

CCA-102: Data Communications

1. What are the different types of networks?

A computer network is an interconnected system of devices, represented as network nodes, that share information, data and resources among each other. Not all networks are the same. There are several types of networks, each existing to support the devices, size and location of the system. Networks also have differing levels of access and forms of connectivity. Below are seven common types of networks, along with their benefits and use cases.

1. Personal area network

A personal area network (PAN) is the smallest and simplest type of network. PANs connect devices within the range of an individual and are no larger than about 10 meters (m). Because PANs operate in such limited areas of space, most are wireless and provide short-range connectivity with infrared technology.

An example of a wireless PAN is when users connect Bluetooth devices, like wireless headsets, to a smartphone or laptop. Although most PANs are wireless, wired PAN options exist, including USB.

2. Local area network

A local area network (LAN) is a system where computers and other devices connect to each other in one location. While PANs connect devices around an individual, the scope of a LAN can range from a few meters in a home to hundreds of meters in a large company office. The network topology determines how devices in LANs interconnect.

LANs use both wired and wireless connectivity options. Wireless LAN (WLAN) has surpassed traditional wired LAN in terms of popularity, but wired LAN remains the more secure and reliable option. Wired LANs use physical cables, like Ethernet, and switches; WLANs use devices, like wireless routers and access points, to interconnect network devices through radio frequency waves.

Network administrators can implement security protocols and encryption standards to secure wireless networks. Wired LANs are usually more secure because they require a physical cable to form a connection and are far less susceptible to compromise.

3. Metropolitan area network

A metropolitan area network (MAN) is an interconnection of several LANs throughout a city, town or municipality. Like LANs, a MAN can use various wired or wireless connectivity options, including fiber optics, Ethernet cables, Wi-Fi or cellular.

MAN benefits

- Municipal coverage. A MAN can span an entire city or town, stretching network connectivity by dozens of miles.
- Efficient networking standards. MAN configurations typically use IEEE 802.11 networking standards to increase bandwidth capacity and frequency levels, which boost network performance.
- High-speed connectivity. Fiber optic cables are the most popular form of MAN connectivity because they provide safe and fast connection data rates.

4. Campus network

A campus network, sometimes referred to as a *campus area network* or *CAN*, is a network of interconnected, dispersed LANs. Like MANs, campus networks extend coverage to buildings close in proximity. The difference between the two configurations is that campus networks connect LANs within a limited geographical area, while MANs connect LANs within a larger metro area. The geographical range of a campus network varies from 1 kilometer to 5 km, while MANs can extend to 50 km.

5. Wide area network

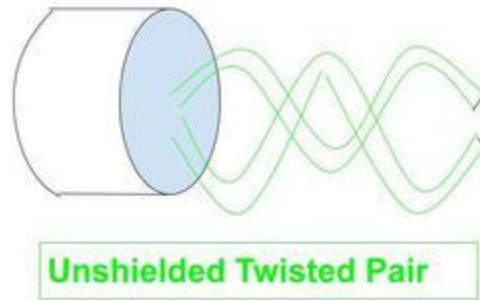
A wide area network (WAN) is the most expansive type of computer network configuration. Like a MAN, a WAN is a connection of multiple LANs belonging to the same network. Unlike MANs, however, WANs aren't restricted to the confines of city limits. A WAN can extend to any area of the globe. For example, an organization with a corporate office in New York can connect a branch location in London in the same WAN. Users in both locations obtain access to the same data, files and applications, and can communicate with each other.

6. Content delivery network

A content delivery network (CDN) is a network of globally distributed servers that deliver dynamic multimedia content -- such as interactive ads or video content -- to web-based internet users. CDNs use specialized servers that deliver bandwidth-heavy rich media content by caching it and speeding up delivery time. CDN providers deploy these digitized servers globally at a network edge, creating geographically distributed points of presence.

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

UTP is the type of twisted pair cable. It stands for Unshielded twisted pair. Both Data and voice are transmitted through UTP because its frequency range is suitable. In UTP grounding cable is not necessary also in UTP much more maintenance is not needed therefore it is cost-effective.

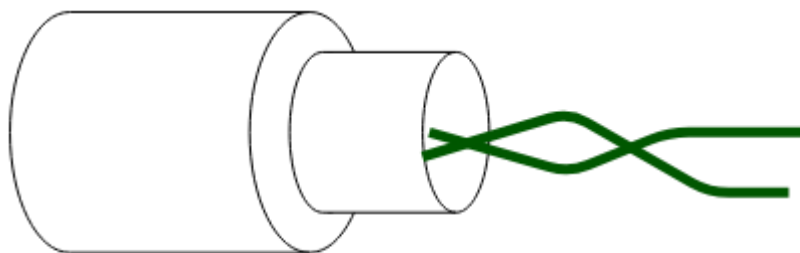


Unshielded Twister Pair cable (UTP)

Features :

- Cost-effective: UTP cables are relatively inexpensive compared to other types of network cables.
- Easy to install: UTP cables are easy to install and terminate, which makes them a popular choice for small and medium-sized networks.
- Vulnerable to interference: UTP cables are vulnerable to interference from nearby sources of electromagnetic radiation, such as power lines, motors, and other electrical equipment. This can cause signal degradation and data loss.
- Limited distance: UTP cables have a limited distance over which they can reliably transmit data, typically up to 100 meters.

STP is also the type of twisted pair which stands for Shielded twisted pair. In [STP](#) grounding cable is required but in [UTP](#) grounding cable is not required. in Shielded Twisted Pair (STP) much more maintenance is needed therefore it is costlier than Unshielded Twisted Pair (UTP).



Shielded Twisted Pair

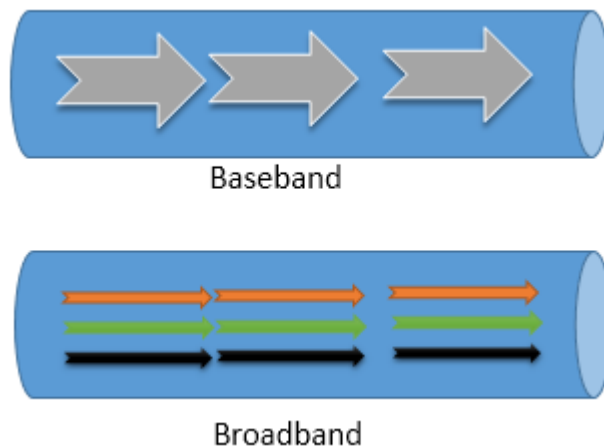
Features :

- Enhanced protection: STP cables are shielded with a layer of metal foil or braided copper mesh, which provides additional protection against electromagnetic interference.
- Better performance: STP cables can transmit data over longer distances and at higher speeds than UTP cables, making them ideal for high-bandwidth applications.
- More complex to install: STP cables are more complex to install and terminate than UTP cables, which can increase installation costs and require specialized skills.
- More expensive: STP cables are more expensive than UTP cables due to the additional shielding and manufacturing costs involved.

3. What is difference between baseband and broadband transmission?

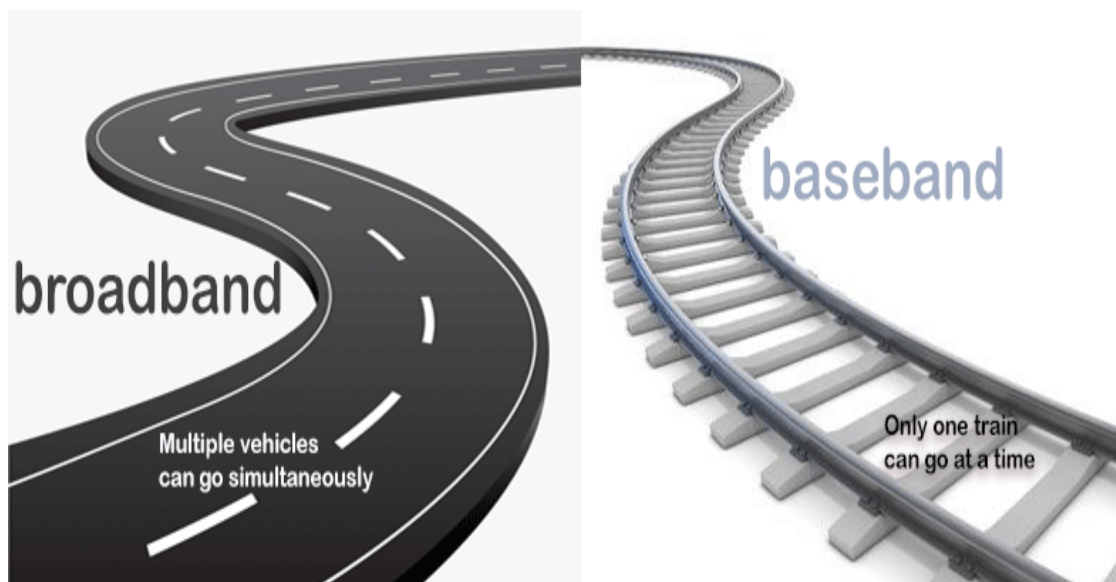
Both baseband and broadband describe how data is transmitted between two nodes. Baseband technology transmits a single data signal/stream/channel at a time while broadband technology transmits multiple data signals/streams/channels simultaneously at the same time.

The following image shows an example of both technologies.



To understand the basic differences between both technologies, consider the baseband as a railway track and the broadband as a highway. Like, at a time, only one train can go on a railway track, in the baseband transmission only one data signal can be transmitted at a time.

Unlike a railway track on a highway, multiple vehicles can go simultaneously. For example, on a 3 lanes highway, 3 vehicles can go at the same time. Same as a highway, in the broadband transmission, multiple data signals can be transmitted at the same time.

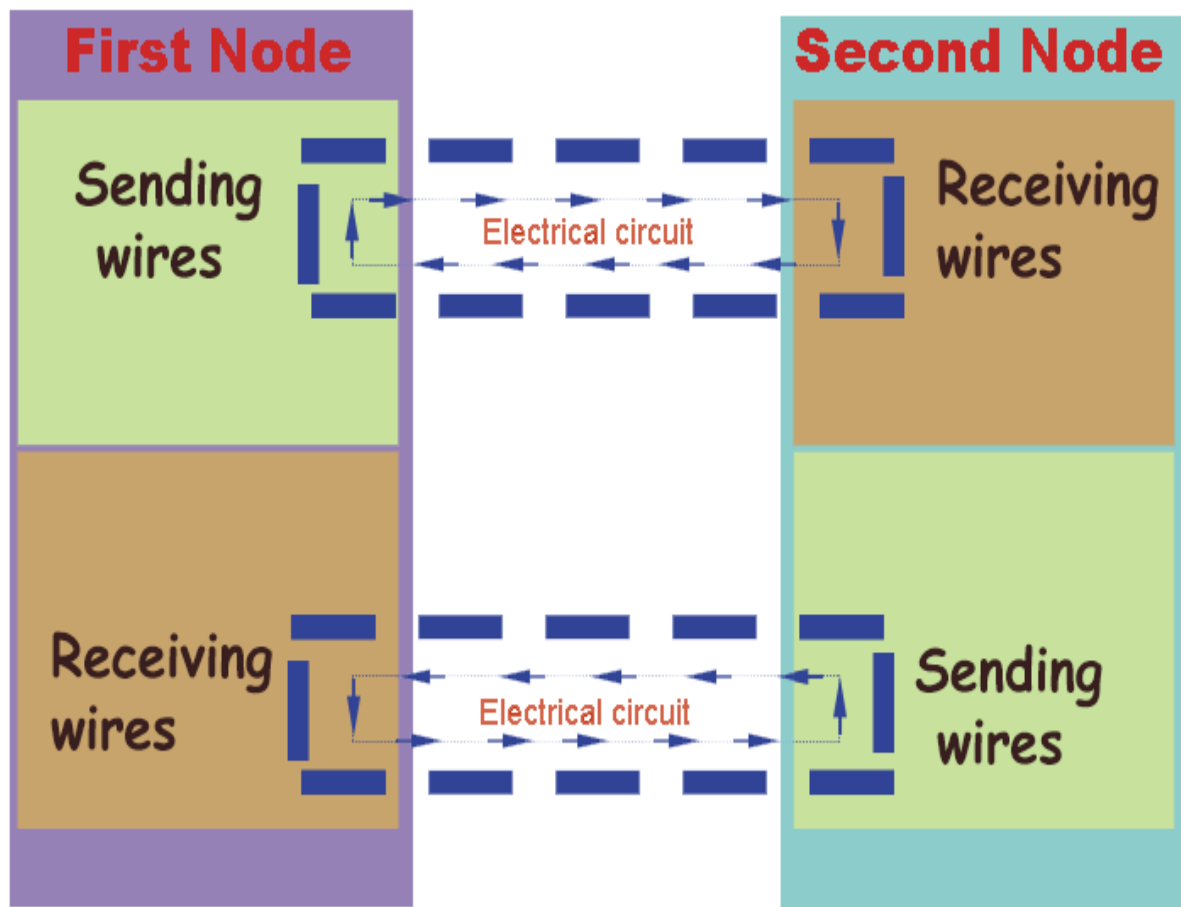


Technical differences between the baseband and broadband transmissions

Baseband technology uses digital signals in data transmission. It sends binary values directly as pulses of different voltage levels. Digital signals can be regenerated using repeaters in order to travel longer distances before weakening and becoming unusable because of attenuation.

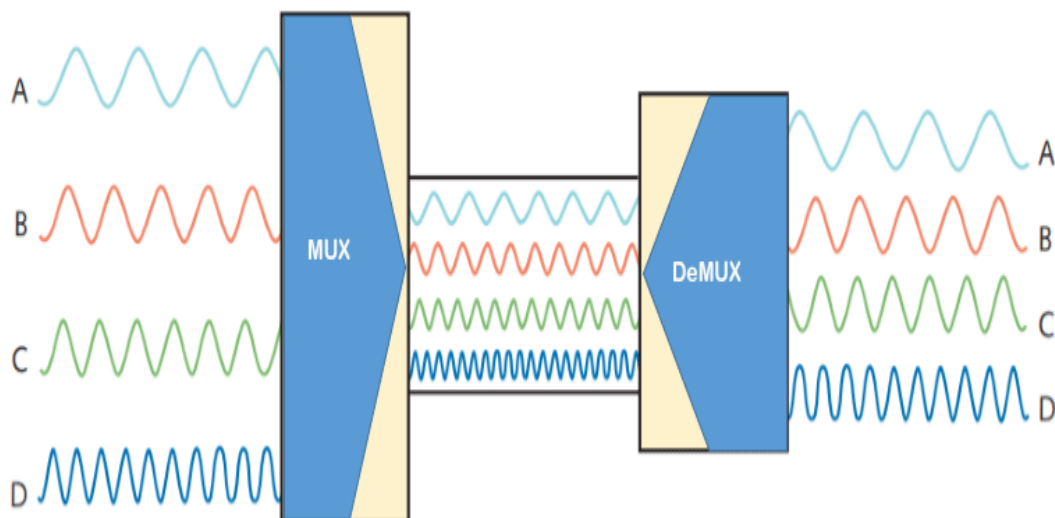
Baseband supports bidirectional communication. It means, this technology can send and receive data simultaneously. To support bidirectional communication, this technology uses two separate electric circuits together; one for sending and another for receiving.

The following image shows an example of this.



Although baseband transmits only a single data stream at a time, it is possible to transmit signals of multiple nodes simultaneously. This is done by combining all the signals into a single data stream. To combine the signals of multiple nodes, a technology known as multiplexing is used. Baseband supports the Time Division Multiplexing (TDM).

The following image shows an example of this process.

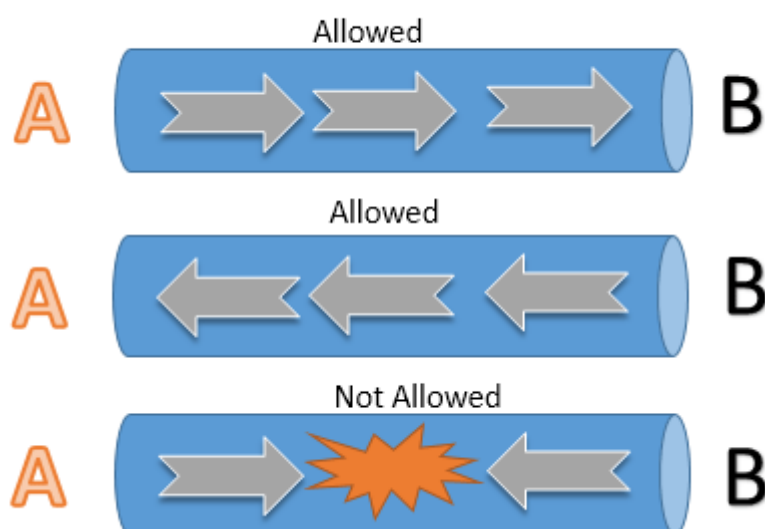


Analog signals can be regenerated using amplifiers in order to travel longer distances.

Broadband supports only unidirectional communication. It means, nodes connected at both ends of a medium can send or receive data but can't perform both actions simultaneously. Only one action is allowed at a time.

For example, two nodes A and B are connected through a cable that uses broadband technology to transmit signals. When node A transmits signals, node B receives the transmitted signals and when node B transmits signals, node A receives the transmitted signals.

The following image shows this example.



Broadband is typically used in an environment that transmits audio, video, and data simultaneously. For example, Cable TV Networks, Radio stations, and Telephone companies. Usually radio waves, coaxial, fiber-optic cables are used for broadband transmission.

Key differences between baseband and broadband transmissions

Baseband transmission	Broadband transmission
Transmit digital signals	Transmit analog signals
To boost signal strength, use repeaters	To boost signal strength, use amplifiers
Can transmit only a single data stream at a time	Can transmit multiple signal waves at a time
Support bidirectional communication simultaneously	Support unidirectional communication only
Support TDM based multiplexing	Support FDM based multiplexing
Use coaxial, twisted-pair, and fiber-optic cables	Use radio waves, coaxial cables, and fiber optic cables
Mainly used in Ethernet LAN networks	Mainly used in cable and telephone networks

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

Hubs

A hub is the simplest type of networking device, and it is typically used to connect multiple devices to a network. Hubs operate at the physical layer of the OSI model, which means they simply repeat incoming network traffic to all connected devices, regardless of whether or not the devices need the information. Because of this, hubs are not very efficient and can lead to network congestion.

Switches

Switches are more advanced networking devices than hubs. They operate at the data link layer of the OSI model and selectively forward network traffic only to the devices that need the information. This makes switches more efficient than hubs and reduces network congestion. Switches typically have more advanced features than hubs, such as virtual LANs (VLANs), Quality of Service (QoS), and port mirroring.

Routers

Routers are networking devices that are used to connect different networks together. They operate at the network layer of the OSI model and are responsible for routing network traffic between different networks, such as between a local network and the internet. [Routers](#) use routing tables to determine the best path for network traffic to reach its destination, and they can also perform [network address translation](#) (NAT), firewalling, and other security functions.

Modems

A modem is a networking device that converts digital signals into analog signals for transmission over phone lines, cable lines, or other types of communication channels. Modems are typically used to connect devices to the internet or other wide-area networks. Modems can be internal or external to a computer or other device, and they can support various connection types, such as DSL, cable, or satellite.

Differences Between Hubs, Switches, Routers, and Modems

The main difference between hubs, switches, routers, and modems is the layer of the OSI model at which they operate and their specific functions. Hubs operate at the physical layer, switches operate at the data link layer, routers operate at the network layer, and modems operate at the physical layer when converting digital signals to analog signals for transmission over communication channels.

Hubs and switches are used to connect devices to a local network, while routers are used to connect different networks together. Modems are used to connect devices to communication channels.

In terms of their capabilities, switches, and routers are more advanced than hubs and modems. Switches can selectively forward network traffic to reduce network congestion, and they can also support advanced features such as VLANs and QoS. Routers can perform more advanced functions such as routing network traffic between different networks, NAT, and firewalling.

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

MAC addresses are burned into the NIC card and transfer with the network adapter.

Having said that, I can't think of an even semi-modern OS that won't let you change it to whatever you want in the configuration of the device. I've changed MAC addresses of computers many times over the years. Usually to fix stupid crap like assigning a software license to a particular MAC address. Worthless because you can easily change it. If I want to move it to a new server I'm just gonna change it rather than deal with trying to contact a company that may or may not even be in business anymore.

The Media Access Control address (MAC address) for any network adapter is hard coded into the card itself. Each manufacturer of network adapters has a group of characters assigned that refer specifically to that company. I believe that is the first 1/2 of the MAC address which is 12 hexadecimal characters long. But the MAC address is part and parcel of the network adapter, just as your internal organs are part of you. When you move to a new house, you take your liver with you. In the same way, when you move a NIC to a different computer, it takes its MAC address with it.

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

When troubleshooting computer network problems, common hardware-related problems can include

- Malfunctioning hard drives
- Broken NICs
- Hardware startups
- Loose cords
- Switched off routers
- Faulty routers, switches, firewalls
- Network bandwidth spikes
- Changes in app configuration
- Security breaches

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

Antivirus should be on each computer, if you implement server and node base antivirus that will be best for controlling.

There are no special problems just because you are two server and 20 computer. Every general issue will come along with critical. It will be same as any other computer setup issue. Network topology such as WIFI is subject to hot and cold spots especially if a mesh is in use. The hardware of course can fail. You need to probably have some HDD recovery tools.

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

Static IP refers to addresses that remain the same. Dynamic IP refers to addresses that periodically change. Most people have a dynamic IP, or an IP address that's assigned by your internet provider and changes periodically. Static IP addresses are typically only set up for external devices and websites that need to remember your IP address. Static IP addresses require a complex manual setup, while dynamic IP addresses are configured and assigned automatically.

What is IPv4?

IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.

For example, **66.94.29.13**

The above example represents the IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255. This address can produce 4,294,967,296 possible unique addresses.

In today's computer network world, computers do not understand the IP addresses in the standard numeric format as the computers understand the numbers in binary form only. The binary number can be either 1 or 0. The IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.

Each bit in an octet can be either 1 or 0. If the bit is 1, then the number it represents will count, and if the bit is 0, then the number it represents does not count.

What is IPv6?

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses. 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.

It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

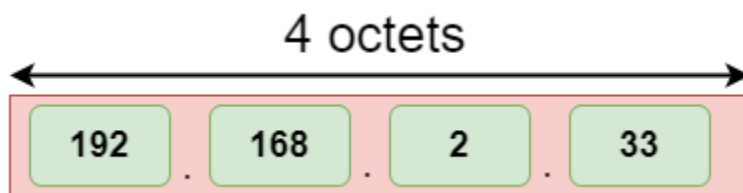
- **Dual stacking:** It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.
- **Tunneling:** In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.
- **Network Address Translation:** The translation allows the communication between the hosts having a different version of IP.

This hexadecimal address contains both numbers and alphabets. Due to the usage of both the numbers and alphabets, IPv6 is capable of producing over 340 undecillion (3.4×10^{38}) addresses.

IPv6 is a 128-bit hexadecimal address made up of 8 sets of 16 bits each, and these 8 sets are separated by a colon. In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time

Address format

The address format of IPv4:



9. Discuss TCP/IP model in detail.

The TCP/IP Reference Model/ DoD Model:

The TCP/IP reference model was developed prior to OSI model. The major design goals of this model were,

1. To connect multiple networks together so that they appear as a single network.
2. To survive after partial subnet hardware failures.
3. To provide a flexible architecture.

Unlike OSI reference model, TCP/IP reference model has only 4 layers. They are,

1. Host-to-Network Layer
2. Internet Layer
3. Transport Layer
4. Application

Layer

Host-to-Network Layer:

The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and varies from host to host and network to network.

Internet Layer:

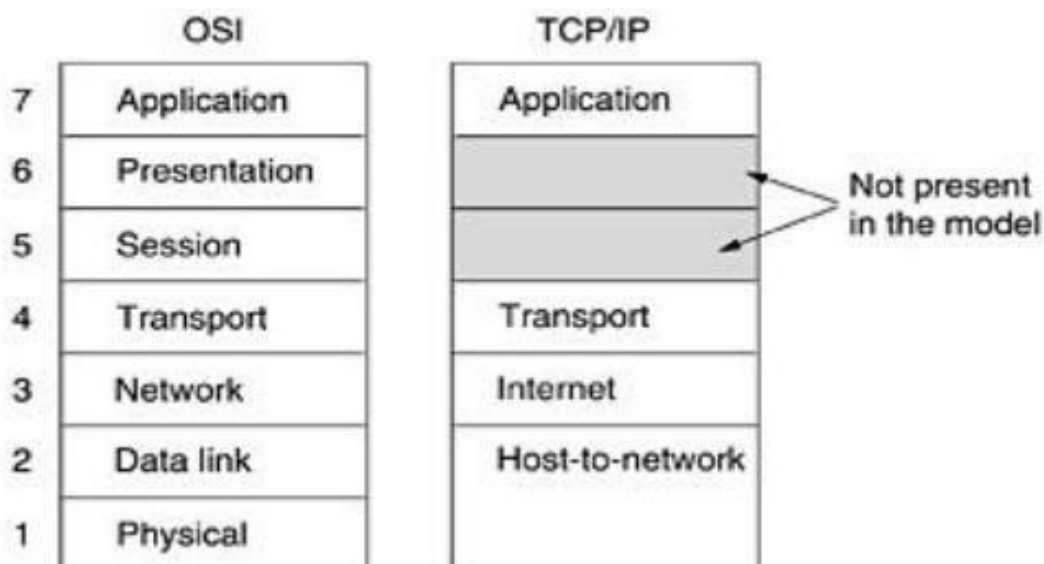
This layer, called the internet layer, is the linchpin that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network). They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired. Note that "internet" is used here in a generic sense, even though this layer is present in the Internet.

The internet layer defines an official packet format and protocol called IP (Internet Protocol). The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that the TCP/IP internet layer is similar in functionality to the OSI network layer. Fig. shows this correspondence.

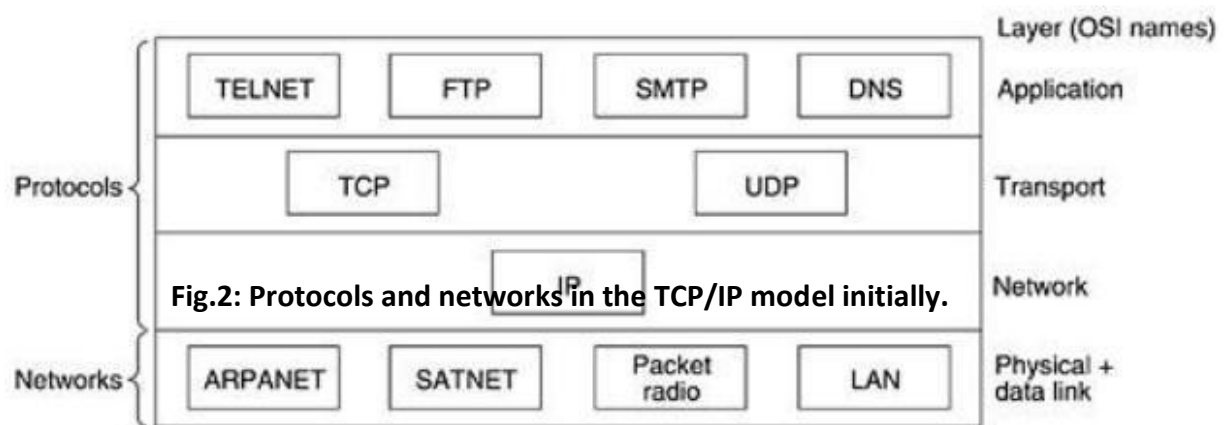
The Transport Layer:

The layer above the internet layer in the TCP/IP model is now usually called the transport layer. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Two end-to-end transport protocols have been defined here. The first one, TCP (Transmission Control Protocol), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control

to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.



The second protocol in this layer, UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. The relation of IP, TCP, and UDP is shown in Fig.2. Since the model was developed, IP has been implemented on many other networks.



The Application Layer:

The TCP/IP model does not have session or presentation layers. On top of the transport layer is the application layer. It contains all the higher-level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP), as shown in Fig.6.2. The virtual terminal protocol allows a user on one machine to log onto a distant machine and work there. The file transfer protocol provides a way to move data efficiently from one machine to another. Electronic mail was originally just a kind of file transfer, but later a specialized protocol (SMTP) was developed for it. Many other protocols have been added to these over the years: the Domain Name System (DNS) for mapping host names onto their network addresses, NNTP, the protocol for moving USENET news articles around, and HTTP, the protocol for fetching pages on the World Wide Web, and many others.

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

A software application used to access information on the World Wide Web is called a Web Browser. When a user requests some information, the web browser fetches the data from a web server and then displays the webpage on the user's screen.

Today web browsers are easily accessible and can be used on devices like computer, laptops, mobile phones, etc. but this evolution of making browsers available for easy use took many years.

Given below are some salient points which one must know with regard to the history of web browsers:

- **"WorldWideWeb"** was the first web browser created by Tim Berners Lee in 1990. This is completely different from the World Wide Web we use today
- In 1993, the **"Mosaic"** web browser was released. It had the feature of adding images and an innovative graphical interface. It was the "the world's first popular browser"
- After this, in 1994, Marc Andreessen (leader of Mosaic Team) started working on a new web browser, which was released and was named **"Netscape Navigator"**
- In 1995, **"Internet Explorer"** was launched by Microsoft. It soon overtook as the most popular web browser
- In 2002, **"Mozilla Firefox"** was introduced which was equally as competent as Internet Explorer
- Apple too launched a web browser in the year 2003 and named it **"Safari"**. This browser is commonly used in Apple devices only and not popular with other devices
- Finally, in the year 2008, Google released **"Chrome"** and within a time span of 3 years it took over all the other existing browsers and is one of the most commonly used web browsers across the world

Types of Web Browser

The functions of all web browsers are the same. Thus, more than the different types there are different web browsers which have been used over the years.

Discussed below are different web browser examples and their specific features:

1. WorldWideWeb

- The first web browser ever
- Launched in 1990
- It was later named **"Nexus"** to avoid any confusion with the World Wide Web
- Had the very basic features and less interactive in terms of graphical interface
- Did not have the feature of bookmark

2. Mosaic

- It was launched in 1993
- The second web browser which was launched

- Had a better graphical interface. Images, text and graphics could all be integrated
- It was developed at the National Center for Supercomputing Applications
- The team which was responsible for creating Mosaic was lead by Marc Andreessen
- It was named “the world’s first popular browser”

3. Netscape Navigator

- It was released in 1994
- In the 1990s, it was the dominant browser in terms of usage share
- More versions of this browser were launched by Netscape
- It had an advanced licensing scheme and allowed free usage for non-commercial purposes

4. Internet Explorer

- It was launched in 1995 by Microsoft
- By 2003, it has attained almost 95% of usage share and had become the most popular browsers of all
- Close to 10 versions of Internet Explorer were released by Microsoft and were updated gradually
- It was included in the Microsoft Windows operating system
- In 2015, it was replaced with “Microsoft Edge”, as it became the default browser on Windows 10

5. Firefox

- It was introduced in 2002 and was developed by Mozilla Foundation
- Firefox overtook the usage share from Internet Explorer and became the dominant browser during 2003-04
- Location-aware browsing was made available with Firefox
- This browser was also made available for mobile phones, tablets, etc.

6. Google Chrome

- It was launched in 2008 by Google
- It is a cross-platform web browser
- Multiple features from old browsers were amalgamated to form better and newer features
- To save computers from malware, Google developed the ad-blocking feature to keep the user data safe and secure
- Incognito mode is provided where private searching is available where no cookies or history is saved
- Till date, it has the best user interface

11. What is a search engine? Give example.

search engine is a software that is accessed on the internet to assist a user to search its query on the world wide web. The search engine is helpful as it carries out a systematic search on the web and displays the results that best match the user's query.

The results are usually retrieved in the form of a list often referred to as SERPs or Search Engine Result Pages. These results or information may be links to web pages, or a mix of images and videos, research papers, newspaper articles, etc.

The search engine follows three steps to execute the query of the user-

1. Crawling
2. Indexing
3. Ranking

The search engine follows these steps to provide relevant results to the user.

Crawling

Discovering new web pages on the internet starts with crawling. All search engines use these bots called web crawlers or spider bots that follow links to the new webpages present in the known ones.

They get the information by crawling from site to site. Once the information is collected it is indexed. While indexing is going on the spider keeps going with discovering new pages. Once a certain amount of time is spent or based on the amount of data collected, the spider stops crawling.

Indexing

Once the data is crawled it is sent for indexing-saving data on the database of the search engine called the index.

It is the job of the index to find information related to the query as soon as possible. This process can be performed quickly by adopting any of these steps-

- Stripping out the stop words.
- Listing links to other pages.
- Listing information about images or embedded media on the page.

Any website has to be indexed to get listed on search results. Sometimes when a query is entered, the index results are obtained quickly because it has already stored a few website links containing the keywords.

Ranking

The last step is to rank the results on the SERP. The search engines have their criteria based on which the search results are listed. These signals or criteria are hidden from the public. It is the work of the ranking to determine the order of the web links on the results page.

Examples of Search Engine are:-

1. Bing (renamed as Microsoft Bing in October 2020)

This one is almost as popular as the Google search. Bing is the default search engine of the Windows PC. One might find various similarities between Google and Bing with result features like – images, videos, places, maps, and news.

Though Microsoft might have attempted to make it as successful as Google it still holds only 2-3 percent of the total search engine market share.

2. Yahoo

Yahoo used to be one of the most popular sites to visit at one time. It is exclusively provided by Bing. It is also a default for Firefox users in the United States.

3. Baidu

This one is a popular engine in China. Though not very popular, its shares are increasing worldwide, according to Alexa. It is available all around the world but only in Chinese.

4. Yandex

Yandex.ru is a popular search engine in countries like Russia, Ukraine, Turkey, etc. Its name is derived from Yet Another Indexer. It has less than 1 percent market share of the overall search engine.

5. DuckDuckGo

This not-so-popular search engine has about 0.45 percent of the market share. Its competitors are also small search engines like Bing and Yahoo. Unlike most search engines it does not have a search index of its own, instead uses a variety of sources.

In other words, it does not have data of its own and depends on other sites like Yahoo, Bing, etc. But what makes it unique from the lot is that it's much cleaner and is not full of trash ads.

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

The Internet is the foremost important tool and the prominent resource that is being used by almost every person across the globe. It connects millions of computers, webpages, websites, and servers. Using the internet we can send emails, photos, videos, and messages to our loved ones. Or in other words, the Internet is a widespread interconnected network of computers and electronic devices(that support Internet). It creates a communication medium to share and get information online. If your device is connected to the Internet then only you will be able to access all the applications, websites, social media apps, and many more services. The Internet nowadays is considered the fastest medium for sending and receiving information.

The **World Wide Web (WWW)**, commonly known as **the Web**, is an information system enabling information to be shared over the Internet through simplified ways meant to appeal to users beyond IT specialists and hobbyists, as well as documents and other web resources to be accessed over the Internet according to specific rules, the Hypertext Transfer Protocol (HTTP).

Documents and downloadable media are made available to the network through web servers and can be accessed by programs such as web browsers. Servers and resources on the World Wide Web are identified and located through character strings called uniform resource locators (URLs). The original and still very common document type is a web page formatted in Hypertext Markup Language (HTML). This markup language supports plain text, images, embedded video and audio contents, and scripts (short programs) that implement complex user interaction. The HTML language also supports hyperlinks (embedded URLs) which provide immediate access to other web resources. Web navigation, or web surfing, is the common practice of following such hyperlinks across multiple websites. Web applications are web pages that function as application software. The information in the Web is transferred across the Internet using the Hypertext Transfer Protocol (HTTP).

Multiple web resources with a common theme and usually a common domain name make up a website. A single web server may provide multiple websites, while some websites, especially the most popular ones, may be provided by multiple servers. Website content is provided by a myriad of companies, organizations, government agencies, and individual users; and comprises an enormous amount of educational, entertainment, commercial, and government information.

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

The term “internet service provider (ISP)” refers to a company that provides access to the internet to both personal and business customers. ISPs make it possible for their customers to surf the web, shop online, conduct business, and connect with family and friends—all for a fee. ISPs may also provide other services, including email services, domain registration, web hosting, and browser packages. An ISP may also be referred to as an information service provider, a storage service provider, an internet network service provider (INSP), or any combination of these three based on the services offered by the company.

- An internet service provider (ISP) is a company that provides web access to businesses and consumers.
- ISPs may also provide other services such as email services, domain registration, web hosting, and browser services.
- An ISP is considered to be an information service provider, storage service provider, internet network service provider (INSP), or a mix of all of them.
- Internet use has evolved from only those with university or government accounts having access to nearly everyone having access, whether it's paid or free.
- Access has gone from dial-up connections to high-speed broadband technology.

Internet service was originally limited to government agencies and specific university departments. The technology was developed to provide access to the general public through the World Wide Web in the late 1980s. Initially, consumers were able to gain limited access through a few ISPs—America Online (AOL) being one of the most recognized names at the time—that used dial-up connections using a phone line.

The number of ISPs increased to several thousand during the mid-1990s, and the boom was on. As the options for connectivity increased and speeds moved away from slower dial-up connections, the internet economy was born. Providers developed more advanced technology, allowing customers high-speed access via broadband technology through cable and digital subscriber line (DSL) modems.

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

The main difference between MAC and IP address is that MAC Address is used to ensure the physical address of the computer. It uniquely identifies the devices on a network. While IP addresses are used to uniquely identify the connection of the network with that device that takes part in a network.

MAC Address and IP Address

MAC Address

Mac address is separated by colons.

Mac address is hardware oriented.

You can't hide the mac address from the device.

IP Address

Ip address is separated by dots.

IP address is software oriented.

It is possible to hide IP addresses using the router or VPN.

Why do we have MAC address IP Address and also port numbers can't we communicate with only one address?

Computer A could potentially learn the IP Address of Computer 2. And that's why computers have both MAC Addresses and IP Addresses. MAC Addresses handle the physical connection

from computer to computer while IP Addresses handle the logical routeable connection from both computer to computer AND network to network.

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

Desktop or laptop computer

If you are using Windows, Linux, or macOS, a quick keyboard shortcut lets you view your history.

Windows and Linux users: **Ctrl+H**


Apple users: **Command+Shift+H**

When one of these keyboard shortcuts is pressed, a history section similar to the example below should appear. In the following screenshot, browsing history is being viewed in Google Chrome.

Android phone or tablet running Google Chrome



Users 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 page that opens contains your device's history.

iPhone or iPad running Safari

Users 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, tap and hold the back arrow.
3. The page that opens contains your browser's history.