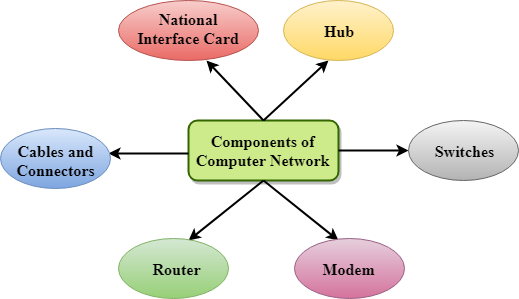
What is a Computer Network?

* **Computer Network** is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.
* The aim of the computer network is the sharing of resources among various devices.
* In the case of computer network technology, there are several types of networks that vary from simple to complex level.

Components Of Computer Network:



Major components of a computer network are:

NIC(National interface card)

NIC is a device that helps the computer to communicate with another device. The network interface card contains the hardware addresses, the data-link layer protocol use this address to identify the system on the network so that it transfers the data to the correct destination.

There are two types of NIC: wireless NIC and wired NIC.

* **Wireless NIC:** All the modern laptops use the wireless NIC. In Wireless NIC, a connection is made using the antenna that employs the **radio wave technology**.
* **Wired NIC:** Cables use the **wired NIC** to transfer the data over the medium.

Hub

Hub is a central device that splits the network connection into multiple devices. When computer requests for information from a computer, it sends the request to the Hub. Hub distributes this request to all the interconnected computers.

Switches

Switch is a networking device that groups all the devices over the network to transfer the data to another device. A switch is better than Hub as it does not broadcast the message over the network, i.e., it sends the message to the device for which it belongs to. Therefore, we can say that switch sends the message directly from source to the destination.

Cables and connectors

Cable is a transmission media that transmits the communication signals. **There are three types of cables:**

* **Twisted pair cable:** It is a high-speed cable that transmits the data over **1Gbps** or more.
* **Coaxial cable:** Coaxial cable resembles like a TV installation cable. Coaxial cable is more expensive than twisted pair cable, but it provides the high data transmission speed.
* **Fibre optic cable:** Fibre optic cable is a high-speed cable that transmits the data using light beams. It provides high data transmission speed as compared to other cables. It is more expensive as compared to other cables, so it is installed at the government level.

Router

Router is a device that connects the LAN to the internet. The router is mainly used to connect the distinct networks or connect the internet to multiple computers.

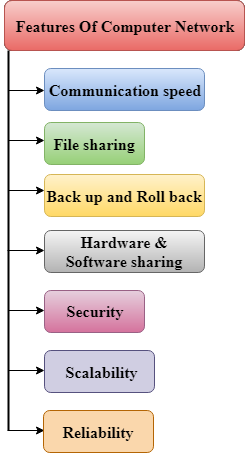
Modem

Modem connects the computer to the internet over the existing telephone line. A modem is not integrated with the computer motherboard. A modem is a separate part on the PC slot found on the motherboard.

Uses Of Computer Network

* **Resource sharing:** Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
* **Server-Client model:** Computer networking is used in the **server-client model**. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.
* **Communication medium:** Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.
* **E-commerce:** Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

Features Of Computer network



A list Of Computer network features is given below.

* Communication speed
* File sharing
* Back up and Roll back is easy
* Software and Hardware sharing
* Security
* Scalability
* Reliability

Communication speed

Network provides us to communicate over the network in a fast and efficient manner. For example, we can do video conferencing, email messaging, etc. over the internet. Therefore, the computer network is a great way to share our knowledge and ideas.

File sharing

File sharing is one of the major advantage of the computer network. Computer network provides us to share the files with each other.

Back up and Roll back is easy

Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.

Software and Hardware sharing

We can install the applications on the main server, therefore, the user can access the applications centrally. So, we do not need to install the software on every machine. Similarly, hardware can also be shared.

Security

Network allows the security by ensuring that the user has the right to access the certain files and applications.

Scalability

Scalability means that we can add the new components on the network. Network must be scalable so that we can extend the network by adding new devices. But, it decreases the speed of the connection and data of the transmission speed also decreases, this increases the chances of error occurring. This problem can be overcome by using the routing or switching devices.

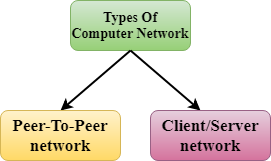
Reliability

Computer network can use the alternative source for the data communication in case of any hardware failure.

Computer Network Architecture

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

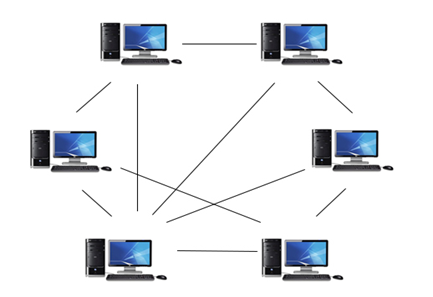
**The two types of network architectures are used:**



* Peer-To-Peer network
* Client/Server network

Peer-To-Peer network

* Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
* Peer-To-Peer network is useful for small environments, usually up to 10 computers.
* Peer-To-Peer network has no dedicated server.
* Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Advantages Of Peer-To-Peer Network:

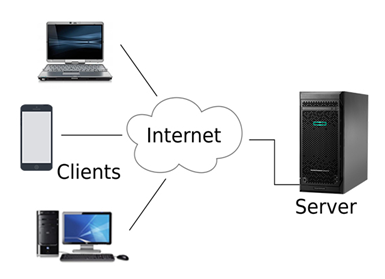
* It is less costly as it does not contain any dedicated server.
* If one computer stops working but, other computers will not stop working.
* It is easy to set up and maintain as each computer manages itself.

Disadvantages Of Peer-To-Peer Network:

* In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
* It has a security issue as the device is managed itself.

Client/Server Network

* Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
* The central controller is known as a **server** while all other computers in the network are called **clients**.
* A server performs all the major operations such as security and network management.
* A server is responsible for managing all the resources such as files, directories, printer, etc.
* All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Advantages Of Client/Server network:

* A Client/Server network contains the centralized system. Therefore we can back up the data easily.
* A Client/Server network has a dedicated server that improves the overall performance of the whole system.
* Security is better in Client/Server network as a single server administers the shared resources.
* It also increases the speed of the sharing resources.

Disadvantages Of Client/Server network:

* Client/Server network is expensive as it requires the server with large memory.
* A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
* It requires a dedicated network administrator to manage all the resources.

Computer Network Components

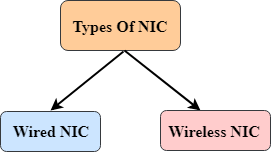
Computer network components are the *major parts* which are needed to *install the software*. Some important network components are **NIC**, **switch**, **cable**, **hub**, **router**, and **modem**. Depending on the type of network that we need to install, some network components can also be removed. For example, the wireless network does not require a cable.

Following are the major components required to install a network:

NIC

* NIC stands for network interface card.
* NIC is a hardware component used to connect a computer with another computer onto a network
* It can support a transfer rate of 10,100 to 1000 Mb/s.
* The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).

There are two types of NIC:



1. Wired NIC
2. Wireless NIC

**Wired NIC:** The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data.

**Wireless NIC:** The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC.

Play Video

Hub

A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.

The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

Switch

A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

Router

* A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
* A router works in a **Layer 3 (Network layer)** of the OSI Reference model.
* A router forwards the packet based on the information available in the routing table.
* It determines the best path from the available paths for the transmission of the packet.

Advantages Of Router:

* **Security:** The information which is transmitted to the network will traverse the entire cable, but the only specified device which has been addressed can read the data.
* **Reliability:** If the server has stopped functioning, the network goes down, but no other networks are affected that are served by the router.
* **Performance:** Router enhances the overall performance of the network. Suppose there are 24 workstations in a network generates a same amount of traffic. This increases the traffic load on the network. Router splits the single network into two networks of 12 workstations each, reduces the traffic load by half.
* **Network range**

Modem

* A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
* A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.
* It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

Based on the differences in speed and transmission rate, a modem can be classified in the following categories:

* Standard PC modem or Dial-up modem
* Cellular Modem
* Cable modem

Cables and Connectors

Cable is a transmission media used for transmitting a signal.

There are three types of cables used in transmission:

* Twisted pair cable
* Coaxial cable
* Fibre-optic cable

Computer Network Types

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



* LAN(Local Area Network)
* PAN(Personal Area Network)
* MAN(Metropolitan Area Network)
* WAN(Wide Area Network)

LAN(Local Area Network)

* Local Area Network is a group of computers connected to each other in a small area such as building, office.
* LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
* It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
* The data is transferred at an extremely faster rate in Local Area Network.
* Local Area Network provides higher security.



PAN(Personal Area Network)

* Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
* Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
* **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
* Personal Area Network covers an area of **30 feet**.
* Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.



**There are two types of Personal Area Network:**



* Wired Personal Area Network
* Wireless Personal Area Network

**Wireless Personal Area Network:** Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

**Wired Personal Area Network:** Wired Personal Area Network is created by using the USB.

Examples Of Personal Area Network:

* **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.
* **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.
* **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

MAN(Metropolitan Area Network)

* A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
* Government agencies use MAN to connect to the citizens and private industries.
* In MAN, various LANs are connected to each other through a telephone exchange line.
* The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
* It has a higher range than Local Area Network(LAN).



Uses Of Metropolitan Area Network:

* MAN is used in communication between the banks in a city.
* It can be used in an Airline Reservation.
* It can be used in a college within a city.
* It can also be used for communication in the military.

WAN(Wide Area Network)

* A Wide Area Network is a network that extends over a large geographical area such as states or countries.
* A Wide Area Network is quite bigger network than the LAN.
* A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
* The internet is one of the biggest WAN in the world.
* A Wide Area Network is widely used in the field of Business, government, and education.



Examples Of Wide Area Network:

* **Mobile Broadband:** A 4G network is widely used across a region or country.
* **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
* **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

* **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
* **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
* **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
* **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
* **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
* **Global business:** We can do the business over the internet globally.
* **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

* **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
* **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
* **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
* **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Internetwork

* An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as **internetworking**.
* An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.
* An internetworking uses the **internet protocol**.
* The reference model used for internetworking is **Open System Interconnection(OSI)**.

Types Of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it must have one connection to the external network.

2. **Intranet:** An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Intranet advantages:

* **Communication:** It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.
* **Time-saving:** Information on the intranet is shared in real time, so it is time-saving.
* **Collaboration:** Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.
* **Platform independency:** It is a neutral architecture as the computer can be connected to another device with different architecture.
* **Cost effective:** People can see the data and documents by using the browser and distributes the duplicate copies over the intranet. This leads to a reduction in the cost.

What are network devices?

Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network.

Types of network devices

Here is the common network device list:

Hub

Switch

Router

Bridge

Gateway

Modem

Repeater

Access Point

Hub

Hubs connect multiple computer networking devices together. A hub also acts as a repeater in that it amplifies signals that deteriorate after traveling long distances over connecting cables. A hub is the simplest in the family of network connecting devices because it connects LAN components with identical protocols.

A hub can be used with both digital and analog data, provided its settings have been configured to prepare for the formatting of the incoming data. For example, if the incoming data is in digital format, the hub must pass it on as packets; however, if the incoming data is analog, then the hub passes it on in signal form.

Hubs do not perform packet filtering or addressing functions; they just send data packets to all connected devices. Hubs operate at the Physical layer of the Open Systems Interconnection (OSI) model. There are two types of hubs: simple and multiple port.

Switch

Switches generally have a more intelligent role than hubs. A switch is a multiport device that improves network efficiency. The switch maintains limited routing information about nodes in the internal network, and it allows connections to systems like hubs or routers. Strands of LANs are usually connected using switches. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination.

Using switches improves network efficiency over hubs or routers because of the virtual circuit capability. Switches also improve network security because the virtual circuits are more difficult to examine with network monitors. You can think of a switch as a device that has some of the best capabilities of routers and hubs combined. A switch can work at either the Data Link layer or the Network layer of the OSI model. A multilayer switch is one that can operate at both layers, which means that it can operate as both a switch and a router. A multilayer switch is a high-performance device that supports the same routing protocols as routers.

Switches can be subject to distributed denial of service (DDoS) attacks; flood guards are used to prevent malicious traffic from bringing the switch to a halt. Switch port security is important so be sure to secure switches: Disable all unused ports and use DHCP snooping, ARP inspection and MAC address filtering.

Router

Routers help transmit packets to their destinations by charting a path through the sea of interconnected networking devices using different network topologies. Routers are intelligent devices, and they store information about the networks they’re connected to. Most routers can be configured to operate as packet-filtering firewalls and use access control lists (ACLs). Routers, in conjunction with a channel service unit/data service unit (CSU/DSU), are also used to translate from LAN framing to WAN framing. This is needed because LANs and WANs use different network protocols. Such routers are known as border routers. They serve as the outside connection of a LAN to a WAN, and they operate at the border of your network.

Router are also used to divide internal networks into two or more subnetworks. Routers can also be connected internally to other routers, creating zones that operate independently. Routers establish communication by maintaining tables about destinations and local connections. A router contains information about the systems connected to it and where to send requests if the destination isn’t known. Routers usually communicate routing and other information using one of three standard protocols: Routing Information Protocol (RIP), Border Gateway Protocol (BGP) or Open Shortest Path First (OSPF).

Routers are your first line of defense, and they must be configured to pass only traffic that is authorized by network administrators. The routes themselves can be configured as static or dynamic. If they are static, they can only be configured manually and stay that way until changed. If they are dynamic, they learn of other routers around them and use information about those routers to build their routing tables.

Routers are general-purpose devices that interconnect two or more heterogeneous networks. They are usually dedicated to special-purpose computers, with separate input and output network interfaces for each connected network. Because routers and gateways are the backbone of large computer networks like the internet, they have special features that give them the flexibility and the ability to cope with varying network addressing schemes and frame sizes through segmentation of big packets into smaller sizes that fit the new network components. Each router interface has its own Address Resolution Protocol (ARP) module, its own LAN address (network card address) and its own Internet Protocol (IP) address. The router, with the help of a routing table, has knowledge of routes a packet could take from its source to its destination. The routing table, like in the bridge and switch, grows dynamically. Upon receipt of a packet, the router removes the packet headers and trailers and analyzes the IP header by determining the source and destination addresses and data type, and noting the arrival time. It also updates the router table with new addresses not already in the table. The IP header and arrival time information is entered in the routing table. Routers normally work at the Network layer of the OSI model.

Bridge

Bridges are used to connect two or more hosts or network segments together. The basic role of bridges in network architecture is storing and forwarding frames between the different segments that the bridge connects. They use hardware Media Access Control (MAC) addresses for transferring frames. By looking at the MAC address of the devices connected to each segment, bridges can forward the data or block it from crossing. Bridges can also be used to connect two physical LANs into a larger logical LAN.

Bridges work only at the Physical and Data Link layers of the OSI model. Bridges are used to divide larger networks into smaller sections by sitting between two physical network segments and managing the flow of data between the two.

Bridges are like hubs in many respects, including the fact that they connect LAN components with identical protocols. However, bridges filter incoming data packets, known as frames, for addresses before they are forwarded. As it filters the data packets, the bridge makes no modifications to the format or content of the incoming data. The bridge filters and forwards frames on the network with the help of a dynamic bridge table. The bridge table, which is initially empty, maintains the LAN addresses for each computer in the LAN and the addresses of each bridge interface that connects the LAN to other LANs. Bridges, like hubs, can be either simple or multiple port.

Bridges have mostly fallen out of favor in recent years and have been replaced by switches, which offer more functionality. In fact, switches are sometimes referred to as “multiport bridges” because of how they operate.

Gateway

Gateways normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous protocols and standards from different vendors; gateways are used to deal with them. Gateways provide translation between networking technologies such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). Because of this, gateways connect two or more autonomous networks, each with its own routing algorithms, protocols, topology, domain name service, and network administration procedures and policies.

Gateways perform all of the functions of routers and more. In fact, a router with added translation functionality is a gateway. The function that does the translation between different network technologies is called a protocol converter.

Modem

Modems (modulators-demodulators) are used to transmit digital signals over analog telephone lines. Thus, digital signals are converted by the modem into analog signals of different frequencies and transmitted to a modem at the receiving location. The receiving modem performs the reverse transformation and provides a digital output to a device connected to a modem, usually a computer. The digital data is usually transferred to or from the modem over a serial line through an industry standard interface, RS-232. Many telephone companies offer DSL services, and many cable operators use modems as end terminals for identification and recognition of home and personal users. Modems work on both the Physical and Data Link layers.

Repeater

A repeater is an electronic device that amplifies the signal it receives. You can think of repeater as a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances, more than 100 meters for standard LAN cables. Repeaters work on the Physical layer.

Access Point

While an access point (AP) can technically involve either a wired or wireless connection, it commonly means a wireless device. An AP works at the second OSI layer, the Data Link layer, and it can operate either as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another.

Wireless access points (WAPs) consist of a transmitter and receiver (transceiver) device used to create a wireless LAN (WLAN). Access points typically are separate network devices with a built-in antenna, transmitter and adapter. APs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired Ethernet LAN. They also have several ports, giving you a way to expand the network to support additional clients. Depending on the size of the network, one or more APs might be required to provide full coverage. Additional APs are used to allow access to more wireless clients and to expand the range of the wireless network. Each AP is limited by its transmission range — the distance a client can be from an AP and still obtain a usable signal and data process speed. The actual distance depends on the wireless standard, the obstructions and environmental conditions between the client and the AP. Higher end APs have high-powered antennas, enabling them to extend how far the wireless signal can travel.

APs might also provide many ports that can be used to increase the network’s size, firewall capabilities and Dynamic Host Configuration Protocol (DHCP) service. Therefore, we get APs that are a switch, DHCP server, router and firewall.

To connect to a wireless AP, you need a service set identifier (SSID) name. 802.11 wireless networks use the SSID to identify all systems belonging to the same network, and client stations must be configured with the SSID to be authenticated to the AP. The AP might broadcast the SSID, allowing all wireless clients in the area to see the AP’s SSID. However, for security reasons, APs can be configured not to broadcast the SSID, which means that an administrator needs to give client systems the SSID instead of allowing it to be discovered automatically. Wireless devices ship with default SSIDs, security settings, channels, passwords and usernames. For security reasons, it is strongly recommended that you change these default settings as soon as possible because many internet sites list the default settings used by manufacturers.

Access points can be fat or thin. Fat APs, sometimes still referred to as autonomous APs, need to be manually configured with network and security settings; then they are essentially left alone to serve clients until they can no longer function. Thin APs allow remote configuration using a controller. Since thin clients do not need to be manually configured, they can be easily reconfigured and monitored. Access points can also be controller-based or stand-alone.

What are servers?

Servers are large data storage and processing devices that exist either as hardware or as virtual storehouses located on the internet. Computers or software systems act as servers that connect to a network.

A server can be any type of device that shares and saves information. Servers can both store and process information within their own system or request it from another.

Servers began as small devices that simply transferred data to a more functional computer then grew in size and ability to perform more complex functions. Now, virtual servers exist within cloud computing platforms that are housed on the internet.

Related: Everything You Need To Know About Computer Networking

Types of servers

The following is a list of all the main types of servers:

1. Web server

An open-source web server is used for accessing the world wide web through public domain software. These servers connect stored information from an internet website to your own computer. Web servers store information for the internet that is retrieved via "HTTP" code and sent to your web browser. This is one of the most widely used types of servers.

Related: HTTP vs. HTTPS: Learning the Differences Between Them

2. Proxy server

Proxy servers act as a bridge between a host server and a client server. A proxy sends data from a website to your computer IP address after it passes through the proxy's server. This practice adds a layer of security since the information is requested then transferred from the source to the proxy server and never directly from a client to another user. A proxy server can filter out various harmful internet entities.

3. Virtual machine (VM)

As their name suggests, virtual machines store and connect data strictly through virtual space. To create a virtual machine, IT teams use a hypervisor, also known as a virtual machine monitor (VMM), which is software that can run thousands of virtual machines through only one piece of physical hardware. This method of server virtualization is widely used for data transfer and storage because they are the most cost-effective type of server to run.

4. File transfer protocol (FTP) server

FTP servers are used to relocate files from one computer to another. Uploaded files move from your computer to the server while downloaded files are extracted from the server onto your device. File transfer protocol also refers to the method of using a server to connect one computer to another in order to share data safely.

5. Application server

These servers connect clients to software applications through virtual server connections. This allows users to bypass downloading data to their own hardware in order to access applications. Application servers can effectively host large amounts of application data to many users at once, making them ideal for businesses.

Related: What Is a Web Application? How It Works, Benefits and Examples

6. File server

A file server stores data files for multiple users. They allow for faster data retrieval and saving or writing files to a computer. This is a basic type of server used commonly by organizations where lots of users need access to files that are more conveniently and safely stored on a server than a personal computer.

7. Database server

Database servers function as large storage spaces that organizations use and access to run multiple programs to meet their needs. A database server can run independently of any database architecture.

8. Mail server

A mail server stores and delivers mail for clients through email service platforms. Because mail servers are set up to continually connect to a network, individual users can access their email without running any systems through their own devices.

9. Print server

A print server connects remotely to local computers to print through a network. These servers give businesses the ability to use a single printer to serve an entire department. Some printers even come with their own built-in server ready to join a network once they're installed in an office area.

10. Domain name system (DNS) server

These servers transform readable computer domain names into computer language IP addresses. The DNS server takes search data from a user and finds the requested address to deliver to the client device.

11. Collaboration server

When work needs to be shared across multiple users, a collaboration server makes it easy to connect. These servers allow you to share and store files, applications and other large amounts of data.

12. Gaming server

Large gaming networks use servers to connect users from around the world. These servers host multi-player online games.

13. Monitoring and management server

Monitoring and management servers function in several capacities. First, they record and track digital transactions and receive user requests. Others simply monitor and don't actively participate in user operations. Monitoring servers are responsive to network administrators who survey network health to check for threats or bugs in the system.

How do servers work?

Servers work in several ways to connect users to different data functions. They house large amounts of data for organizations and make it accessible to users through internal networks or via the internet. They respond to user requests to retrieve appropriate files from stored or interconnected data sources. They also work in tandem with an operating system to better listen to and respond to user requests.

IT professionals can increase the functionality of a server by installing software that creates additional roles such as responding to website requests from an internet browser. Servers can also act as safeguards to verify the identity of users before allowing access to a network.

Server components

Physical servers are made up of the following parts:

Motherboard: A motherboard connects all parts of a server. A motherboard's size dictates the amount of storage and the number of hard drives that can connect to a server.

Central Processing Unit (CPU): The CPU controls the overall functions of a server. It's the center for all processing within a server device. CPUs are measured by processing speed.

Memory: This part of a server dictates the amount of storage available. Memory needs to be compatible with the motherboard.

Hard drives: A hard drive stores both user and software data for a computer. It uses a controller card for optimum processing functions. A server housing large amounts of data may need multiple hard drives.

Network connection: A server needs to connect to a network in order to function. A good network connection will ensure a server is able to receive and respond to user requests. Many motherboards already contain a network adapter however, if they don't, the server will need an external network connection installed.

Power supply: Servers that provide data to large numbers of clients need a bigger power supply than a typical personal computer. Most servers need a power supply of at least 300 watts.

# Types of Internet Connection

There are many connections that can be used for internet access. All the connections have their own speed range that can be used for different purposes like for home, or for personal use.

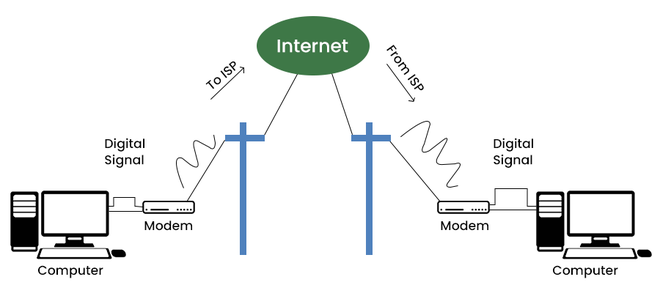
In this article, we will discuss different types of internet connections.

### Dial-Up Connection

A [dial-up connection](https://www.geeksforgeeks.org/difference-between-dialup-and-broadband-connection/) is established between your computer and the ISP server using a modem.

A dial-Up Connection is a cheap and traditional connection that is not preferred these days as this type of connection is very slow.

To access the internet connection in the dial-up connection we need to dial a phone number on the computer and that’s why it requires a telephone connection. It requires a modem to set up a dial-up connection, which works as interference between your computer and the telephone line. In this connection, we can use either an internet connection or telephone at a time.

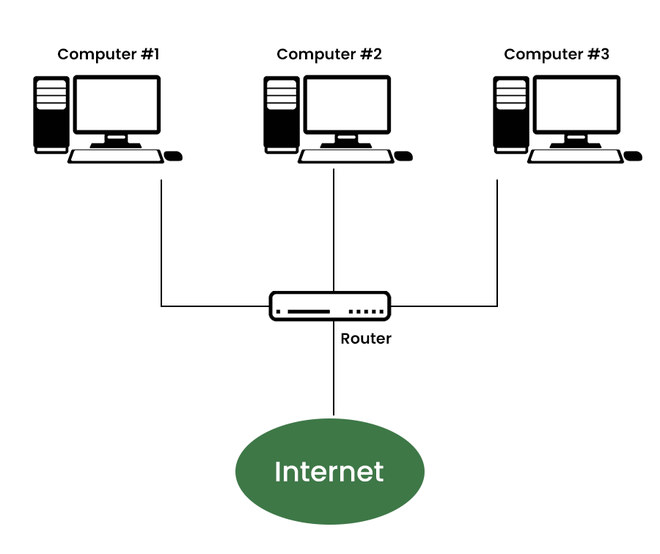


*Dial Up Connection*

### Broadband Connection

Broadband refers to high-speed internet access that is faster than traditional dial-up access. It is provided through either cable or telephone composition. It does not require any telephone connection that’s why here we can use telephone and internet connection simultaneously. In this connection, more than one person can access the internet connection simultaneously.

It is a wide bandwidth data transmission that transports several signals and traffic types. In this connection, the medium used is coaxial cable, optical fiber cable, radio, or twisted pair cable.

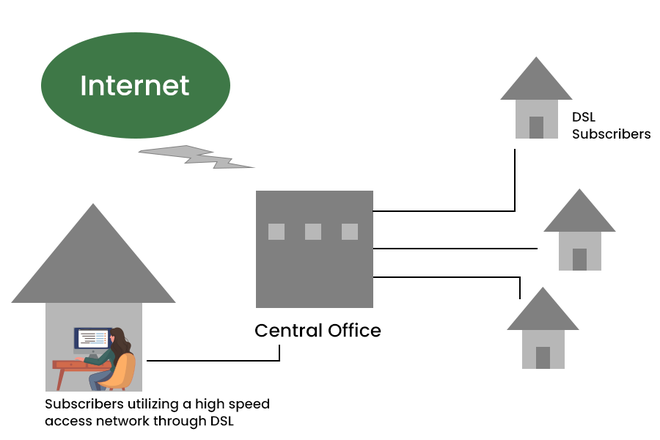


*Broadband Connection*

### ****DSL****

DSL stands for [Digital Subscriber Line](https://www.geeksforgeeks.org/digital-subscriber-line-dsl/). It provides an internet connection through the telephone line(network). DSL is a form of broadband communication that is always on, there is no need to dial a phone number to connect. DSL connection uses a router to transport data and the speed of this connection range between 128k to 8Mbps depending on the service offered. A DSL connection can translate data at 5 million bytes per second, or 5mbps.

DSL service can be delivered simultaneously with wired telephone service on the same telephone line due to high-frequency bands for data.

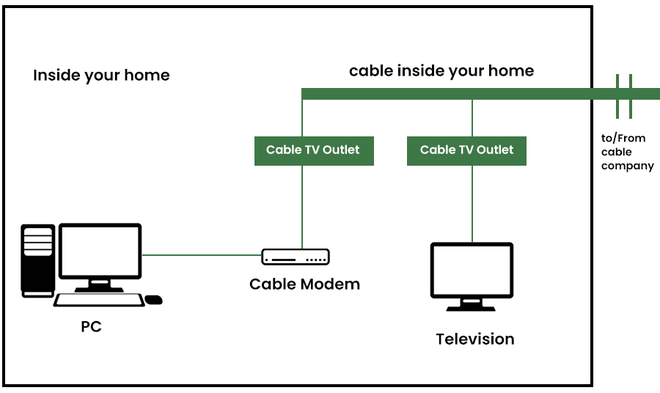


*DSL*

### Cable

It is a form of broadband access cable modem that can provide extremely fast access to the internet. The speed of this connection varies which can be different for uploading data transmission or downloading.

It uses a cable modem to provide an internet connection and operates over cable TV lines. The speed of cable connection ranges from 512k to 20Mbps.h

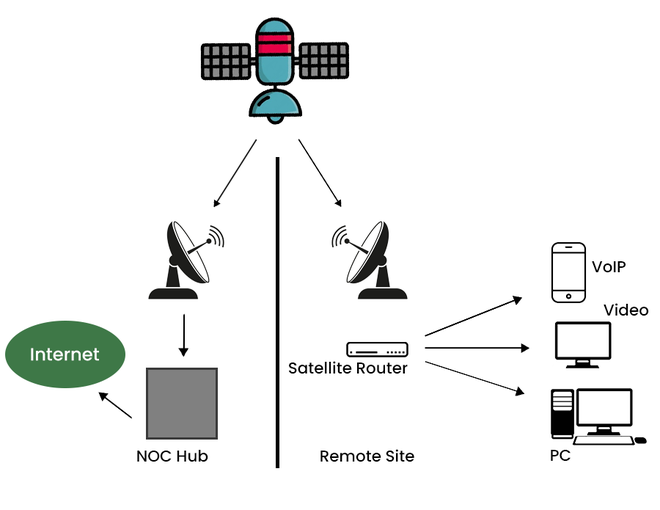


*Cable*

### Satellite Connection

This type of connection is provided mainly in rural areas where a broadband connection is not yet offered. It accesses the internet via a satellite that is in Earth’s orbit.

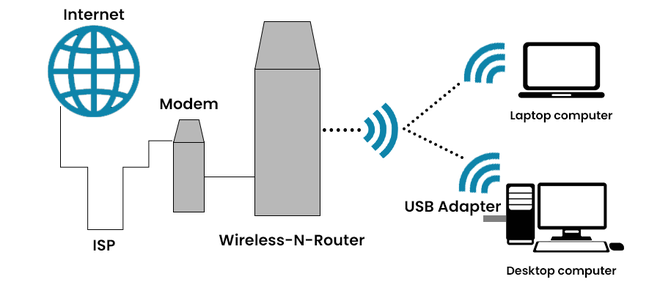
The signal travels from a long distance that is from earth to satellite and back again which provides a delayed connection. Satellite connection speeds range from 512k to 2.0Mbps.



*Satellite Connection*

### Wireless Connection

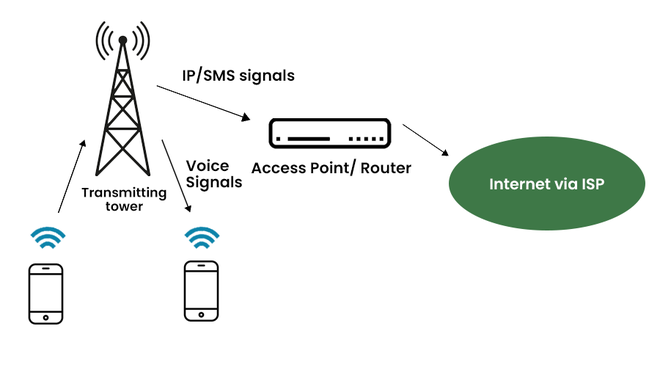
As the name suggests wireless connection does not use telephone lines or cables to connect to the internet. The wireless connection uses a radio frequency band to connect to the internet. It is also an always-on connection and this connection can be accessed from anywhere and speed may vary for different locations. It ranges from 5Mbps to 20Mbps.



*Wireless Connection*

### Cellular

[Cellular technology](https://www.geeksforgeeks.org/mobile-technologies-definition-types-uses-advantages/) provides wireless Internet access through cell phones. Speed may vary depending on the service provider. The most common are 3G and 4G which means from 3rd generation and 4th generation respectively. The speed of the 3G cellular network is around 2.0Mbps and the 4G cellular network is around 21Mbps the goal of the 4G network is to achieve peak mobile speeds of 100Mbps but the current speed of the 4G network is about 21Mbps.

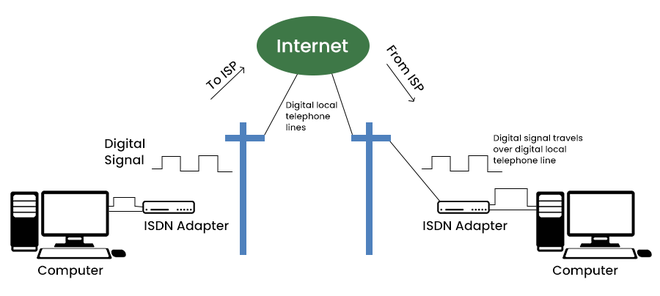


*Cellular*

### ****ISDN****

ISDN stands for [Integrated Service Digital Network](https://www.geeksforgeeks.org/integrated-services-digital-network-isdn/) and it is a circuit-switched telephone network system, but it also provides access to packet-switched networks that transmits both voice and data over a digital line. It provides a packet-switched connection for data in increments of 64 kilobit/s.

ISDN connection provides better speeds and higher quality than traditional connections. It provided a maximum of 128kbit/s bandwidth in both upstream and downstream directions.



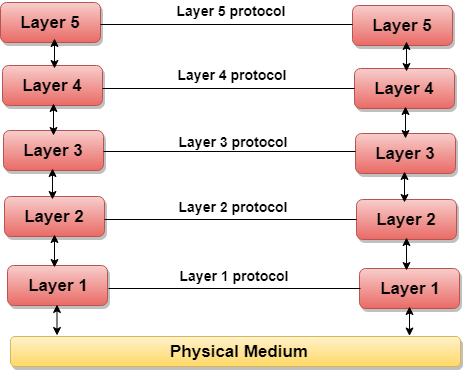
# Computer Network Models

A communication subsystem is a complex piece of Hardware and software. Early attempts for implementing the software for such subsystems were based on a single, complex, unstructured program with many interacting components. The resultant software was very difficult to test and modify. To overcome such problem, the ISO has developed a layered approach. In a layered approach, networking concept is divided into several layers, and each layer is assigned a particular task. Therefore, we can say that networking tasks depend upon the layers.

## Layered Architecture

* The main aim of the layered architecture is to divide the design into small pieces.
* Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
* It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
* It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.
* The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a higher layer and hiding the details from the layers of how the services are implemented.
* The basic elements of layered architecture are services, protocols, and interfaces.
  + **Service:** It is a set of actions that a layer provides to the higher layer.
  + **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
  + **Interface:** It is a way through which the message is transferred from one layer to another layer.
* In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.

**Let's take an example of the five-layered architecture.**



* In case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.
* Below layer 1 is the physical medium through which the actual communication takes place.
* In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
* The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.
* A set of layers and protocols is known as network architecture.

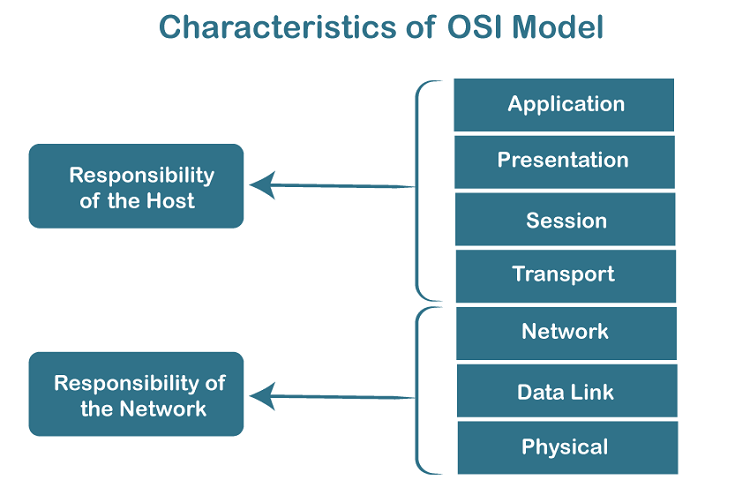
## Why do we require Layered architecture?

* **Divide-and-conquer approach:** Divide-and-conquer approach makes a design process in such a way that the unmanageable tasks are divided into small and manageable tasks. In short, we can say that this approach reduces the complexity of the design.
* **Modularity:** Layered architecture is more modular. Modularity provides the independence of layers, which is easier to understand and implement.
* **Easy to modify:** It ensures the independence of layers so that implementation in one layer can be changed without affecting other layers.
* **Easy to test:** Each layer of the layered architecture can be analyzed and tested individually.

# OSI Model

* OSI stands for **Open System Interconnection** is a reference model that describes how information from a [software](https://www.javatpoint.com/software) application in one [computer](https://www.javatpoint.com/what-is-computer) moves through a physical medium to the software application in another computer.
* OSI consists of seven layers, and each layer performs a particular network function.
* OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
* OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
* Each layer is self-contained, so that task assigned to each layer can be performed independently.

## Characteristics of OSI Model:

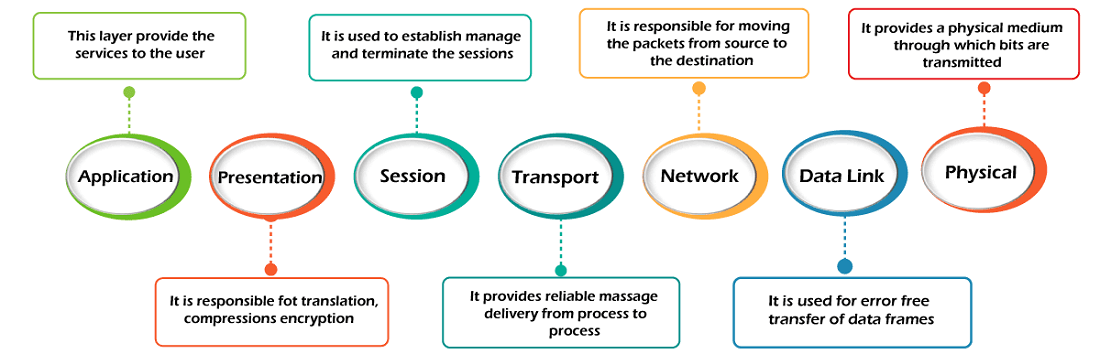


* The OSI model is divided into two layers: upper layers and lower layers.
* The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
* The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

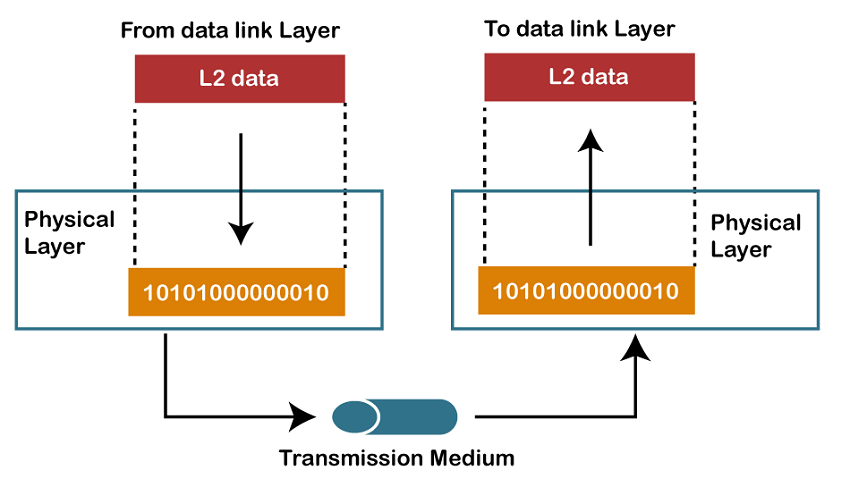
## 7 Layers of OSI Model

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



## 1) Physical layer

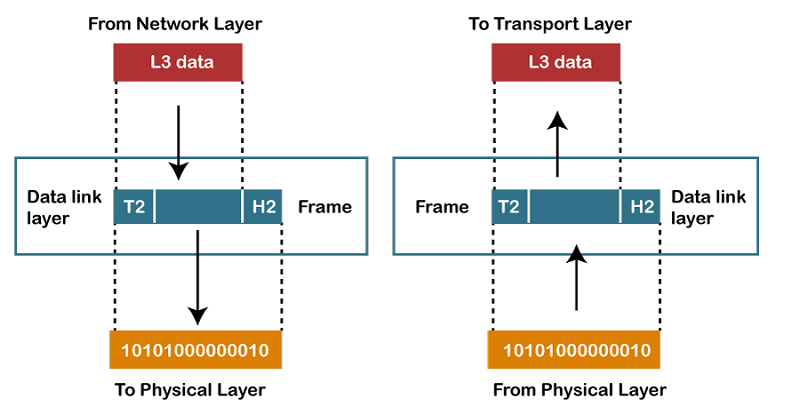


* The main functionality of the physical layer is to transmit the individual bits from one node to another node.
* It is the lowest layer of the OSI model.
* It establishes, maintains and deactivates the physical connection.
* It specifies the mechanical, electrical and procedural network interface specifications.

## Functions of a Physical layer:

* **Line Configuration:** It defines the way how two or more devices can be connected physically.
* [**Data Transmission**](https://www.javatpoint.com/computer-network-transmission-modes)**:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
* [**Topology**](https://www.javatpoint.com/computer-network-topologies)**:** It defines the way how network devices are arranged.
* **Signals:** It determines the type of the signal used for transmitting the information.

## 2) Data-Link Layer



* This layer is responsible for the error-free transfer of data frames.
* It defines the format of the data on the network.
* It provides a reliable and efficient communication between two or more devices.
* It is mainly responsible for the unique identification of each device that resides on a local network.
* It contains two sub-layers:
  + **Logical Link Control Layer**
    - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
    - It identifies the address of the network layer protocol from the header.
    - It also provides flow control.
  + **Media Access Control Layer**
    - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
    - It is used for transferring the packets over the network.

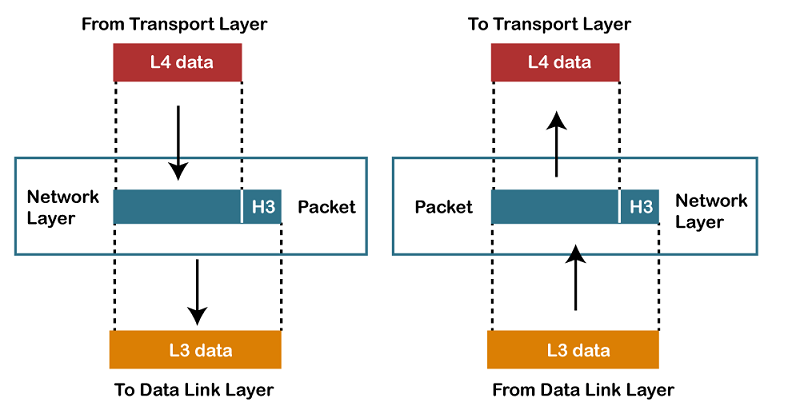
## Functions of the Data-link layer

* **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.



* **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
* **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
* **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
* **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

## 3) Network Layer

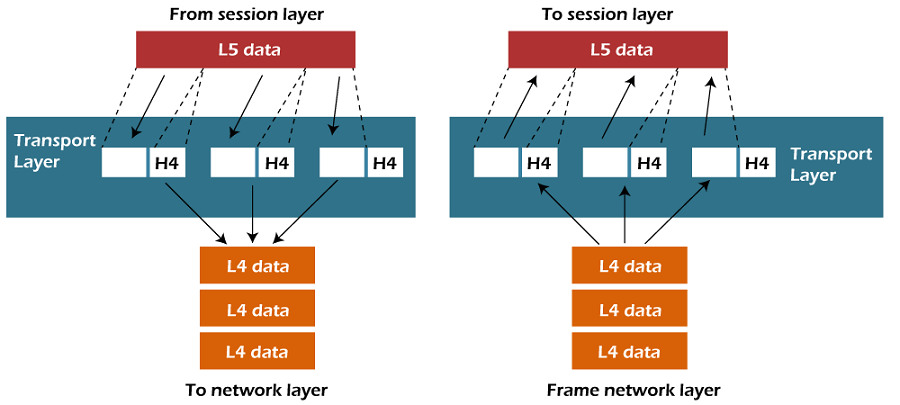


* It is a layer 3 that manages device addressing, tracks the location of devices on the network.
* It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
* The Data link layer is responsible for routing and forwarding the packets.
* Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
* The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

## Functions of Network Layer:

* **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
* [**Addressing**](https://www.javatpoint.com/network-addressing)**:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
* [**Routing**](https://www.javatpoint.com/computer-network-routing)**:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
* **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

## 4) Transport Layer



* The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
* The main responsibility of the transport layer is to transfer the data completely.
* It receives the data from the upper layer and converts them into smaller units known as segments.
* This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

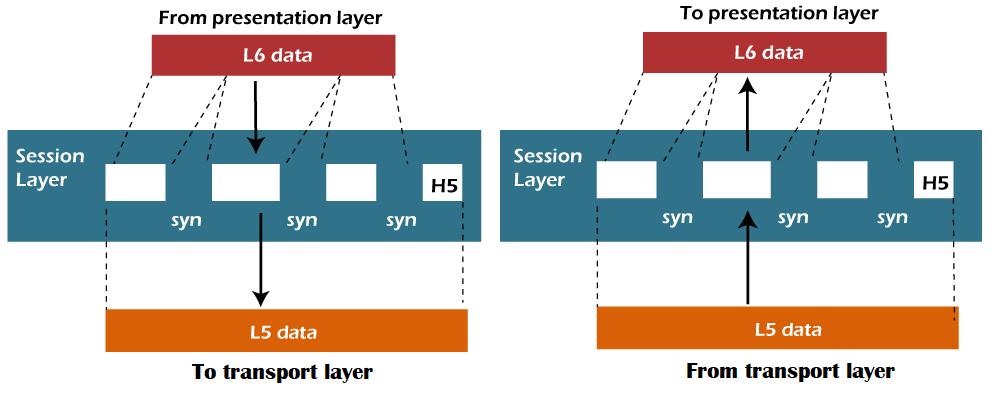
**The two protocols used in this layer are:**

* **Transmission Control Protocol**
  + It is a standard protocol that allows the systems to communicate over the internet.
  + It establishes and maintains a connection between hosts.
  + When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
* **User Datagram Protocol**
  + User Datagram Protocol is a transport layer protocol.
  + It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

## Functions of Transport Layer:

* **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
* **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
* **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
* **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
* **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

## 5) Session Layer

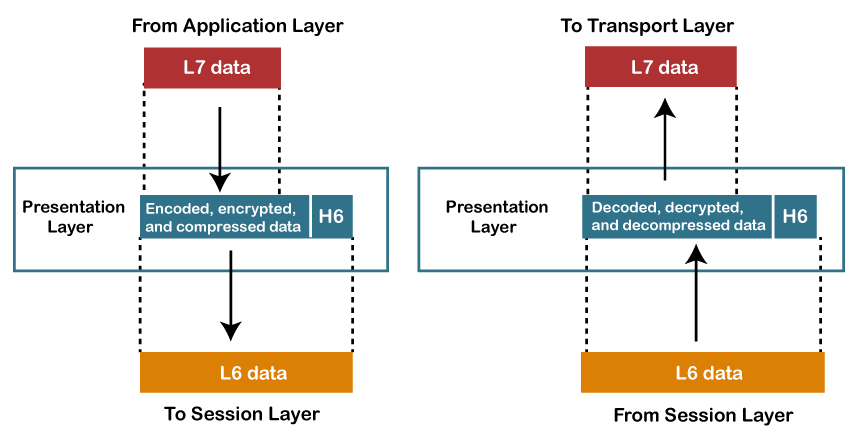


* It is a layer 3 in the OSI model.
* The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

## Functions of Session layer:

* **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
* **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

## 6) Presentation Layer

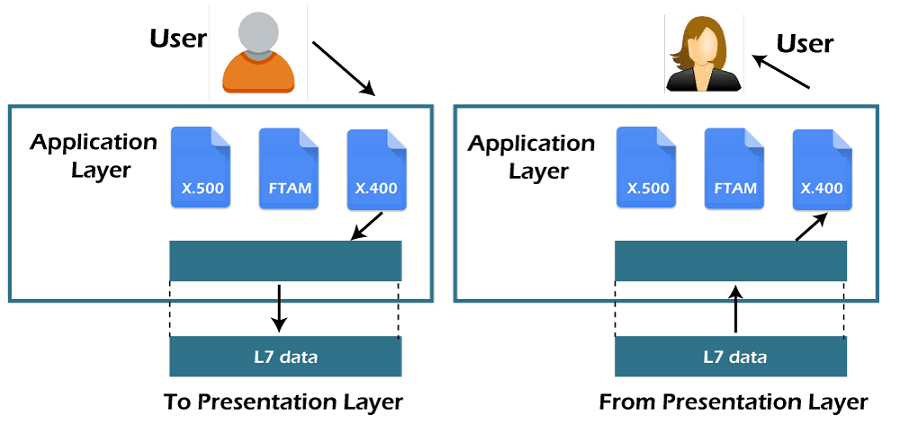


* A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
* It acts as a data translator for a network.
* This layer is a part of the operating system that converts the data from one presentation format to another format.
* The Presentation layer is also known as the syntax layer.

## Functions of Presentation layer:

* **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
* **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
* **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

## 7) Application Layer



* An application layer serves as a window for users and application processes to access network service.
* It handles issues such as network transparency, resource allocation, etc.
* An application layer is not an application, but it performs the application layer functions.
* This layer provides the network services to the end-users.

## Functions of Application layer:

* **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
* **Mail services:** An application layer provides the facility for email forwarding and storage.
* Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

# TCP/IP model

* 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**

Play Video

* 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**

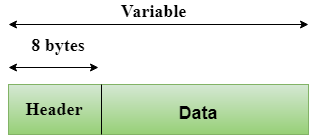
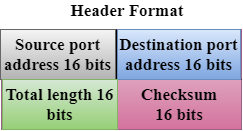
* **ICMP** stands for Internet Control Message Protocol.
* It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
* A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because 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.

* **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.