It uses 32-bit addresses, which means that there are a total of 4.3 billion unique IP addresses available. IPv4 addresses are typically represented in a dotted-decimal notation, such as "192.0.2.1".

2. IPv6: IPv6 stands for Internet Protocol version 6. It uses 128-bit addresses, which means that there are a total of 340 undecillion (3.4 x 10^38) unique IP addresses available. IPv6 addresses are typically represented in a colon-separated hexadecimal notation, such as "2001:0db8:85a3:0000:0000:8a2e:0370:7334".

IP addresses play a crucial role in the functioning of the internet by allowing devices to communicate with each other and enabling the routing of data packets across the network. Each device connected to a network must have a unique IP address so that data packets can be correctly directed to the intended recipient.

It's important to note that IP addresses are not permanent, they can change and can be assigned dynamically by DHCP (Dynamic Host Configuration Protocol) or statically by network administrators. Also, the IP addresses can be private or public, private IP addresses are used on a local network while public IP addresses are used on the internet.

Client-server concept, Architecture, and Applications.

The client-server architecture is a model for distributed computing where a central server provides services to multiple clients over a network. In this model, the client is responsible for the user interface and user interaction, while the server is responsible for processing the requests and providing the requested services.

1. **Client:** The client is a device or software application that requests services from the server. Clients can be computers, smartphones, tablets, or other devices that are connected to the network. Clients are typically lightweight and rely on the server to perform complex processing tasks.
2. **Server**: The server is a device or software application that provides services to clients. Servers can be computers, servers, or other devices that are connected to the network. Servers are typically more powerful than clients and are responsible for processing requests and providing the requested services.
3. **Architecture**: The client-server architecture can be divided into three main components: the client, the server, and the network. The client and server communicate through the network, which can be a local area network (LAN), a wide area network (WAN), or the internet.
4. **Applications:** The client-server architecture is used in many different types of applications, including:

- **Web applications**: Websites are accessed by clients using web browsers and the server provides the website content and services.
- **Database systems:** Database servers store and manage data, while clients use database management software to interact with the database.
- **Email systems**: Email clients send and receive messages, while email servers are responsible for managing and storing messages.
- **Remote access systems**: Remote clients use remote access software to connect to servers and access resources remotely.

It's important to note that the client-server architecture is a flexible model, and it can be implemented in different ways, such as in a three-tier architecture, where there is a middle tier that acts as a bridge between the client and the server, or in a peer-to-peer architecture where all devices are both clients and servers.

Getting connected: Items needed to connect to the internet

connect to the internet, there are several items that you will need:

1. **A device:** The device you use to connect to the internet can be a computer, laptop, tablet, smartphone, or another internet-enabled device.
2. **An internet connection:** You will need an internet connection to access the internet. This can be a wired or wireless connection and can be provided by an Internet Service Provider (ISP) through a variety of technologies such as DSL, cable, fiber optic, or satellite.
3. **A modem:** A modem is a device that modulates and demodulates signals to enable communication between your device and the internet. If you have a wired connection, you will need a modem that can connect to the internet via an Ethernet cable. If you have a wireless connection, you will need a modem that can connect to the internet via Wi-Fi.
4. **A router:** If you have a wireless connection, you will need a router to create a wireless network in your home. A router connects to the modem and creates a Wi-Fi network that allows your devices to connect to the internet wirelessly.
5. **An Ethernet cable:** If you have a wired connection, you will need an Ethernet cable to connect your device to the modem or router.
6. **Network interface card (NIC):** A NIC is a hardware component that connects a device to a network and it's sometimes built-in to the device or can be added as an expansion card.

It's important to note that depending on your specific setup and the type of internet connection you have, you may not need all of these items. For example, if you have a wireless connection and your device has built-in Wi-Fi

Levels of connectivity

here are several levels of connectivity that describe the various ways in which devices can connect to the internet:

1. Offline: A device that is offline is not connected to the internet and cannot access online resources or services.
2. Dial-up: Dial-up connectivity uses a telephone line to connect to the internet. It is considered to be one of the slowest forms of internet connectivity.
3. Broadband: Broadband connectivity uses a wired or wireless connection to provide a faster and more reliable internet connection than dial-up. It includes technologies such as DSL, cable, fiber optic, and satellite.
4. Mobile: Mobile connectivity uses cellular networks to connect to the internet. It can be provided through mobile data plans or through Wi-Fi hotspots.
5. High-speed: High-speed connectivity provides faster internet speeds than broadband and is typically used for applications such as streaming video and online gaming.
6. Cloud-based: Cloud-based connectivity refers to the use of internet-based services to store, manage, and process data, rather than storing it on a local device.

It's important to note that the level of connectivity can vary depending on the location and the availability of different technologies. In some areas, only certain types of connectivity may be available, and the quality of the connection can also vary depending on factors such as network congestion and distance from the nearest tower or exchange point.

Some Questions for practice

1. What is the internet?
2. What is the purpose of the internet?
3. How does the internet work?
4. What are the main technologies used for connecting to the internet?
5. What are some common internet protocols?

6. How does the World Wide Web (WWW) function in relation to the internet?
7. What are some of the most popular websites on the internet?
8. What is a search engine and how does it work?
9. What is an IP address and how is it used on the internet?
10. What is a domain name and how is it used on the internet?
11. What is a URL and how is it used on the internet?
12. What are the different types of internet connections?
13. What are some of the potential dangers of using the internet?
14. How has the internet changed over the years?
15. What are the benefits and drawbacks of using the internet?
16. What is the topology of the internet?
17. How is the internet structured?
18. What are the different types of internet network topologies?
19. How does data travel across the internet?
20. What is a router and how does it work in internet networking?
21. What is a switch and how does it work in internet networking?
22. What is a gateway and how does it work in internet networking?
23. What is a network address translator (NAT) and how does it work?
24. What are the different types of internet connections?
25. How does the internet handle high-bandwidth traffic?
26. What are the main protocols used for internet networking?
27. How does the internet handle data encryption and security?
28. What is a virtual private network (VPN) and how does it work?
29. What are the main challenges facing internet network topology today?
30. How does the internet routing works?