DATA COMUNICATION ASSIGNMENT

1.What are the different types of networks?

11 Types of Networks in Use Today:

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 single mode 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 (UTP)?

Shielded twisted pair cable (STP) has the individual pairs of wires wrapped in foil, which are then wrapped again for double protection. Unshielded twisted pair cable (UTP) **has each pair of wires twisted together**. Those wires are then wrapped in tubing without any other protection.

Shielded Cables Necessary?

Knowing which cable to use for a specific application depends on the protection needed from power frequency and any electromagnetic interference (EMI). This is where shielded vs. unshielded cable becomes important.

DATA COMUNICATION ASSIGNMENT

Preventing Electromagnetic Interference (EMI)

Electromagnetic interference (EMI), or radio frequency interference (RFI) as it's also referred to, is an electronic disturbance generated by external electronic or electrical sources such as electrostatic coupling, electromagnetic radiation, or electrical circuit noise. The truth is, EMI/RFI is all around us. Just like the static you may hear during a phone call, the same is true for networking. If the EMI 'noise' is strong enough it may interfere with the actual data traffic and prevent computers from 'hearing' each other.

When this happens, data is lost and the network has to resend the information a second time. The more often this process is repeated, the more often the network slows down. Thus, EMI disturbances can lower performance of a circuit or prevent it from functioning properly. Data paths can be interrupted ranging from an increase in error rate to a complete loss of information.

Different Types of Shielded Cable

Shielded twisted pair cabling (STP) reduces electromagnetic and radio frequency interference from other devices and electronic objects to ensure a steady signal. Cables consist of a bundle of wires divided into four pairs. Each pair is twisted together to reduce crosstalk interference from the other wire pairs in the bundle. There are 3 different shielding configurations, each with their own level of protection:

- **Braided** (90% EMI shielding)
- **Spiral** (98% EMI shielding)
- **Metal-coated Mylar or foil** (100% EMI shielding)

When to Use Shielded Cable

Shielded cables are useful in any environments where there is a high chance of electronic interference, such as radio stations (**telecom cable assemblies**) and airports (**aerospace cable assemblies**). STP cables are also used in security systems to provide protection from power frequency and radio frequency interference, or in **box builds** where there are multiple different components operating in close proximity. As well as being protected from external interference, the shielding also keeps noise from exiting the cable, minimizing the chance of causing interference in other devices.

When to Use Unshielded Cable

Unshielded cable (UTP) does not utilize shielding to reduce interference. UTP cables are designed to limit electromagnetic interference by the way the pairs are twisted inside the cable. UTP cable is most suitable for office LANS and similar **network cabling systems**. While offering less protection from interference, unshielded cables are popular because they are

- Versatile
- Inexpensive
- Easy to install
- Lightweight
- Flexible

The main disadvantage of UTP cables is their susceptibility to electromagnetic interference and radio frequency interference. They also have a smaller bandwidth compared to coaxial cables or fiber optic cables.

3. What is difference between baseband and broadband transmission?

Let us discuss some of the major key differences between Baseband and Broadband:

- The major difference between broadband transmission and baseband transmission is that the baseband transmissions uses the complete bandwidth for transmitting the signals and occupy the whole cable while in broadband transmission, at the same time, multiple signals can be transmitted using multiple frequencies using only one channel. In baseband transmission, the frequency cannot be divided or multiplexed, but time can be multiplexed as only one signal is transmitted in the cable. In broadband transmission, multiple signals can be transmitted, and one channel can transmit analog signals. The frequency multiplexing can be done in broadband transmission.

- The other difference between broadband transmission and baseband transmission in the direction of signals transmitted. In the baseband transmission, the signals can be transmitted in both directions at the same time. In broadband transmission, the signals can be transmitted in a single direction. The baseband transmission uses digital signaling for transmitting the signals. The broadband transmission uses analog signaling for transmitting analog signals.
- The other key difference between broadband transmission and baseband transmission is the range of the signal. In baseband transmission, the range of signal distance is too short. Thus in baseband transmission, external devices are placed in the network for the transmission of digital signals. The external device includes attenuators and repeaters, which transmit the signals to the destination node. The LAN network uses the baseband transmission to transmit the signals as in the LAN network; there is a requirement to send signals in a short distance. In broadband transmission, the signal range is long, and the signals can be easily transmitted to a long distance without using any external device for signal transmission. The radio network and TV uses broadband transmission as in this communication there is a requirement of sending signals to long distance.
- The other key difference between broadband transmission and baseband transmission is costing of signal transmission. In baseband transmission, as there is a requirement to send the signals to a short distance only, the setup cost is less as a requirement of wire is less, which decreases the setup cost. On the other hand, in broadband transmission, the setup cost is significantly higher when it is compared to baseband transmission. As in broadband transmission, the signals are transmitted over a long distance; it requires more wires and cables, which increases the transmission cost in broadband transmission. The

maintenance cost of the baseband transmission is also less when it is compared to broadband transmission. The maintenance cost increases the overall cost of broadband transmission.

- The other major difference between broadband transmission and baseband transmission is the capability of both signaling. The baseband transmission is capable of transmitting the data and voice only on the network. In broadband transmission, the network can send data, voice and video calls in the transmission medium over a long distance. The quality of videos is not compromised as the optical fibers are used for transmitting the analog signals in broadband transmission. The transmitting speed of broadband transmission is nearly about 100 MB per second.

Baseband vs Broadband Comparison Table

Let's discuss the top comparison between Baseband vs Broadband:

Factor	Baseband	Broadband
The signal used for transmission.	The baseband transmits the digital signal using the physical medium like wires.	The broadband transmits the analog signals using optical fibers and twisted cables as a medium of transmission.

Transmission direction	The baseband signaling is termed as bidirectional and is capable of sending digital signals in both directions.	The broadband signaling is termed as bidirectional and is capable of sending digital signals in only one direction.
Encoding scheme used	The baseband signaling used Manchester encoding scheme while transmitting the digital signals.	The broadband signaling used Manchester encoding scheme while transmitting the analog signals.
Range of signals	The baseband transmission can transmit the digital signals over a short distance only when compared to broadband transmission. If the digital signals need to be transmitted for a long distance, the attenuation process is required.	The broadband transmission can transmit the analog signals over a long distance compared to baseband transmission, and for transmitting the signals, no need for

		attenuation technique is required.
Topology used	The baseband transmission uses the bus topology as the application.	The broadband transmission uses the tree and bus topology as the application.
A number of data streams transmitted.	The baseband transmission can transmit the single data type stream at one glance and can send in bidirectional.	The broadband transmission can transmit multiple data streams at the same time but in one direction only.
Medium of transfer	The baseband signals used twisted-pair cables, coaxial cables and wires as a medium of transmitting digital signals.	The broadband signals used optical fiber cables, coaxial cables, and radio waves to transmit the analog signals.

Application	The baseband transmission is mostly used for the LAN networks as the baseband signaling can transmit the digital signal for a short distance only. And there is a requirement of repeaters for transmitting the signals.	Broadband transmission is mostly used for telephone networks. The broadband signaling can transmit the analog signals for long-distance without using any external device like a repeater or attenuator.

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

Hub:

Hub is commonly used to connect segments of a LAN (Local Area Network). A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets. Hub acts as a common connection point for devices in a network.

Switch:

A switch operates at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI (Open Systems Interconnection) Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of

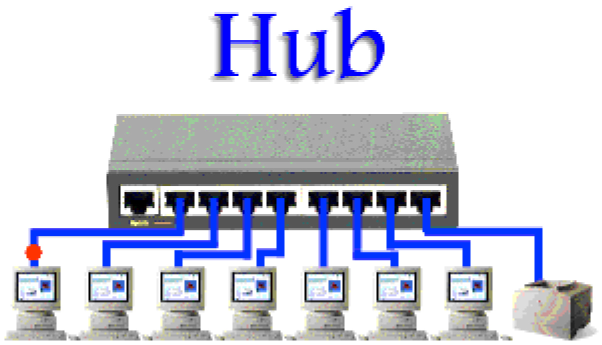
Ethernet networks, switched Ethernet LANs. In networks, the switch is the device that filters and forwards packets between LAN segments. See more information on Network Switch and Selection Suggestions.

Router:

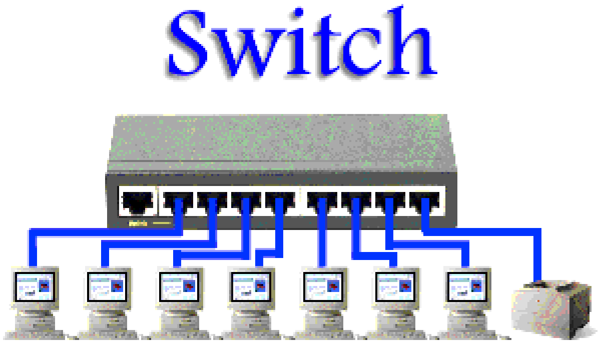
A router is connected to at least two networks, commonly two LANs or WANs (Wide Area Networks) or a LAN and its ISP.s (Internet Service Provider's) network. The router is generally located at gateways, the places where two or more networks connect. Using headers and forwarding tables, router determines the best path to forward the packets. In addition, router uses protocols such as ICMP (Internet Control Message Protocol) to communicate with each other and configures the best route between any two hosts. In a word, router forwards data packets along with networks.

Hub vs Switch vs Router:

In network equipment and devices, data is usually transmitted in the form of a frame. When a frame is received, it is amplified and then transmitted to the port of the destination PC (Personal Computer). The big difference between hub and switch is in the method in which frames are being delivered.



In a hub, a frame is passed along or "broadcast" to every one of its ports. It doesn't matter that the frame is only destined for one port. The hub has no way of distinguishing which port a frame should be sent to. Additionally, a 10/100Mbps hub must share its bandwidth with each and every one of its ports. In comparison, a switch keeps a record of the MAC (Media Access Control) addresses of all the devices connected to it. With this information, a network switch can identify which system is sitting on which port. So when a frame is received, it knows exactly which port to send it to, without significantly increasing network response times. In addition, unlike a hub, a 10/100Mbps switch will allocate a full 10/100Mbps to each of its ports. So regardless of the number of PCs transmitting, users will always have access to the maximum amount of bandwidth.



Unlike an Ethernet hub or switch that is concerned with transmitting frames, a router is to route packets to other networks until that packet ultimately reaches its destination. One of the key features of a packet is that it not only contains data but the destination address of where it's going. What's more, router is the only one of these three devices that will allow you to share a single IP (Internet Protocol) address among multiple network clients.

You can have a clear view of the comparison among hub vs switch vs router here:

Template	Hub	Switch	Router
Layer	Physical layer	Data link layer	Network layer
Function	To connect a network of personal computers together, they can be joined through a central hub	Allow connections to multiple devices, manage ports, manage VLAN security settings	Direct data in a network
Data Transmission form	electrical signal or bits	frame & packet	packet
Port	4/12 ports	multi-port, usually between 4 and 48	2/4/5/8 ports

Transmission type	Frame flooding, unicast, multicast or broadcast	First broadcast, then unicast and/or multicast depends on the need	At Initial Level Broadcast then Uni-cast and multicast
Device type	Non-intelligent device	Intelligent device	Intelligent device
Used in(LAN, MAN, WAN)	LAN	LAN	LAN, MAN, WAN
Transmission mode	Half duplex	Half/Full duplex	Full duplex
Speed	10Mbps	10/100Mbps, 1Gbps	1-100Mbps(wireless); 100Mbps-1Gbps(wired)
Address used for data transmission	MAC address	MAC address	IP address

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

Yes, 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 another one replaced the NIC card.

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

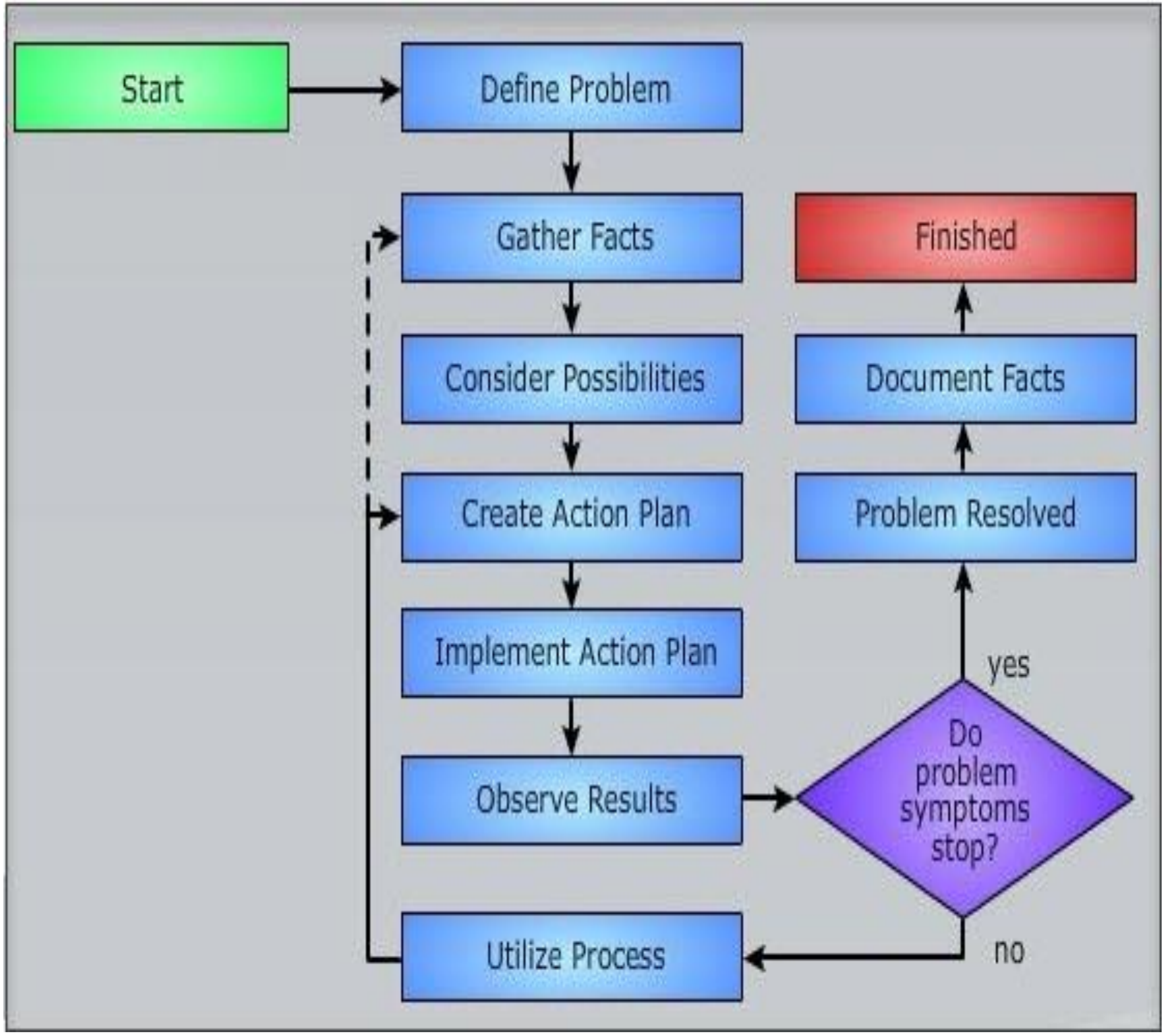
When troubleshooting computer network problems, what common hardware-related problems can occur? A large percentage of a network is made up of hardware. Problems in these areas can range from **malfunctioning hard drives, broken NICs, and even hardware startups**.

DATA COMUNICATION ASSIGNMENT

Basic Network Problems

- **Cable Problem**: The cable which is used to connect two devices can get faulty, shortened or can be physically damaged.
- **Connectivity Problem**: The port or interface on which the device is connected or configured can be physically down or faulty due to which the source host will not be able to communicate with the destination host.
- **Configuration Issue**: Due to a wrong configuration, looping the IP, routing problem and other configuration issues, network fault may arise and the services will get affected.
- **Software Issue**: Owing to software compatibility issues and version mismatch, the transmission of IP data packets between the source and destination is interrupted.
- **Traffic overload:** If the link is over utilized then the capacity or traffic on a device is more than the carrying capacity of it and due to overload condition the device will start behaving abnormally.
- **Network IP issue:** Due to improper configuration of IP addresses and subnet mask and routing IP to the next hop, the source will not be able to reach the destination IP through the network.

Network Troubleshooting Flowchart:



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

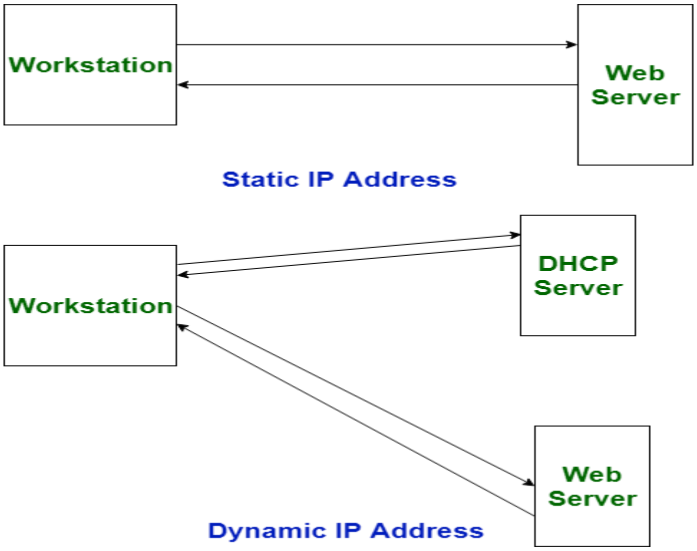
In a network that contains two servers and twenty workstations, the best place to install an Anti-virus program. The best solution is **to install anti-virus on all the computers in the network**.

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

When a device is assigned a static IP address, **the address does not change**. Most devices use dynamic IP addresses, which are assigned by the network when they connect and change over time.

IP stands for **Internet Protocol**. IP address may be a distinctive numerical symbol allotted to every device on a network to spot each affiliation unambiguously.

The distinction between Static and Dynamic IP address lies inside the length of allotted scientific discipline address. The static scientific discipline address is fastened scientific discipline address that is manually allotted to a tool for a protracted amount of your time. On the opposite hand, the Dynamic scientific discipline address oft changes whenever user boots his/her machine and it's mechanically allotted.



DATA COMUNICATION ASSIGNMENT

Difference between Static and Dynamic IP address:

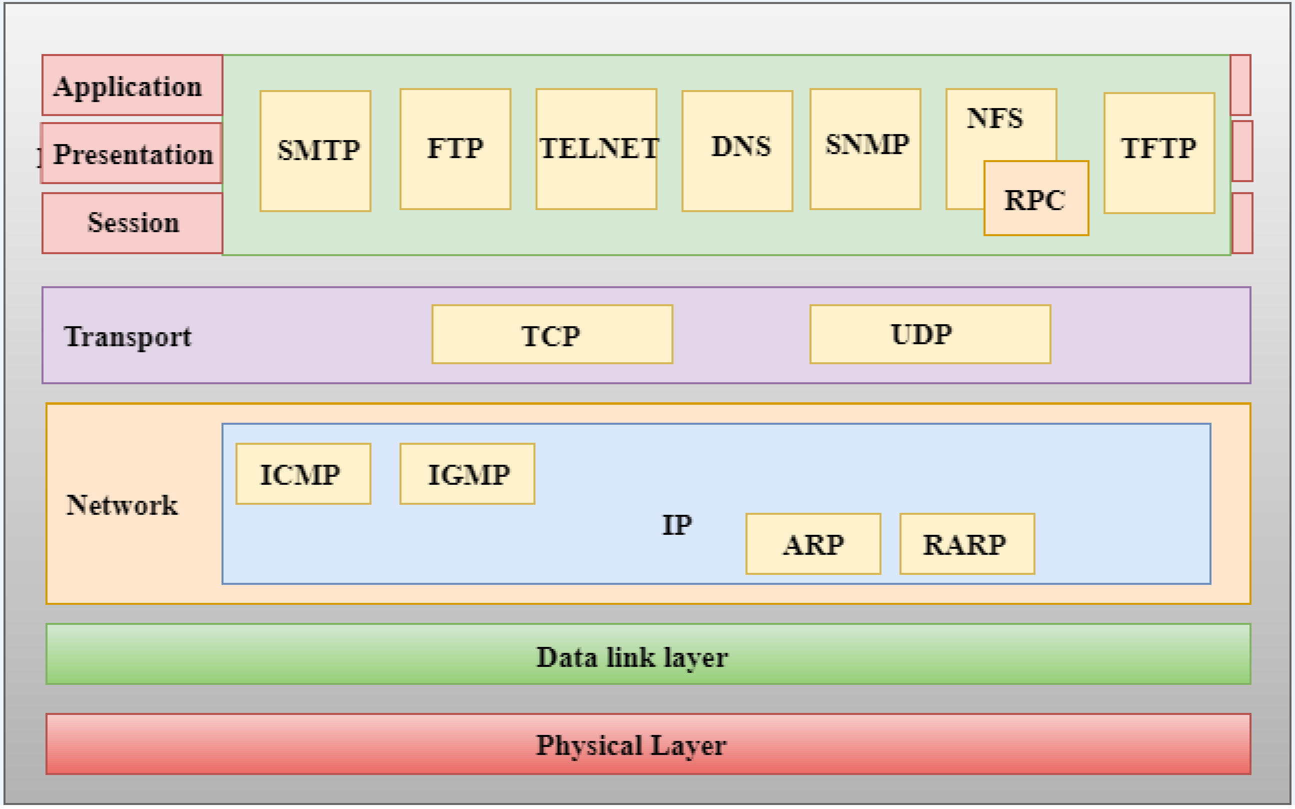
S.NO	Static IP Address	Dynamic IP address
1.	It is provided by ISP (Internet Service Provider).	While it is provided by DHCP (Dynamic Host Configuration Protocol).
2.	Static ip address does not change any time, it means if a static ip address is provided then it can't be changed or modified.	While dynamic ip address change any time.
3.	Static ip address is less secure.	While in dynamic ip address, there is low amount of risk than static ip address's risk.
4.	Static ip address is difficult to designate.	While dynamic ip address is easy to designate.
5.	The device designed by static ip address can be trace.	But the device designed by dynamic ip address can't be trace.
6.	Static ip address is more stable than dynamic ip address.	While dynamic ip address is less stable than static ip address.
7.	The cost to maintain the static ip address is higher than dynamic ip address.	While the maintaining cost of dynamic ip address is less than static ip address.
8.	It is used where computational data is less confidential.	While it is used where data is more confidential and needs more security.

9. Discuss TCP/IP model in detail?

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:



Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are Ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.

- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
  - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- An ICMP protocol mainly uses two terms:

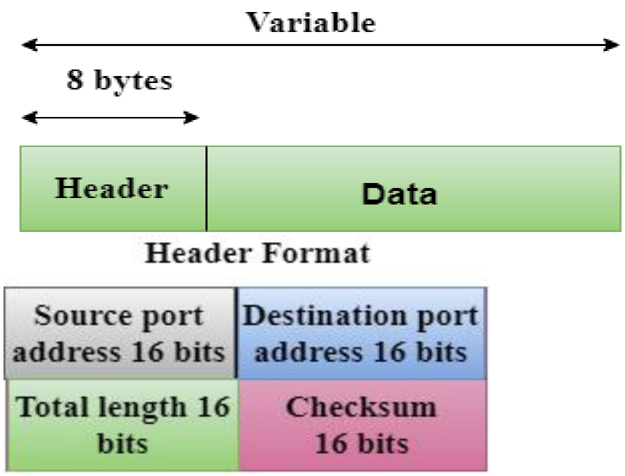
    - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
    - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

- **User Datagram Protocol (UDP)**
    - It provides connectionless service and end-to-end delivery of transmission.
    - It is an unreliable protocol as it discovers the errors but not specify the error.
    - User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
    - **UDP consists of the following fields:**
Source port address: The source port address is the address of the application program that has created the message.
Destination port address: The destination port address is the address of the application program that receives the message.
Total length: It defines the total number of bytes of the user datagram in bytes.
Checksum: The checksum is a 16-bit field used in error detection.
    - UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.



Source port address 16 bits	Destination port address 16 bits
Total length 16 bits	Checksum 16 bits

- **Transmission Control Protocol (TCP)**
  - It provides a full transport layer services to applications.
  - It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
  - TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
  - At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
  - At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system.

For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the World Wide Web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

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

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

- **Microsoft Edge**
- **Internet Explorer**
- **Google Chrome**
- **Mozilla Firefox**
- **Apple Safari**

11. What is a search engine? Give example.

A **search engine** is software accessed on the Internet that searches a database of information according to the user's query. The engine provides a list of results that best match what the user is trying to find. Today, there are many different search engines available on the Internet, each with its own abilities and features. The first search engine ever developed is considered Archie, which was used to search for FTP files, and the first text-based search engine is considered Veronica. Currently, the most popular and well-known search engine is Google. Other popular search engines include AOL, Ask.com, Baidu, Bing, DuckDuckGo, and Yahoo.

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

The Internet is very much useful in our daily routine tasks. For example, it helps us **to see our notifications and emails**. Apart from this, people can use the internet for money transfers, shopping order online food, etc.

1. **Electronic mail.** At least 85% of the inhabitants of cyberspace send and receive e-mail. Some 20 million e-mail messages cross the Internet every week.
2. **Research.**
3. **Downloading files.**
4. **Discussion groups.** These include public groups, such as those on Usenet, and the private mailing lists that List Serv manages.
5. **Interactive games.** Who hasn’t tried to hunt down at least one game?
6. **Education and self-improvement.** On-line courses and workshops have found yet another outlet.
7. **Friendship and dating.** You may be surprised at the number of electronic “personals” that you can find on the World Wide Web.
8. **Electronic newspapers and magazines.** This category includes late-breaking news, weather, and sports. We’re likely to see this category leap to the top five in the next several years.
9. **Job-hunting.** Classified ads are in abundance, but most are for technical positions.
10. **Shopping.** It’s difficult to believe that this category even ranks. It appears that “cybermalls” are more for curious than serious shoppers.

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

An **Internet service provider** (**ISP**) is an organization that provides a myriad of services for accessing, using, or participating in the Internet. Internet service providers can be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.

Internet services typically provided by ISPs can include Internet access, Internet transit, domain name registration, web hosting, Usenet service, and collocation.

Rank	ISP	Net Addition (Wire line Subscribers)
1	Jio	253,823
2	Airtel	108,148
3	Vi	7870
4	BSNL	-90,851

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

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.

Following are the important differences between MAC Address and IP Address.

Sr. No.	Key	MAC Address	IP Address
1	Definition	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
2	Usage	MAC Address ensure that physical address of the computer is unique.	IP Address is a logical address of the computer and is used to uniquely locate computer connected via a network.
3	Format	MAC Address is of six byte hexadecimal address.	IP Address is of 4 bytes or of 16 bytes.
4	Access Protocol	MAC Address can be retrieved using ARP protocol.	IP Address can be retrieved using RARP protocol.
5	Provider	Chip maker manufacturer	Internet Service Provider, ISP provides

DATA COMUNICATION ASSIGNMENT

Sr. No.	Key	MAC Address	IP Address
		provides the MAC Address.	the IP Address.

Difference between IP address and Port Number :

Serial No	IP address	Port Number
01.	Internet Protocol address (IP address) used to identify a host in network.	Port number is used to identify an processes/services on your system
02.	IPv4 is of 32 bits (4 bytes) size and for IPv6 is 128 bits (16 bytes).	The Port number is 16 bits numbers.
03.	IP address is the address of the layer-3 IP protocol.	Port number is the address of the layer-4 protocols.
04.	IP address is provided by admin of system or network administrator.	Port number for application is provided by kernel of Operating System.
05.	ipconfig command can be used to find IP address .	netstat command can be used to find Network Statistics Including Available TCP Ports.
06.	IP address identify a host/computer on a computer network.	Port numbers are logical interfaces used by communication protocols.
07.	192.168.0.2, 172.16.0.2 are some of IP address examples.	80 for HTTP, 123 for NTP, 67 and 68 for DHCP traffic, 22 for SSH etc.

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

Today, all major browsers have functionality that allows you to quickly and easily view your Internet browser's history. However, as multiple devices contain browser history, there are multiple ways to view as well. To proceed, choose your devices from the section below and follow the instructions.

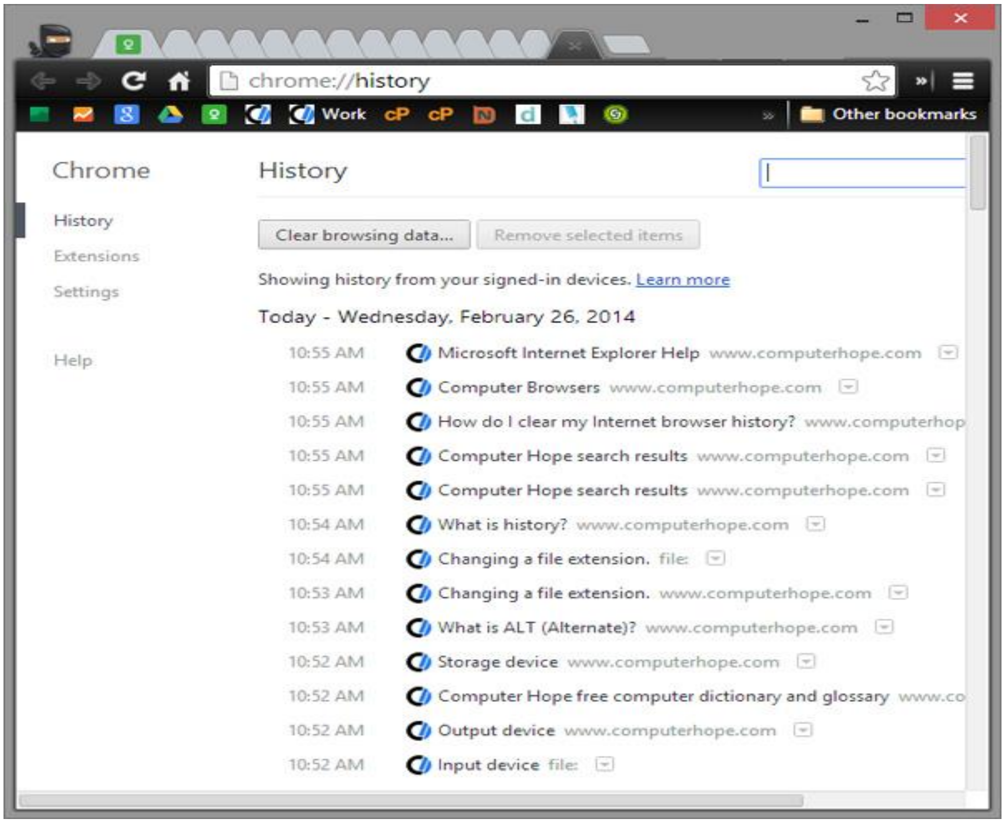
Desktop or laptop computer

If you are using Windows, Linux, or macOS, there are quick shortcut key combinations that allow you to view your history.

Windows and Linux users: Ctrl+H

Apple users: Command + Shift + H

Once one of the above shortcut keys is pressed, a history section similar to the example below should appear. In the following screenshot, browsing history is being viewed in Google Chrome.



Showing history from your signed-in devices. Learn more

Today - Wednesday, February 26, 2014

10:55 AM Microsoft Internet Explorer Help www.computerhope.com

10:55 AM Computer Browsers www.computerhope.com

10:55 AM How do I clear my Internet browser history? www.computerhop

10:55 AM Computer Hope search results www.computerhope.com

10:55 AM Computer Hope search results www.computerhope.com

10:54 AM What is history? www.computerhope.com

10:54 AM Changing a file extension. file:

10:53 AM Changing a file extension. www.computerhope.com

10:53 AM What is ALT (Alternate)? www.computerhope.com

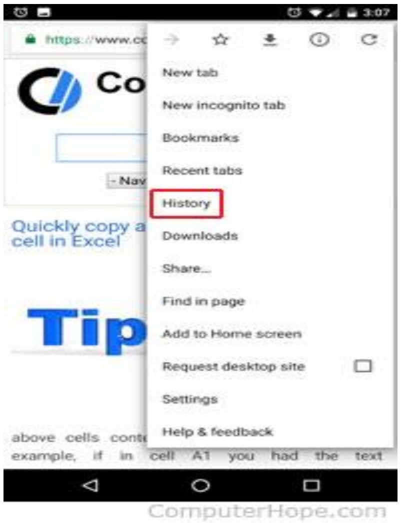
10:52 AM Storage device www.computerhope.com

10:52 AM Computer Hope free computer dictionary and glossary www.co

10:52 AM Output device www.computerhope.com

10:52 AM Input device file:

Android phone or tablet running Google Chrome



Users who are running Google Chrome on their Android phone or tablet can view their history with the following steps.

1. Open the Google Chrome Internet browser.
2. In the upper-right corner of the screen **tap the** ⋮ **icon**.
3. In the drop-down menu that appears, select **history** and shown in the image.
4. The following page contains your device's history.

iPhone or iPad running Safari

Users who are running Safari for iOS on their iPhone or iPad can view their history with the following steps.

1. On your device, open the Safari Internet browser.
2. In the lower-left corner of the browser window, press and hold the back arrow.
3. The next screen contains your browser's history.