1. What are the different types of networks?

1. Personal Area Network (PAN)

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

2. Local Area Network (LAN)

We're confident that you've heard of these types of networks before – LANs are the most frequently discussed networks, one of the most common, one of the most original and one of the simplest types of networks. LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs.

Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidly and safely transfer data.

3. Wireless Local Area Network (WLAN)

Functioning like a LAN, WLANs make use of wireless network technology, such as Wi-Fi. Typically seen in the same types of applications as LANs, these types of networks don't require that devices rely on physical cables to connect to the network.

4. Campus Area Network (CAN)

Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large K-12 school districts or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.

5. Metropolitan Area Network (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either a single person or company (a local council, a large company, etc.).

6. Wide Area Network (WAN)

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're miles apart.

The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN's vast reach, it is typically owned and maintained by multiple administrators or the public.

7. Storage-Area Network (SAN)

As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don't rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network. SANs can be accessed in the same fashion as a drive attached to a server. Types of storage-area networks include converged, virtual and unified SANs.

8. System-Area Network (also known as SAN)

This term is fairly new within the past two decades. It is used to explain a relatively local network that is designed to provide high-speed connection in server-to-server applications (cluster environments), storage area networks (called "SANs" as well) and processor-to-processor applications. The computers connected on a SAN operate as a single system at very high speeds.

9. Passive Optical Local Area Network (POLAN)

As an alternative to traditional switch-based Ethernet LANs, POLAN technology can be integrated into structured cabling to overcome concerns about supporting traditional Ethernet protocols and network applications such as PoE (Power over Ethernet). A point-to-multipoint LAN architecture, POLAN uses optical splitters to split an optical signal from one strand of singlemode optical fiber into multiple signals to serve users and devices.

10. Enterprise Private Network (EPN)

These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.

11. Virtual Private Network (VPN)

By extending a private network across the Internet, a VPN lets its users send and receive data as if their devices were connected to the private network – even if they're not. Through a virtual point-to-point connection, users can access a private network remotely.

2. Explain the shielded twisted pair (STP) and unshielded twisted pair (USTP)

.NO	UTP	STP
1.	UTP stands for Unshielded twisted pair.	STP stands for Shielded twisted pair.
2.	In UTP grounding cable is not necessary.	While in STP grounding cable is required.
3.	Data rate in UTP is slow compared to STP.	Data rate in STP is high.
4.	The cost of UTP is less.	While STP is costlier than UTP.
5.	In UTP much more maintenance are not needed.	While in STP much more maintenance are needed.
6.	In UTP noise is high compared to STP.	While in STP noise is less.
7.	In UTP the generation of crosstalk is also high compared to STP.	While in STP generation of crosstalk is also less.
8.	In UTP, attenuation is high in comparison to STP.	While in STP attenuation is low.
9.	In UTP, speed offered is about 10 to up to 1000 Mbps.	While in STP speed offered is about 10 to up to 100 Mbps.
10.	It is used for data transmission within short distance such as for home and office networks.	Generally used for connecting organizations over a long distance.

3. What is difference between baseband and broadband transmission ?

	Baseband Transmission	Broadband Transmission
1.	In baseband transmission, the type of signalling used is digital.	In broadband transmission, the type of signalling used is analog.
2.	Baseband Transmission is bidirectional in nature.	Broadband Transmission is unidirectional in nature.
3.	Signals can only travel over short distances.	Signals can be travelled over long distances without being attenuated.
4.	It works well with bus topology.	It is used with a bus as well as tree topology.
5.	In baseband transmission, Manchester and Differential Manchester encoding are used.	Only PSK encoding is used.
6.	Baseband transmission have 50 ohm impedance.	Broadband transmission have 70 ohm impedance.

7.	Baseband transmission is easy to install and maintain.	Broadband transmission is difficult to install and maintain.
8.	This transmission is cheaper to design.	This transmission is expensive to design.

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

Hub	Switch	Router
1.	Hub is a physical layer device i.e. layer 1.	Switch is a data link layer device i.e. layer 2.	Router is a network layer device i.e. layer 3.
2.	A Hub works on the basis of broadcasting.	Switch works on the basis of MAC address.	A router works on the basis of IP address.
3.	A Hub is a multiport repeater in which a signal introduced at the input of any port appears at the output of the all available ports.	A Switch is a tele-communication device which receives a message from any device connected to it and then transmits the message only to the device for which the message is intended.	A router reads the header of incoming packet and forward it to the port for which it is intended there by determines the route. It can also perform filtering and encapsulation.
4.	Hub is not an intelligent device that may include amplifier on repeater.	A Switch is an intelligent device as it passes on the message to the selective device by inspecting the address.	A route is more sophisticated and intelligent device as it can read IP address and direct the packets to another network with specified IP address. Moreover routers can built address tables that helps in routing decisions.

	Hub	Switch	Router
5.	At least single network is required to connect.	At least single network is required to connect.	Router needs at least two networks to connect.
6.	Hub is cheaper as compared to switch and router.	Switch is an expensive device than hub.	Router is a relatively much more expensive device than hub and switch.

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

Just like each house has it's own postal address, every device connected on a network has a Media Access Control (MAC) address, that uniquely identifies it. The MAC address is tied to the Network Interface Controller (NIC), a subcomponent of the larger device.

6**. When troubleshooting computer network problems, what common hardware – related problems an occur?**

When troubleshooting computer network problems, what common hardware-related problems can occur? A large percentage of a network is made up of hardware. Problems in these areas can range from malfunctioning hard drives, broken NICs, and even hardware startups.

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

In a network that contains two servers and twenty workstations, where is the best place to install an Anti-virus program? The best solution is to install anti-virus on all the computers in the network.

Putting antivirus software on an Internet border device, whether the device is an email server or firewall, is the next best option. In today's world of email worms, Trojan horses, and infected Web pages, placing virus-scanning protection at the border offers excellent benefits for the cost.

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

Static IP address is provided by Internet Service Provider and remains fixed till the system is connected to the network. Dynamic IP address is provided by DHCP, generally a company gets a single

static IP address and then generates the dynamic IP address for its computers within the organization's network.

The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

9. Discuss the TCP/ IP in model detail.

TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.

10. What is the web Browser (Browser)? Give soe examples of some browsers.

A web browser, or simply 'browser,' is an application used to access and view websites. Common web browsers include

EXAMPLES

Microsoft Edge, Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

11. What is a search engine? Give examples.

A search engine is a web-based tool that enables users to locate information on the Popular.

EXAMPLES

Google, Yahoo!, and MSN Search.

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

The Internet is a vast network that connects computers all over the world. Through the Internet, people can share information and communicate from anywhere with an Internet connection.

The Internet carries many applications and services, most prominently the World Wide Web, including social media, electronic mail, mobile applications, multiplayer online games, Internet telephony, file sharing, and streaming media services.

13. What is an internet service provider? Give some examples of ISP in india.

The examples of some internet service providers are Hathway, BSNL, Tata teleservices, Verizon, Reliance Jio, ACT Fibernet and many more working in India as well as worldwide. Internet service providers or ISPs are responsible for providing services for using the Internet.

SPs use fiber-optics, satellite, copper wire, and other forms to provide Internet access to its customers.

14. Discuss the difference between MAC address, IP address and port address?

S.No	MAC Address	IP Address
1.	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
2.	MAC Address is a six byte hexadecimal address.	IP Address is either a four-byte (IPv4) or a sixteen-byte (IPv6) address.
3.	A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
4.	NIC Card's Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.
5.	MAC Address is used to ensure the physical address of a computer.	IP Address is the logical address of the computer.
6.	MAC Address operates in the data link layer.	IP Address operates in the network layer.
7.	MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.
8.	MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.
9.	MAC Addresses can't be found easily by a third party.	IP Addresses can be found by a third party.
10.	It is a 48-bit address that contains 6 groups of 2 hexadecimal digits, separated by either hyphens (-) or colons(.). Example: 00:FF:FF:AB:BB:AA	IPv4 uses 32-bit addresses in dotted notations, whereas IPv6 uses 128-bit addresses in hexadecimal notations. Example: IPv4 192.168.1.1 IPv6 FFFF:F200:3204:0B00

S.No	MAC Address	IP Address
	or 00-FF-FF-AB-BB-AA	
11.	No classes are used for MAC addressing.	IPv4 uses A, B, C, D, and E classes for IP addressing.
12.	MAC Address sharing is not allowed.	In IP address multiple client devices can share the IP address.

15. How do we view my internet browser's History?

On your Android phone or tablet, open the Chrome app

1. At the top right, tap More > History.
    - If your address bar is at the bottom, swipe up on the address bar. Tap History .
2. To visit a site, tap the entry.
    - To open the site in a new tab, touch and hold the entry. At the top right, tap More > Open in new tab.
    - To copy the site, touch and hold the entry. At the top right, tap More .