1. What are the different types of networks?

There are basically 3 types of networks, each designed for specific purposes and functionalities.

- Local Area Network (LAN): A LAN is a network that is limited to a small geographic area, such as a single building or a campus. It allows connected devices to share resources like files, printers, and internet connections.

- Wide Area Network (WAN): A WAN spans a larger geographic area, connecting multiple LANs. The internet itself is an example of a global WAN. WANs use various technologies, including leased lines, satellites, and public networks.

- Metropolitan Area Network (MAN): A MAN falls between a LAN and WAN in terms of geographic scope, typically covering a city or a large campus. It connects multiple LANs within a specific metropolitan area.

2. Explain the Shielded twisted pair (STP) and Unshielded twisted pair(UTP).

Twisted pair cables are a common type of copper cabling used in network infrastructure for transmitting data. The "twisted pair" refers to the pairs of insulated copper wires that are twisted together. There are two main types of twisted pair cables: Shielded Twisted Pair (STP) and Unshielded Twisted Pair (UTP).

- Unshielded Twisted Pair (UTP):
    - **Construction**: UTP consists of pairs of insulated copper wires twisted together without any additional shielding. Each pair is typically color-coded for identification.
    - **Advantages**:
        - Cost-Effective: UTP is generally less expensive than shielded alternatives.
        - Flexibility: UTP cables are more flexible and easier to install than shielded cables.
        - Common Usage: UTP is widely used in networking environments, such as Ethernet installations.

- Shielded Twisted Pair (STP):
    - **Construction:** STP cables have pairs of insulated copper wires that are twisted together and surrounded by an additional metallic shield, which can be made of foil or braided strands.
    - **Advantages:**

- Improved Protection: The shielding in STP cables helps protect against electromagnetic interference (EMI) and radio-frequency interference (RFI).
- Enhanced Performance: STP cables are often used in environments with high levels of interference, providing better performance in such conditions.
- Longer Transmission Distances: STP cables may have a longer effective transmission distance due to reduced susceptibility to interference.

3. What is difference between baseband and broadband transmission?

S. No	Basis of Comparison	Baseband Transmission	Broadband Transmission
1.	**Type of Signal**	In baseband transmission, the type of signaling used is digital.	In broadband transmission, the type of signaling used is analog.
2.	**Direction Type**	Baseband Transmission is bidirectional in nature.	Broadband Transmission is unidirectional in nature.
3.	**Signal Transmission**	The Signal can be sent in both directions.	Sending of Signal in one direction only.
4.	**Distance covered by the signal**	Signals can only travel over short distances. For long distances, attenuation is required.	Signals can be traveled over long distances without being attenuated.
5.	**Topology**	It works well with bus topology.	It is used with a bus as well as tree topology.
6.	**Device used to increase signal strength**	Repeaters are used to enhance signal strength.	Amplifiers are used to enhance signal strength.
7.	**Type of Multiplexing used**	It utilizes Time Division Multiplexing	It utilizes Frequency Division Multiplexing.

S. No	Basis of Comparison	Baseband Transmission	Broadband Transmission
8.	**Encoding Techniques**	In baseband transmission, Manchester and Differential Manchester encoding are used.	Only PSK encoding is used.
9.	**Transfer medium**	Twisted-pair cables, coaxial cables, and wires are used as a transfer medium for digital signals in baseband transmission.	Broadband signals were sent through optical fiber cables, coaxial cables, and radio waves.
10.	**Impedance**	Baseband transmission has a 50-ohm impedance.	Broadband transmission has a 70-ohm impedance.

4. What is the difference between a hub, modem, router and a switch?

Hubs, modems, routers, and switches are all devices used in computer networks, but they serve different functions. Here's a brief explanation of each:

- **Hub:**
  - **Function**: Hubs are simple networking devices that operate at the physical layer (Layer 1) of the OSI model. They connect multiple devices in a network, but they do not differentiate between devices or manage data traffic. When a hub receives data on one port, it broadcasts it to all other ports.
  - **Characteristic**: Hubs are considered outdated and less efficient compared to other devices due to their inability to intelligently manage network traffic.

- **Modem:**
  - **Function:** A modem (modulator-demodulator) is a device that modulates and demodulates analog signals to enable digital data transmission over analog communication lines, such as telephone lines or cable systems. Modems are commonly used to connect to the internet via DSL or cable connections.
  - **Characteristic:** Modems are essential for converting digital data from computers into analog signals for transmission over analog lines and vice versa.

- **Router:**
  - **Function:** Routers operate at the network layer (Layer 3) of the OSI model. They connect different networks and make decisions about where to send data

packets based on IP addresses. Routers help direct data between devices on a local network and devices on other networks, including the internet.
    - **Characteristic:** Routers provide network address translation (NAT), firewall capabilities, and typically have multiple ports for connecting devices.

- **Switch:**
    - **Function:** A switch operates at the data link layer (Layer 2) of the OSI model. It connects multiple devices within a local area network (LAN) and uses MAC addresses to forward data only to the specific device intended to receive it. Unlike hubs, switches are more efficient in managing network traffic because they create dedicated paths between connected devices.
    - **Characteristic:** Switches are commonly used in modern networks to improve performance and reduce collisions compared to traditional hubs.

5. When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?

When you move a Network Interface Card (NIC) from one PC to another, the MAC (Media Access Control) address does not get transferred. The MAC address is a unique identifier assigned to the NIC by the manufacturer, and it is typically hardcoded into the NIC's hardware.

When you move the NIC to a different computer, the MAC address remains associated with the original NIC. The new computer will recognize the presence of the NIC, but it will continue to use the MAC address assigned to that NIC by the manufacturer. The MAC address is not altered or transferred when you physically move the NIC to another machine.

It's worth noting that some NICs allow for the modification of their MAC addresses through software configuration, but this is a separate process and is not automatically transferred when moving the physical card to a different computer.

6. When troubleshooting computer network problems, what common hardware-related problems can occur?

When troubleshooting computer network problems, various hardware-related issues may contribute to connectivity or performance issues. Here are some common hardware-related problems to consider:

- **Faulty Cables:**
    - Symptoms: Intermittent connectivity, slow network speeds, or complete network failure.

- Solution: Inspect cables for physical damage, replace damaged cables, and ensure proper cable termination.

- **Network Interface Card (NIC) Issues:**
  - Symptoms: No network connectivity, slow performance, or intermittent connectivity.
  - Solution: Check for driver issues, update NIC drivers, try using a different NIC or reinstall the NIC drivers.

- **Switch or Hub Problems:**
  - Symptoms: Devices unable to communicate, slow network speeds, or intermittent connectivity.
  - Solution: Check for physical damage, verify power and connectivity to the switch or hub, replace if necessary.

- **Router Issues:**
  - Symptoms: Internet connectivity problems, difficulty accessing specific websites, or intermittent connectivity.
  - Solution: Check router configuration, power cycle the router, update firmware, and inspect for hardware failures.

- **Modem Problems:**
  - Symptoms: Internet connection issues, no connectivity, or slow speeds.
  - Solution: Verify connections, power cycle the modem, check for service provider issues, and replace the modem if necessary.

- **Power Supply Problems:**
  - Symptoms: Unstable or unreliable network operation, sudden network failures.
  - Solution: Verify power sources, replace faulty power supplies, and check for issues with power distribution.

7. In a network that contains two servers and twenty workstations, where is the best place to install an Anti-virus program?

The best place to install an antivirus program in a network that contains two servers and twenty workstations is on each of the individual workstations. Installing the antivirus software on the workstations offers several advantages:

- **Localized Protection:**

Reasoning: Workstations are the primary endpoints where users interact with the network and can be exposed to various sources of malware. Installing antivirus software on each workstation ensures that these devices are protected from potential threats.

- **Immediate Threat Detection:**

Reasoning: Workstations are more likely to encounter external devices, files, and network connections. By having antivirus protection on individual workstations, threats can be detected and addressed immediately, reducing the risk of spreading malware across the network.

- **Resource Efficiency:**

Reasoning: Servers typically have specific roles and responsibilities in managing network resources and services. Installing antivirus software on servers may consume unnecessary resources and impact their performance. By focusing antivirus protection on workstations, you optimize resource usage for each device's specific function.

- **Centralized Management:**

Reasoning: Most modern antivirus solutions offer centralized management consoles, allowing administrators to monitor and manage antivirus activities centrally. This approach provides efficient control over the antivirus software deployed on individual workstations without the need to install it on servers.

- **Isolation of Threats:**

Reasoning: Workstations are more likely to encounter threats through user interactions, email attachments, or removable media. Isolating antivirus protection to workstations ensures that threats are contained at the endpoint, minimizing the potential impact on critical server functions.

8. Define Static IP and Dynamic IP? Discuss the difference between IPV4 and IPV6.

Static IP (Internet Protocol):

- Definition: A static IP address is a fixed, permanent IP address assigned to a device on a network. It does not change over time and remains constant.
- Usage: Static IPs are often used for devices that need a consistent and easily identifiable address, such as servers, printers, and network devices.

Dynamic IP (Internet Protocol):

- Definition: A dynamic IP address is one that is assigned to a device temporarily by a DHCP (Dynamic Host Configuration Protocol) server. It can change over time as devices connect and disconnect from the network.
- Usage: Dynamic IPs are commonly used for devices like computers, smartphones, and other end-user devices. They are suitable for scenarios where devices don't need a permanent, fixed address.

Differences between IPv4 and IPv6:

- ✓ **Address Length:** IPv4 addresses are 32 bits long, while IPv6 addresses are 128 bits long.
- ✓ **Address Notation:** IPv4 addresses use dotted-decimal notation, whereas IPv6 addresses use hexadecimal notation separated by colons.
- ✓ **Address Space:** IPv4 has a limited address space, leading to address exhaustion. IPv6 provides an immensely larger address space to accommodate the growing number of devices on the internet.
- ✓ **Configuration:** IPv4 addresses can be configured statically or dynamically. IPv6 is designed with stateless address auto configuration, allowing devices to generate their addresses or use DHCPv6.
- ✓ **Broadcasting:** IPv4 uses broadcast for communication to all devices on a network segment, while IPv6 uses multicast and any cast.
- ✓ **NAT (Network Address Translation):** NAT is commonly used in IPv4 to address the shortage of public IP addresses. IPv6 has a large enough address space to minimize the need for NAT.

9. Discuss TCP/IP model in detail.

The TCP/IP model, also known as the Internet protocol suite, is a conceptual framework used to understand and describe the functions of networking protocols in computer networks. It consists of four layers, each responsible for specific aspects of network communication. The layers, from the bottom to the top, are:

Link Layer (or Network Interface Layer):

- ✓ Function: The link layer deals with the physical connection between devices on the same network. It is responsible for transmitting raw bits over a physical medium and handles issues like addressing, framing, and error detection at the data link level.
- ✓ Protocols: Ethernet, Wi-Fi, PPP (Point-to-Point Protocol), and others.

Internet Layer:

- ✓ Function: The internet layer focuses on routing and forwarding packets between different networks. It enables communication between devices on different subnets by using logical addressing (IP addresses). Additionally, it handles fragmentation and reassembly of data packets.
- ✓ Protocols: IP (Internet Protocol), ICMP (Internet Control Message Protocol), and IGMP (Internet Group Management Protocol).

Transport Layer:

- ✓ Function: The transport layer provides end-to-end communication between devices on different hosts. It ensures data reliability, flow control, and error recovery. Two primary transport layer protocols are TCP (Transmission Control Protocol) for reliable

and connection-oriented communication and UDP (User Datagram Protocol) for connectionless and lightweight communication.

- ✓ Protocols: TCP, UDP.

Application Layer:

- ✓ Function: The application layer is the topmost layer, responsible for providing network services directly to end-users and applications. It includes various protocols and services for tasks such as file transfer, email, remote login, and web browsing.
- ✓ Protocols: HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System), and others.

The TCP/IP model has become the foundation for the design and implementation of the modern internet. It is widely used, and its protocols are the basis for communication in a variety of network environments, including local area networks (LANs) and the global internet.

10. What is a Web Browser (Browser)? Give some example of browsers.

A web browser, often referred to simply as a "browser," is a software application that allows users to access and navigate the World Wide Web. Browsers interpret and display web content, including text, images, videos, and other multimedia elements. Users interact with web browsers to view websites, download files, and access various online services.

Key functions of web browsers include:

Rendering HTML: Browsers interpret HTML (Hypertext Markup Language) and CSS (Cascading Style Sheets) to display web pages with text, images, and formatting.

Executing JavaScript: Browsers execute JavaScript code embedded in web pages, enabling dynamic and interactive features.

Managing URLs (Uniform Resource Locators): Browsers handle URL input, allowing users to navigate to specific websites and web pages.

Some popular web browsers include:

Google Chrome: Developed by Google, Chrome is known for its speed, simplicity, and strong support for web standards. It is available for multiple platforms, including Windows, macOS, Linux, Android, and iOS.

Mozilla Firefox: An open-source browser developed by the Mozilla Foundation. Firefox emphasizes speed, privacy, and customization. It is available for various operating systems.

Microsoft Edge: Developed by Microsoft, Edge is the default browser in Windows 10 and is based on the Chromium engine (the same engine that powers Google Chrome).

Apple Safari: The default browser for Apple devices, including macOS, iOS, and iPadOS. Safari is known for its performance and integration with the Apple ecosystem.

Opera: A feature-rich browser that includes built-in ad-blocking, VPN functionality, and a customizable interface. Opera is available for multiple platforms.

Brave: A privacy-focused browser that blocks ads and trackers by default. Brave aims to provide a faster and more secure browsing experience. It is available for various platforms.

Vivaldi: A highly customizable browser designed for power users. Vivaldi allows users to personalize their browsing experience with a range of features. It is available for Windows, macOS, Linux, and Android.

11. What is a search engine? Give example.

A search engine is a software program or online service that allows users to search for information on the internet by entering specific keywords, phrases, or queries. The search engine then returns a list of results, typically in the form of links to web pages, documents, images, videos, or other types of content that are relevant to the user's query. Search engines play a crucial role in helping users find information efficiently on the vast and diverse World Wide Web.

Key functions of search engines include:

Crawling: Search engines use automated programs called spiders or bots to crawl and index web pages across the internet. These bots follow links on websites, collecting information about the content on each page.

Indexing: The collected information is organized and stored in a searchable index. This index is like a massive catalog that allows the search engine to quickly retrieve relevant results when users enter queries.

Ranking: Search engines use algorithms to rank the indexed pages based on relevance to a user's query. Pages with higher relevance are typically displayed higher in the search results.

Retrieval: When a user submits a search query, the search engine retrieves the most relevant results from its index and presents them to the user in a list.

Example of search engines include:

Google: Google is the most widely used search engine globally, known for its speed, accuracy, and sophisticated algorithms. It is the default search engine for many internet users.

Bing: Developed by Microsoft, Bing is another popular search engine that provides web search, image search, video search, and other features.

Yahoo: Yahoo Search is a search engine powered by Bing. It offers web search, image search, and various other search services.

DuckDuckGo: DuckDuckGo emphasizes privacy and does not track users' search history. It provides anonymous searching and has gained popularity among users concerned about privacy.

Baidu: Baidu is the leading search engine in China, providing web search, image search, and other services.

Yandex: Yandex is a Russian search engine that offers web search, image search, news, and other services.

12. What is the Internet & WWW? What are the uses of internet in our daily life?

Internet:
The internet is a global network of interconnected computers and computer networks that use standardized communication protocols to transmit data. It is a vast network infrastructure that enables the exchange of information and communication among users worldwide. The internet allows for the transfer of data in various forms, including text, images, videos, and more.

World Wide Web (WWW):
The World Wide Web (WWW or simply the web) is a system of interlinked hypertext documents and multimedia content that is accessed via the internet using web browsers. It provides a user-friendly interface for navigating and accessing information on the internet. The WWW is a subset of the broader internet and is a crucial component of how people interact with online content.

Uses of Internet in Daily Life:

Information Retrieval: The internet is a vast repository of information on almost every conceivable topic. Users can access websites, online encyclopedias, news sources, and educational resources for information retrieval.

Communication: Email, instant messaging, and social media platforms enable real-time communication with friends, family, and colleagues, regardless of geographical distances.

Online Shopping: E-commerce platforms allow users to browse, purchase, and sell goods and services online. Online shopping provides convenience and access to a wide range of products.

Entertainment: Streaming services, online gaming, and social media platforms offer a variety of entertainment options. Users can watch movies, listen to music, play games, and engage with online content.

Education: The internet facilitates online learning through educational websites, virtual classrooms, and e-learning platforms. Students can access resources, attend classes, and collaborate with peers globally.

Work and Business: The internet has transformed the way business is conducted. Companies use online platforms for communication, collaboration, marketing, and e-commerce. Remote work and virtual meetings have become more prevalent.

Social Networking: Social media platforms allow users to connect, share updates, and communicate with a broader audience. They serve as a means of social interaction and information dissemination.

Travel and Navigation: The internet provides tools for travel planning, booking flights, hotels, and finding directions. Navigation apps help users navigate unfamiliar locations.

Banking and Finance: Online banking enables users to check account balances, transfer funds, pay bills, and conduct financial transactions from the convenience of their devices.

File Sharing and Cloud Services: Cloud storage and file-sharing services allow users to store, access, and share documents and media files from various devices.

13. What is an Internet Service Provider? Give some example of ISP in India.

An Internet Service Provider (ISP) is a company or organization that provides internet access to users. ISPs offer various types of internet connectivity services, allowing individuals, businesses, and institutions to connect to the internet. ISPs play a crucial role in enabling users to access online content, communicate, and utilize internet-based services.

In India, there are several ISPs that offer internet services to a wide range of users. Here are some examples of ISPs in India:

BSNL (Bharat Sanchar Nigam Limited): BSNL is a government-owned telecommunications company in India that provides broadband and mobile services across the country. It is one of the largest ISPs in India.

Airtel (Bharti Airtel): Bharti Airtel is a major telecommunications company in India that offers broadband services along with mobile and digital TV services. Airtel is known for its widespread network coverage.

Jio Fiber (Reliance Jio): Reliance Jio is a telecommunications company in India that offers high-speed fiber-optic broadband services under the brand Jio Fiber. Jio is also known for its 4G mobile network services.

Hathway: Hathway is a popular ISP in India that offers broadband services, cable TV, and digital TV services. They provide internet services in multiple cities.

14. Discuss the difference between MAC address, IP address and Port address

MAC address, IP address, and port address are three distinct identifiers used in networking to facilitate communication between devices. Each serves a specific purpose in the context of data transmission and network connectivity.

MAC Address (Media Access Control Address):
Purpose: A MAC address is a unique hardware address assigned to a network interface card (NIC) or network adapter. It serves as a physical identifier for devices within a local network.
Format: MAC addresses are 48 bits (or 6 bytes) long and typically expressed as a series of hexadecimal digits separated by colons or dashes (e.g., 00:1A:2B:3C:4D:5E).

IP Address (Internet Protocol Address):
Purpose: An IP address is a logical address assigned to devices on a network to identify and locate them. It allows for communication between devices across different networks.
Format: IPv4 addresses are 32 bits (4 bytes) long, expressed in dotted-decimal format (e.g., 192.168.1.1). IPv6 addresses are 128 bits (16 bytes) long and use hexadecimal notation.

Port Address:

Purpose: A port address is a numerical identifier that helps distinguish different services or applications running on a device. It allows multiple processes to coexist on the same device and share the same IP address.

Format: Port numbers are 16 bits (2 bytes) long, ranging from 0 to 65535. They are specified as part of the transport layer protocol (TCP or UDP).

Key Differences:

Scope: MAC addresses are used for communication within a local network, while IP addresses facilitate communication between devices across different networks.

Layer of Operation: MAC addresses operate at the data link layer, IP addresses at the network layer, and port addresses at the transport layer.

Length and Format: MAC addresses are 48 bits in length, while IP addresses are 32 bits (IPv4) or 128 bits (IPv6). Port addresses are 16 bits.

Uniqueness: MAC addresses are globally unique, while IP addresses should be unique within a network. Port numbers are unique within the context of a specific IP address.

Assignment: MAC addresses are typically assigned by the device's manufacturer, IP addresses can be assigned statically or dynamically, and port numbers are specified by the application or protocol.

15. How do we view my Internet browser's history?

The process of viewing your internet browser's history may vary slightly depending on the browser you are using. Here are general instructions for popular web browsers:

Google Chrome:

1. Open Google Chrome.
2. Press `Ctrl + H` (Windows/Linux) or `Command + Y` (Mac) to open the History page directly.
   - Alternatively, click on the three vertical dots in the top-right corner, go to "History," and select "History" from the menu.
3. The History page will show a list of visited websites organized by date and time.

Mozilla Firefox:

1. Open Mozilla Firefox.
2. Press `Ctrl + H` (Windows/Linux) or `Command + Shift + H` (Mac) to open the Library window.
   - Alternatively, click on the three horizontal lines in the top-right corner, go to "History," and select "Show All History."
3. The Library window will display your browsing history, organized by date and site.

Microsoft Edge:

1. Open Microsoft Edge.
2. Press `Ctrl + H` (Windows/Linux) to open the History pane.

- Alternatively, click on the three horizontal dots in the top-right corner, go to "History," and select "History."
3. The History pane will show your browsing history.

Safari:
1. Open Safari.
2. Press `Command + Y` to open the History page.
- Alternatively, click on the clock icon in the top-left corner to access the History page.
3. The History page will display your visited sites.