1. types of networks

1. Personal area network. A personal area network (PAN) is the smallest and simplest type of network. ...

2. Local area network.

3. Metropolitan area network.

4.Campus network.

5. Wide area network.

6.Content delivery network.

7.Virtual private network.

2.

Shielded twisted pair STP

Shielded twisted pair (STP) is a special kind of copper telephone and local area network (LAN) wiring used in some business installations. It adds an outer covering or shield that functions as a ground to ordinary twisted pair wiring. Twisted pair is the ordinary copper wire that connects many computer networks to the telephone company. To reduce cross-talk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Each signal on twisted pair requires both wires.

Unlike unshielded twisted pair (UTP), shielded twisted pair also encloses these wires in a shield and grounds them to further reduce electromagnetic and radio frequency interference. STP cables are more expensive and harder to install than UTP wiring.

Unshielded twisted pair cables.

The word unshielded in UTP refers to the lack of metallic shielding around the copper wires. By its nature, the twisted-pair design helps minimize electronic interference by providing balanced signal transmission, making a physical shield unnecessary. The copper conductor of both horizontal and backbone UTP cables are either 22 AWG or 24 AWG. 24 AWG is the most common size, but higher-performance cables like Category 6 UTP employ the larger 23 AWG copper wires.

3.Difference between Broadband and Baseband Transmission

Broadband systems use modulation techniques to reduce the effect of noise in the environment. Broadband transmission employs multiple channel unidirectional transmission using a combination of phase and amplitude modulation.

Baseband is a digital signal transmitted on the medium using one of the signal codes like NRZ, RZ Manchester biphase-M code, etc. called baseband transmission.

These are the following differences between Broadband and Baseband transmission.

Baseband transmission:

Digital signaling.

Frequency division multiplexing is not possible.

Baseband is the bi-directional transmission.

A short-distance signal traveling.

The entire bandwidth is for single signal transmission.

Example: Ethernet is using Basebands for LAN.

Broadband transmission:

Analog signaling.

The transmission of data is unidirectional.

Signal traveling distance is long.

Frequency division multiplexing is possible.

Simultaneous transmission of multiple signals over different frequencies.

Example: Used to transmit cable TV to premises.

4. Difference between a hub, modem, router and a switch?

A switch is a multicast networking device that works under the Datalink layer of the OSI model and connects a bunch of computers or devices in a network. It's mainly used to send a private message and it does not waste data.

A switch can easily identify which device is connected to which port by using a MAC

address giving it the ability to deliver the message to a particular machine.

Advantages of using a Switch

It's secure since it delivers data to the specified node.

It lowers the chances of frame collisions domains.

It increases the bandwidth in a network.

It increases the number of ports needed to connect the nodes available in a network.

It operates under full-duplex.

Disadvantages of using Switches

They are more expensive compared to hubs and other devices used in a network.

To deal with multicast parcels, proper planning is required.

Problems may arise when broadcasting traffic.

Advantages of using hubs

They have the ability to connect to the network using different physical media.

They can be used to increase the network distance.

Hubs are relatively cheap compared to switches and other devices in the network.

Disadvantages of using a hub

It increases the chances of collision domains between packets when being transferred from one device to another.

Hubs operate under half-duplex. Only one device can send or receive data at a time

Hubs share data to all the devices in a network thus making the network insecure.

Hubs waste lots of bandwidth when transmitting data.

Switch vs Hub

A Hub is a broadcast device that sends data from one node to all nodes but a Switch is a multicast device that can send data to a particular node.

A Hub supports half-duplex i.e., only one device can send or receive data at a time while a switch supports full-duplex i.e., both devices can send and receive data at the same time.

A switch is located on the second layer of the OSI model while a Hub is located on the first layer.

5.
that's because MAC addresses are hard-wired into the NIC circuitry, not the PC. This also means that a PC can have a different MAC address when the NIC card was replace by another one.

6.
Some network problems can arise from faulty hardware, such as routers, switches, firewalls, and even from unexpected usage patterns, like network bandwidth spikes, changes in app configuration, or security breaches.

7.
You need AT LEAST three levels of security.

A good firewall. This can stop intrusions, malware, unauthorized access, etc. before they reach the workstations.
Antivirus software on the servers and at the endpoint workstations. This software should be centrally managed to keep end users updated constantly and to minimize user meddling with the settings. Good antivirus will also protect email clients. Educated and aware users who: do not casually install downloaded programs; don't click on unknown links; don't fall for phishing emails, etc. Establish a strong password policy for all users. You should consider not giving your users Administrative rights on their accounts. They will complain that they cannot install what they need and your workload will increase but, I guarantee you, your entire environment will be more reliable and secure.

8.
Static IP address is provided by the Internet Service Provider and remains fixed till the system is connected to the network. Dynamic IP address is provided by the

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

9.

The main work of TCP/IP is to transfer the data of a computer from one device to another. The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end.

Difference between TCP and IP

TCP and IP are different protocols of Computer Networks. The basic difference between TCP (Transmission Control Protocol) and IP (Internet Protocol) is in the transmission of data. In simple words, IP finds the destination of the mail and TCP has the work to send and receive the mail. UDP is another protocol, which does not require IP to communicate with another computer. IP is required by only TCP. This is the basic difference between TCP and IP.

Whenever we want to send something over the internet using the TCP/IP Model, the TCP/IP Model divides the data into packets at the sender's end and the same packets have to be recombined at the receiver's end to form the same data, and this thing happens to maintain the accuracy of the data. TCP/IP model divides the data into a 4-layer procedure, where the data first go into this layer in one order and again in reverse order to get organized in the same way at the receiver's end.

1. Physical Layer

It is a group of applications requiring network communications. This layer is responsible for generating the data and requesting connections. It acts on behalf of the sender and the Network Access layer on the behalf of the receiver. During

this article, we will be talking on the behalf of the receiver.

2. Data Link Layer

The packet's network protocol type, in this case, TCP/IP, is identified by the data-link layer. Error prevention and "framing" are also provided by the data-link layer. Point-to-Point Protocol (PPP) framing and Ethernet IEEE 802.2 framing are two examples of data-link layer protocols.

3. Internet Layer

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for the logical transmission of data over the entire network. The main protocols residing at this layer are as follows:

IP: IP stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.
ICMP: ICMP stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
ARP: ARP stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP.The Internet Layer is a layer in the Internet Protocol (IP) suite, which is the set of protocols that define the Internet. The Internet Layer is responsible for routing packets of data from one device to another across a network. It does this by assigning each device a unique IP address, which is used to identify the device and determine the route that packets should take to reach it.

Example: Imagine that you are using a computer to send an email to a friend.

When you click "send," the email is broken down into smaller packets of data, which are then sent to the Internet Layer for routing. The Internet Layer assigns an IP address to each packet and uses routing tables to determine the best route for the packet to take to reach its destination. The packet is then forwarded to the next hop on its route until it reaches its destination. When all of the packets have been delivered, your friend's computer can reassemble them into the original email message.

10.

A web browser is a type of software that allows you to find and view websites on the Internet. Even if you didn't know it, you're using a web browser right now to read this page! There are many different web browsers, but some of the most common ones include Google Chrome, Safari, and Mozilla Firefox. The first web browser WorldWideWeb was invented in the year of 1990 by Tim Berners-Lee. Later, it becomes Nexus. In the year of 1993, a new browser Mosaic was invented by Mark Andreessen and their team. It was the first browser to display text and images at a time on the device screen. He also invents another browser Netscape in 1994. Next year Microsoft launched a web browser Internet Explorer which was already installed in the Windows operating system. After this many browsers were invented with various features like Mozilla Firefox, Google Chrome, Safari, Opera, etc.
Here is a list of 7 popular web browsers:

Google Chrome: Developed by Google, Chrome is one of the most widely-used web browsers in the world, known for its speed and simplicity.
Mozilla Firefox: Developed by the Mozilla Foundation, Firefox is an open-source browser that is known for its privacy features and customization options.
Apple Safari: Developed by Apple, Safari is the default browser on Mac and iOS devices and is known for its speed and integration with other Apple products.
Microsoft Edge: Developed by Microsoft, Edge is the default browser on Windows 10 and is known for its integration with other Microsoft products and services.
Opera: Developed by Opera Software, Opera is a web browser that is known for its

speed and built-in VPN feature.
Brave: Developed by Brave Software, Brave is a web browser that is focused on privacy and security and blocks third-party ads and trackers by default.
Tor Browser: Developed by The Tor Project, Tor Browser is a web browser that is designed for anonymous web browsing and is based on Mozilla Firefox.

11.
A web search engine is a software system that is designed to search for information on the World Wide Web. The search results are generally presented in a line of results often referred to as search engine results pages (SERPs). ... Some search engines also mine data available in databases or open directories.

A search engine is an information retrieval system designed to help find information stored on a computer system. The search results are usually presented in a list and are commonly called hits.

There are many browsers such as Internet Explorer, Firefox, Safari, and Opera, etc. A browser is used to access various websites and web pages. A search engine is also a software program that searches for some particular document when specific keywords are entered. ... Google and Yahoo are the most popular search engines.

A search engine is a web-based tool that enables users to locate information on the World Wide Web. Popular examples of search engines are Google, Yahoo!, and MSN Search. ... The information gathered by the spiders is used to create a searchable index of the Web.

12.
The internet is a public network of network with a maze of wired and wireless connections between separate groups of servers computers and countless devices from around the world. The World Wide Web is distinguished from other systems through its use of HTTP (Hypertext Transfer Protocol).

1. Internet :

The internet is a globally connected network system facilitating worldwide communication and access to data resources through a huge collection of personal, public, business, academic and government networks. it's governed by agencies just like Internet Assigned Numbers Authority (or IANA) that establish universal protocols.

2. World Wide Web (WWW) :

World Wide Web (WWW), byname Web, is leading information retrieval service of web (the worldwide computer network). Online gives users access to a huge array of documents that are connected to every other by means of hypertext or hypermedia links—i.e., hyperlinks, electronic connections that link related pieces of data so as to permit a user quick access to them. Hypertext allows the user to pick a word or phrase from text and thereby access other documents that contain additional information concerning that word or phrase.

13.

Internet access is the primary service offered by ISPs, but there are a variety of other services they may provide. These can include:

Equipment rental: Many ISPs will rent equipment like modems and routers to their customers. This can be a convenient option for those who do not want to purchase their own equipment or do not need the latest and greatest technology.
Tech support: Many ISPs offer tech support to their customers. This can be a valuable service for those unfamiliar with setting up or troubleshooting internet connections.
Email access: Some ISPs offer email services to their customers. This can be a convenient way to have an email address linked to your ISP account.
Tiered connection plans: ISPs typically offer different tiers of service, with different speeds and data allowances. This is a good option for those who want to pay for a higher-speed connection or who need more data than what is included in

the basic package.

14.

A MAC address is responsible for local identification and an IP address for global identification. This is the primary difference between a MAC address and IP address, and it affects how they differ in their number of bits, address assignment and interactions.

Both MAC Address and IP Address are used to uniquely identify a machine on the internet. MAC address is provided by the chip maker while IP Address is provided by the Internet Service Provider.

Mac Address

Media Access Control (MAC) address is a physical address that works at the data link layer of the OSI model.

A MAC address is a 48 or 64-bit address associated with a network adapter.

MAC addresses are linked to the hardware of the network adapters, hence they are also known as the "hardware address" or "physical address."

MAC addresses uniquely identify the adapter on the LAN.

MAC addresses are expressed in hexadecimal notation. For example, "01-23-45-67-89-AB" in a 48-bit address or "01-23-45-67-89-AB-CD-EF" in a 64-bit address.

Sometimes, colons (:) are used instead of dashes (-).

MAC addresses are often considered permanent, but in some conditions, they can be changed.

15. If you want to view your search history to delete or manage certain websites, you can easily do so by navigating to your browser's History settings. The steps may vary slightly depending on the platform you're using, such as Windows and Mac or

iPhone and Android. This wikiHow will teach you how to view your Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari history on both desktop and mobile platforms.