Computer Networking

A computer network is a set of computers sharing resources located on or provided by network nodes. The computers use common communication protocols over digital interconnections to communicate with each other.

LAN (Local area network)- A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school

MAN (Metropolitan area network) - A MAN is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings. A MAN is larger than a local area network (LAN) but smaller than a wide area network (WAN).

WAN (Wide area network)- In its simplest form, a wide-area network (WAN) is a collection of local-area networks (LANs) or other networks that communicate with one another. A WAN is essentially a network of networks, with the Internet the world's largest WAN.

Wi-Fi (Wireless Fidelity) - Wi-Fi is a family of wireless network protocols, which are commonly used for local area networking of devices and Internet access, allowing nearby digital devices to exchange data by radio waves. These are the most widely used computer networks in the world, used globally in home and small office networks to link desktop and laptop computers, tablet computers, smartphones, smart TVs, printers, and smart speakers together and to a wireless router to connect them to the Internet, and in wireless access points in public places like coffee shops, hotels, libraries and airports to provide the public Internet access for mobile devices.

Switching

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission. Switching technique is used to connect the systems for making one-to-one communication.

Circuit Switching -

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Packet Switching -

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.

Components involved in Computer Network

- **Hosts −** Hosts are said to be situated at ultimate end of the network, i.e. a host is a source of information and another host will be the destination. Information flows end to end between hosts. A host can be a user’s PC, an internet Server, a database server etc.

- **Media −** If wired, then it can be copper cable, fiber optic cable, and coaxial cable.If wireless, it can be free-to-air radio frequency or some special wireless band. Wireless frequencies can be used to interconnect remote sites too.

- **Hub −** A hub is a multiport repeater and it is used to connect hosts in a LAN segment. Because of low throughputs hubs are now rarely used. Hub works on Layer-1 (Physical Layer) of OSI Model.

- **Switch −** A Switch is a multiport bridge and is used to connect hosts in a LAN segment. Switches are much faster than Hubs and operate on wire speed. Switch works on Layer-2 (Data Link Layer), but Layer-3 (Network Layer) switches are also available.

- **Router −** A router is Layer-3 (Network Layer) device which makes routing decisions for the data/information sent for some remote destination. Routers make the core of any interconnected network and the Internet.

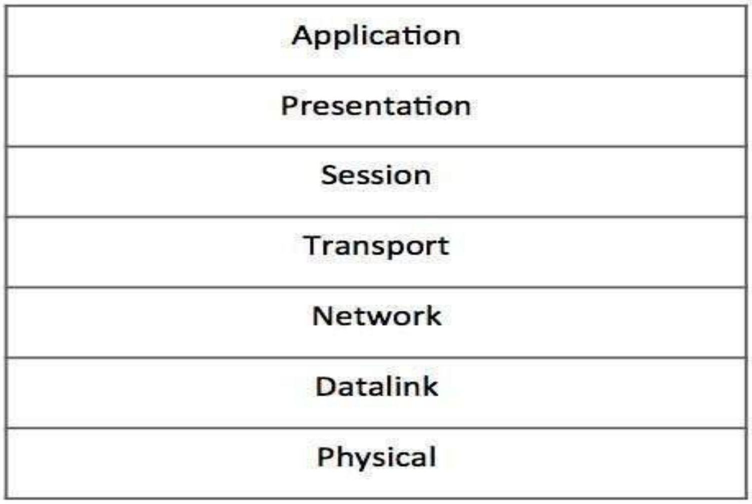
- **Gateways −** A software or combination of software and hardware put together, works for exchanging data among networks which are using different protocols for sharing data.

- **Firewall −** Software or combination of software and hardware, used to protect users data from unintended recipients on the network/internet.

Open System Interconnection (OSI Model)

The International Standard Organization has a well-defined model for Communication Systems known as Open System Interconnection, or the OSI Model. This layered model is a conceptualized view of how one system should communicate with the other, using various protocols defined in each layer. Further, each layer is designated to a well-defined part of communication system. For example, the Physical layer defines all the components of physical nature, i.e. wires, frequencies, pulse codes, voltage transmission etc. of a communication system.

The OSI Model has the following seven layers −



Application
Presentation
Session
Transport
Network
Datalink
Physical

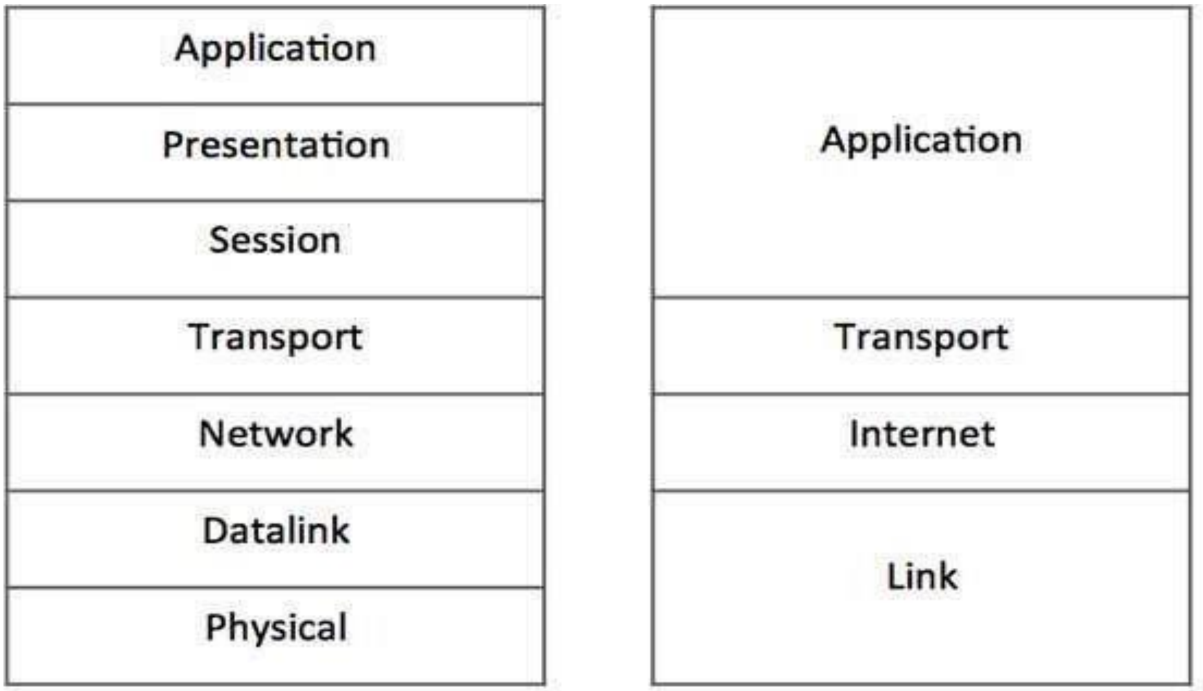
- **Physical Layer (Layer-1) −** This layer deals with hardware technology and actual communication mechanism such as signaling, voltage, cable type and length, etc.
- **Data Link Layer (Layer-2) −** This layer takes the raw transmission data (signal, pulses etc.) from the Physical Layer and makes Data Frames, and sends that to the upper layer and vice versa. This layer also checks any transmission errors and sorts it out accordingly.
- **Network Layer (Layer-3) −** This layer helps to uniquely identify hosts beyond the subnets and defines the path which the packets will follow or be routed to reach the destination.
- **Transport Layer (Layer-4) −** This layer provides end to end data delivery among hosts. This layer takes data from the above layer and breaks it into smaller units called Segments and then gives it to the Network layer for transmission.
- **Session Layer (Layer-5) −** This layer provides session management capabilities between hosts. For example, if some host needs a password verification for access and if credentials are provided then for that session password verification

does not happen again. This layer can assist in synchronization, dialog control and critical operation management (e.g., an online bank transaction).

- **Presentation Layer (Layer-6) −** This layer helps to understand data representation in one form on a host to other host in their native representation. Data from the sender is converted to on-the-wire data (general standard format) and at the receiver's end it is converted to the native representation of the receiver.
- **Application Layer (Layer-7) −** This is where the user application sits that needs to transfer data between or among hosts. For example − HTTP, file transfer application (FTP) and electronic mail etc.

TCP / IP

A majority of the internet uses a protocol suite called the Internet Protocol Suite also known as the TCP/IP protocol suite. This suite is a combination of protocols which encompasses a number of different protocols for different purpose and need. Because the two major protocols in this suites are TCP (Transmission Control Protocol) and IP (Internet Protocol), this is commonly termed as TCP/IP Protocol suite. This protocol suite has its own reference model which it follows over the internet. In contrast with the OSI model, this model of protocols contains less layers.



OSI Reference Model

TCP/IP Reference Model

This model is indifferent to the actual hardware implementation, i.e. the physical layer of OSI Model. This is why this model can be implemented on almost all underlying technologies. Transport and Internet layers correspond to the same peer layers. All three top layers of OSI Model are compressed together in single Application layer of TCP/IP Model.

OSI Model	**TCP/IP Model**
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI layers have seven layers.	TCP/IP has four layers.
In the OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are a part of the OSI model.	There is no session and presentation layer in the TCP model.
It is defined after the advent of the Internet.	It is defined before the advent of the internet.

IP Address

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

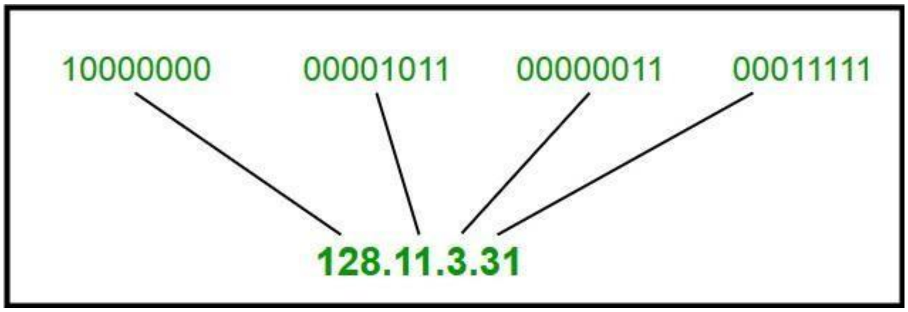
IP addresses are not random. They are mathematically produced and allocated by the Internet Assigned Numbers Authority (**IANA**), a division of the Internet Corporation for Assigned Names and Numbers (**ICANN**).

A **Private IP** address is the address your network router assigns to your device. Each device within the same network is assigned a unique private IP address (sometimes called a private network address) — this is how devices on the same internal network talk to each other.

A **Public IP** address is an IP address that can be accessed directly over the internet and is assigned to your network router by your internet service provider (ISP). Your personal device also has a private IP that remains hidden when you connect to the internet through your router's public IP.

IP Addressing

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IPv4 address is a 32-bit unique address having an address space of 2^{32}.

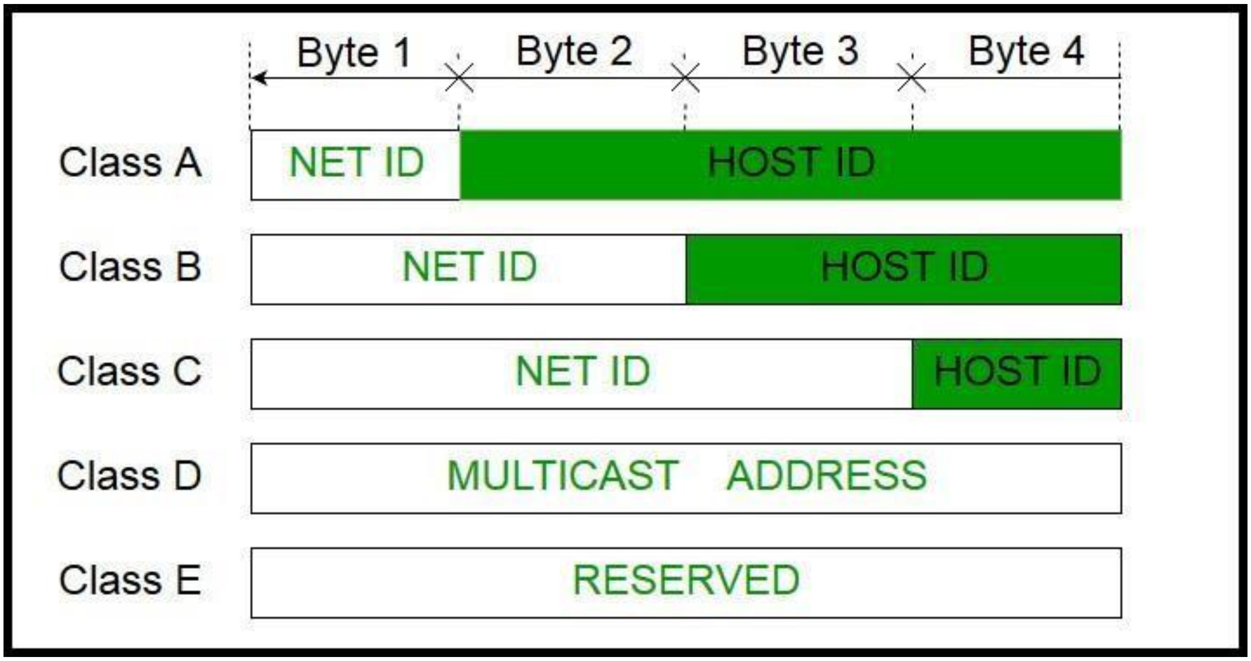


The 32 bit IPv4 address is divided into five sub-classes. These are:

- Class A
- Class B
- Class C
- Class D
- Class E

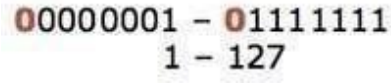
Again, IPv4 address is divided into two parts:

- **Network ID**
- **Host ID**



Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.



00000001 – 01111111
1 – 127

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.IP 0.0.0.0 is is a non-routable meta-address used to designate an invalid, unknown, or non applicable target.

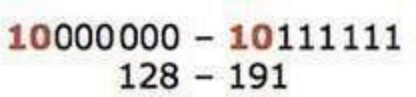
The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^{7}-2) and 16777214 hosts (2^{24}-2).

Class A IP address format is thus:

0NNNNNNN .HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.



10000000 - 10111111
128 - 191

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

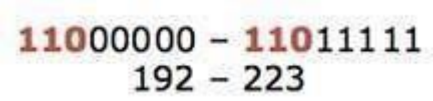
Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.

Class B IP address format is:

10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is −



11000000 - 11011111
192 - 223

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

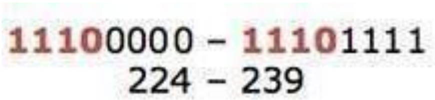
Class C gives 2097152 (2^{21}) Network addresses and 254 (2^{8}-2) Host addresses.

Class C IP address format is:

110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of −



11100000 - 11101111
224 - 239

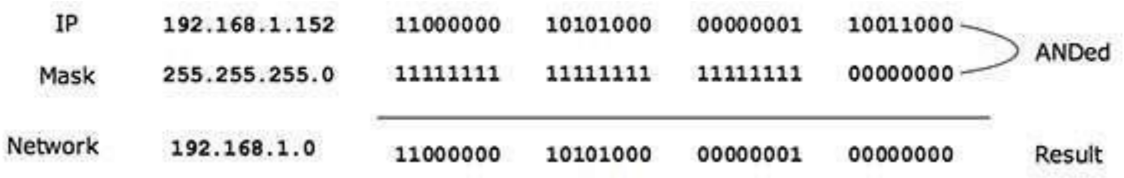
Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

Subnet Mask

The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its Subnet Mask, the result yields the Network address. For example, say the IP Address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then −



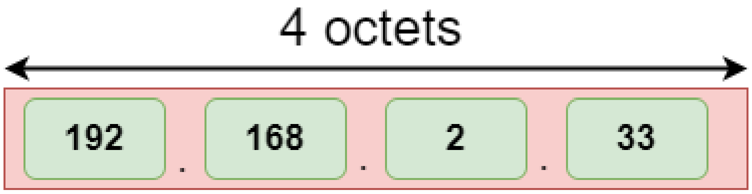
IP	192.168.1.152	11000000	10101000	00000001	10011000	ANDed
Mask	255.255.255.0	11111111	11111111	11111111	00000000	
Network	192.168.1.0	11000000	10101000	00000001	00000000	Result

This way the Subnet Mask helps extract the Network ID and the Host from an IP Address. It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.

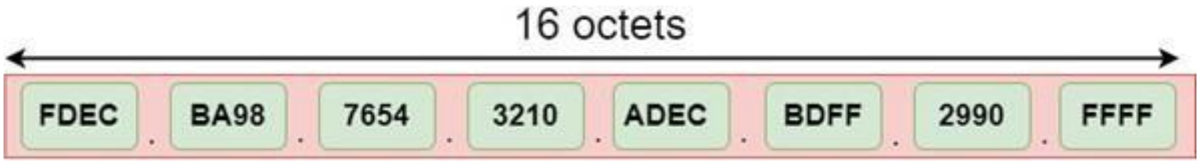
Drawback - Currently, the population of the world is 7.6 billion. Every user is having more than one device connected with the internet, and private companies also rely on the internet. As we know that IPv4 produces 4 billion addresses, which are not enough for each device connected to the internet on a planet. Although the various techniques were invented, such as variable- length mask, network address translation, port address translation, classes, inter-domain translation, to conserve the bandwidth of IP address and slow down the depletion of an IP address. In these techniques, public IP is converted into a private IP due to which the user having public IP can also use the internet. But still, this was not so efficient, so it gave rise to the development of the next generation of IP addresses, i.e., IPv6.

IPv6 Address -

The address format of IPv4



The address format of IPv6



The above diagram shows the address format of IPv4 and IPv6. An IPv4 is a 32-bit decimal address. It contains 4 octets or fields separated by 'dot', and each field is 8-bit in size. The number that each field contains should be in the range of 0-255. Whereas an IPv6 is a 128-bit hexadecimal address. It contains 8 fields separated by a colon, and each field is 16-bit in size.

Different types of Ports

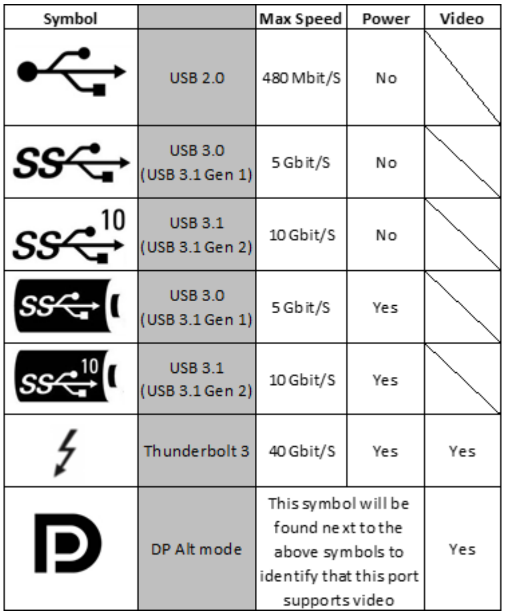
Serial Port - In computing, a serial port is a serial communication interface through which information transfers in or out sequentially one bit at a time. This is in contrast to a parallel port, which communicates multiple bits simultaneously in parallel.

Parallel Port - In computing, a parallel port was a type of interface found on computers for connecting peripherals. The name refers to the way the data is sent; parallel ports send multiple bits of data at once, as opposed to serial communication, in which bits are sent one at a time

shutterstock.com · 1933326275

Ethernet Port -An Ethernet port (also called a jack or socket) is an opening on computer network equipment that Ethernet cables plug into. Their purpose is to connect wired network hardware in an Ethernet LAN, metropolitan area network (MAN), or wide area network (WAN).

USB Port -A USB port is a standard cable connection interface for personal computers and consumer electronics devices. USB stands for Universal Serial Bus, an industry standard for short-distance digital data communications. USB ports allow USB devices to be connected to each other with and transfer digital data over USB cables



Symbol		Max Speed	Power	Video
	USB 2.0	480 Mbit/S	No	
SS	USB 3.0 (USB 3.1 Gen 1)	5 Gbit/S	No	
SS 10	USB 3.1 (USB 3.1 Gen 2)	10 Gbit/S	No	
SS	USB 3.0 (USB 3.1 Gen 1)	5 Gbit/S	Yes	
SS 10	USB 3.1 (USB 3.1 Gen 2)	10 Gbit/S	Yes	
⚡	Thunderbolt 3	40 Gbit/S	Yes	Yes
D	DP Alt mode	This symbol will be found next to the above symbols to identify that this port supports video		Yes

HDMI (High-Definition Multimedia Interface)-

It is proprietary audio/video interface for transmitting uncompressed video data and compressed or uncompressed digital audio data from an HDMI-compliant source device, such as a display controller, to a compatible computer monitor, video projector, digital television, or digital audio device.

SAS - In computing, Serial Attached SCSI (**S A Small Computer System Interface**) is a point-to-point serial protocol that moves data to and from computer-storage devices such as hard disk drives and tape drives SAS, like its predecessor, uses the standard SCSI command set.

<u>Wireless Modem-</u> A wireless modem is a modem that bypasses the telephone system and connects directly to a wireless network, through which it can directly access the Internet connectivity provided by an Internet service provider (ISP).

Cables

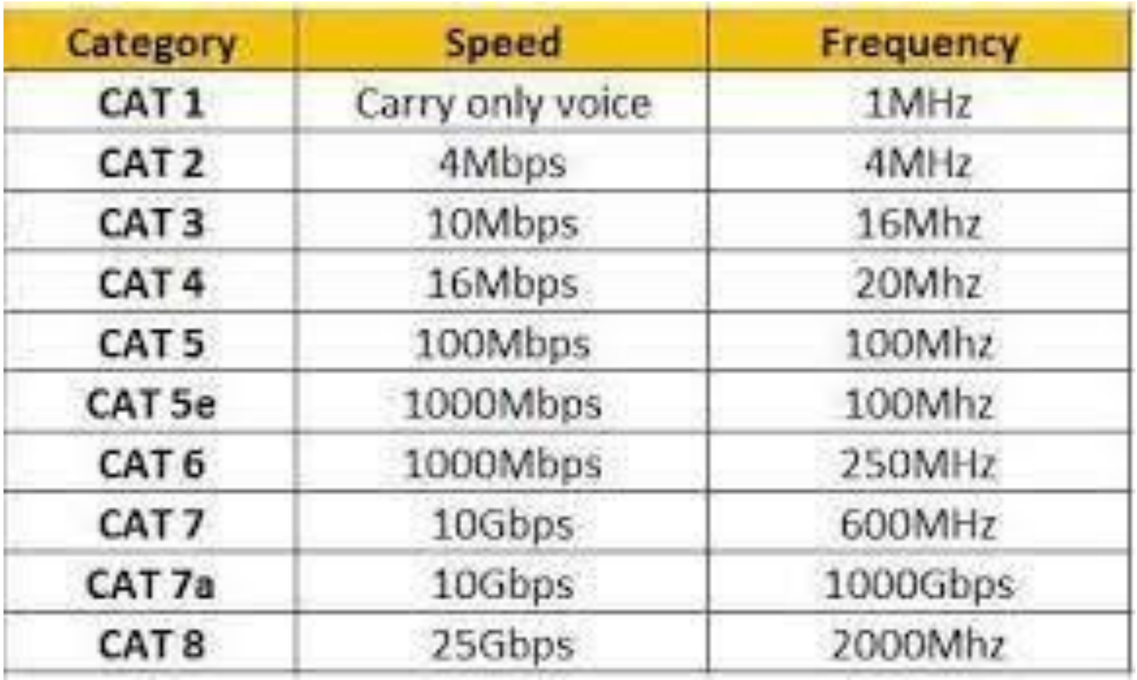
RS-232- In telecommunications, RS-232, Recommended Standard 232 is a standard originally introduced in 1960 for serial communication transmission of data. It formally defines signals connecting between a *DTE* (*data terminal equipment*) such as a computer terminal, and a *DCE* (*data circuit-terminating equipment* or *data communication equipment*), such as a modem.

RS-422- It also known as TIA/EIA-422, is a technical standard originated by the Electronic Industries Alliance that specifies electrical characteristics of a digital signaling circuit. It was intended to replace the older RS-232C standard with a standard that offered much higher speed, better immunity from noise, and longer cable lengths. RS-422 systems can transmit data at rates as high as 10 Mbit/s, or may be sent on cables as long as 1,200 meters at lower rates. It is closely related to RS-423.

RS-485- It is also known as TIA-485(-A) or EIA-485, is a standard defining the electrical characteristics of drivers and receivers for use in serial communications systems. Electrical signaling is balanced, and multipoint systems are supported. The standard is jointly published by the Telecommunications Industry Association and Electronic Industries Alliance (TIA/EIA). Digital communications networks implementing the standard can be used effectively over long distances and in electrically noisy environments. Multiple receivers may be connected to such a network in a linear, multidrop bus. These characteristics make RS-485 useful in industrial control systems and similar applications, used the same signaling systems but on a different wiring arrangement.

RJ 45 - RJ abbreviated for the **Registered Jack**. RJ45 is a type of cable connector which is mainly used in computer networks. RJ45 is mainly used for ethernet networking which is used to connect different type of devices like a swit ch, hub, PC, router, firewall to each other.

CAT Cables - A variety of different cables are available for Ethernet and other telecommunications and networking applications. These network cables that are described by their different categories, e.g. Cat 5 cables, Cat-6 cables, etc., which are often recognized by the TIA (telecommunications Industries Association) and they are summarized below:



Category	Speed	Frequency
CAT 1	Carry only voice	1MHz
CAT 2	4Mbps	4MHz
CAT 3	10Mbps	16Mhz
CAT 4	16Mbps	20Mhz
CAT 5	100Mbps	100Mhz
CAT 5e	1000Mbps	100Mhz
CAT 6	1000Mbps	250MHz
CAT 7	10Gbps	600MHz
CAT 7a	10Gbps	1000Gbps
CAT 8	25Gbps	2000Mhz

MODEM

A modulator-demodulator or modem is a computer hardware device that converts data from a digital format into a format suitable for an analog transmission medium such as telephone or radio. A modem transmits data by modulating one or more carrier wave signals to encode digital information, while the receiver demodulates the signal to recreate the original digital information. The **modulator** part of the modem converts digital signals to analog signals, and the **demodulator** part converts analog signals to digital signals.

Types of Modem

Wireless Modem: Wireless Modem is also known as "**Radiofrequency Modem**", and these modems are developed to work with cellular technology and wireless **local area networks.**

Fax Modem: Fax modem is used for transmitting and receiving any document over the telephone line, and this modem works like as fax machine.

Dial-up Modem: Dial-up modems transmits analog signal via telephone lines.

Functions of Modem

Here, we will explain various **functions of modem in computer networking**, such as –

Data Compression: To decrease the amount of time when it try to send data and for cutting down on the percentages of errors in the all flowing of signals, then modem required the data compression mechanism. So, this data compression method helps to reduce the size of signals, which are required for sending data.

Error Correction: In the error correction techniques, all devices monitor all information while receiving is undamaged. It splits all information into small units that is called the "**Frames**". In this process, it tags all frames along with checksums, but it is done before sending information. Checksum is a special technique that helps to check redundancy in the presented data in the computer. If, this information matches with checksums then device grabs the verified information. That is sent by error-correcting modem. But, if it gets to fail in matching with checksum then information is moved back.

Flow Control: Each modem has different speed of sending signals. so, it can generate issues during to receive signals if any one device's speed down of them. So, in the flow control technique, slower one signals the faster one to pause, by sending a 'character'. If, slow device will try to send character to faster modem, then this character would be a signal to the faster modem for Pausing the information transfer until the slow modem gets caught up.

Modem Standards

V.21 Modem

This modem supports asynchronous transmission at rates up to 300 baud. Modulation is Frequency Shift Keying (FSK). In this modulation scheme, different carrier frequencies are used between the Originating and Answering modems. A Space is transmitted by a change in carrier frequency of +100 Hz. A Mark is represented by a change in carrier frequency of -100 Hz. For the carrier frequency of 1080 Hz, a Space is represented by a 1180 Hz signal and a Mark is represented by a 980 Hz signal. For the carrier frequency of 1750 Hz, a Space is represented by a 1850 Hz signal and a Mark is represented by a 1650 Hz signal.

V.22 Modem

This modulation is described in CCITT Recommendation. V.22 and FED-STD-1008! It utilizes Differential Phase Shift Keying (DPSK) and is designed for synchronous or asynchronous operation at 1200 BPS. Operation is full-duplex with different carrier frequencies used between the Originating and Answering modems.

The modem modulation rate is 600 bauds, with each baud representing two data bits.This modem modulation scheme supports a "fallback" rate of 600 BPS.

V.27 Modem

CCITT Recommendation V.27 describes a modulation scheme that is capable of supporting 4800 BPS, full-duplex, synchronous data. Operation may be full-duplex on a 4-Wire leased line or half-duplex on a 2-Wire, switched, voice circuit. The modulation scheme is known as D8PSK (Differential 8 Phase Shift Keying) and operates by breaking the incoming data stream into groups of three bits ("tribit"). These "tribits" are represented by one of eight possible phase shifts:

The modulation rate is 1600 bauds, with each baud representing three data bits.

The second and third releases of the V.27 Recommendation (V.27bis and V.27ter, respectively) added the ability to fallback to a 2400 BPS rate using V.26, Alternative "A" modulation. Also, the start-up/training times are reduced in the V.27bis Recommendation.

V.29 Modem

This modulation scheme was first standardized by the CCITT in 1976. It uses a form of Quadrature Amplitude Modulation (QAM), which transports data in groups of four bits ("quadbits"). V.29 modulation is capable of transporting synchronous data at rates up to9600 BPS. It operates full-duplex on a 4-Wire leased line or half-duplex on a 2-Wire, switched, voice line.

The V.29 modulation rate is 2400 bauds, with each baud representing four data bits.

V.32 Modem

First defined in 1984 by the CCITT, V.32 defines a modem that can support 9600 BPS asynchronous or synchronous data. Operation is full-duplex over a 2-Wire, switched, voice circuit. The modulation used may be Quadrature Amplitude Modulation (QAM), or QAM with Trellis coding. Trellis coding is actually a Forward Error Correcting (FEC) scheme.

V.34 Modem

It is capable of supporting full-duplex synchronous or asynchronous data over 4-Wire leased lines or 2-Wire circuits.

The modulation rate (baud or "symbol" rate) can vary. The carrier frequency can vary. The V.34 Recommendation also describes a "line probing" process that allows the modem to automatically setup optimally for any type of line connection. The training time has been reduced, but the modem will recover automatically from most line disturbances.

Modem & Routers - Modems and routers are fundamentally different devices. modems transform one type of data signal into a different type (one that is appropriate for devices within a local area network), whereas routers distribute the data received from the modem to smartphones, laptops, and other end devices in the network.

Routers also create and maintain local area networks, allowing multiple devices to communicate and share data with each other. A LAN can exist regardless of the availability of Internet access.

Modems, on the other hand, cannot create LANs, nor can they directly communicate with multiple devices. However, they are necessary in providing accessto the Internet.