**UNIT 1   
INTRODUCTION TO COMPUTER NETWORK**

**The concept of networking:-**

* **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.

**Data communications** refers to the transmission of this digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media. The best-known computer network is the Internet.

**Computer Network Elements:** The objects basically used in a computer network are known as Computer Network Elements (CNEs). There are basically 4 computer networking elements:

1. Computers
2. Transmission medium (wired or wireless)
3. Protocols
4. Network software

All the elements of a computer network are described below:

**1. Computers:**   
A computer is a digital device that is able to accept data as input, a process that data using predefined algorithms and data structures, and perform tasks as output – that includes the transformation of raw data into information, then knowledge, and finally insight about the data’s domain. The output also takes the form of the performance of physical tasks along with data storage, data transformation, and data retrieval. The network is also formed by computers for the purposes of data interchange and leveraging a distributed programming model for parallel processing.

**2. Transmission medium:**   
The means through which we send our data from one place to another is known as the Transmission medium.   
Signals are used to represent data by computers and other telecommunication devices. The signals (i.e., data or information) are transmitted in the form of electromagnetic energy from one device to another. These signals travel through a vacuum, air, or other transmission mediums to move from one point to another (from sender to receiver).

The transmission medium is of two types:

* **(i) Wired or Guided:** For example, Twisted Pair Cable, Coaxial Cable, and Optical Fiber Cable.
* **(i) Wireless or Unguided:** For example, Radiowaves, Microwaves, and Infrared.

**3. Protocols:**   
There are some defined rules and conventions for communication between network devices.   
These are called Protocols. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into sent and received messages.

Protocols may be of 3 types:

1. Internet Protocols
2. Wireless Network Protocols
3. Network Routing Protocols

**4. Network Software:**   
Network software is a foundational element for any network. This type of software helps administrators deploy, manage and monitor a network. The traditional networks are made up of specialized hardware, such as routers and switches, that bundle the networking software into the solution.

Such types of software encompasses a broad range of software used for the design, implementation, and operation, and monitoring of computer networks. Traditional networks were hardware-based with software embedded. When software like Defined Networking (SDN) emerged, the software is separated from the hardware thus making it more adaptable to the ever-changing nature of the computer network.

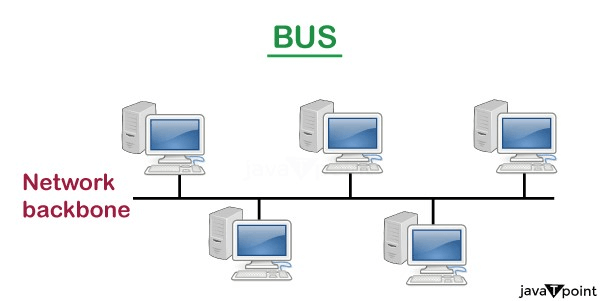
**What is Network Topology?**

Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

**Types of Network Topology**

Physical topology is the geometric representation of all the nodes in a network. There are six types of network topology which are Bus Topology, Ring Topology, Tree Topology, Star Topology, Mesh Topology, and Hybrid Topology.

**1) Bus Topology**



* The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
* Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
* When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
* The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
* The configuration of a bus topology is quite simpler as compared to other topologies.
* The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
* The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

**CSMA:** It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

* **CSMA CD:** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
* **CSMA CA:** **CSMA CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

**Advantages of Bus topology:**

* **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
* **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
* **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
* **Limited failure:** A failure in one node will not have any effect on other nodes.

**Disadvantages of Bus topology:**

* **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
* **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
* **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
* **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
* **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

**2) Ring Topology**



* Ring topology is like a bus topology, but with connected ends.
* The node that receives the message from the previous computer will retransmit to the next node.
* The data flows in one direction, i.e., it is unidirectional.
* The data flows in a single loop continuously known as an endless loop.
* It has no terminated ends, i.e., each node is connected to other node and having no termination point.
* The data in a ring topology flow in a clockwise direction.
* The most common access method of the ring topology is **token passing**.
  + **Token passing:** It is a network access method in which token is passed from one node to another node.
  + **Token:** It is a frame that circulates around the network.

**Working of Token passing**

* A token moves around the network, and it is passed from computer to computer until it reaches the destination.
* The sender modifies the token by putting the address along with the data.
* The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
* In a ring topology, a token is used as a carrier.

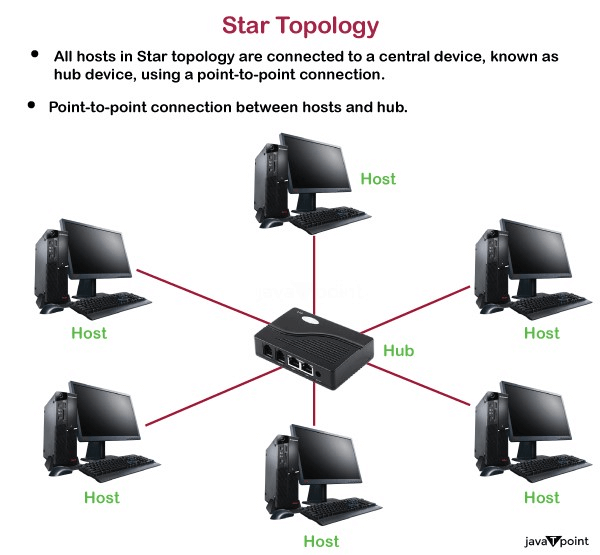
**Advantages of Ring topology:**

* **Network Management:** Faulty devices can be removed from the network without bringing the network down.
* **Product availability:** Many hardware and software tools for network operation and monitoring are available.
* **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
* **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

**Disadvantages of Ring topology:**

* **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
* **Failure:** The breakdown in one station leads to the failure of the overall network.
* **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
* **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

**3) Star Topology**



* Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
* The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
* Coaxial cable or RJ-45 cables are used to connect the computers.
* Hubs or Switches are mainly used as connection devices in a **physical star topology**.
* Star topology is the most popular topology in network implementation.

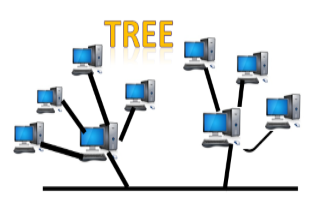
**Advantages of Star topology**

* **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
* **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
* **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
* **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
* **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
* **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
* **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

**Disadvantages of Star topology**

* **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
* **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

**4) Tree topology**



* Tree topology combines the characteristics of bus topology and star topology.
* A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
* The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
* There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

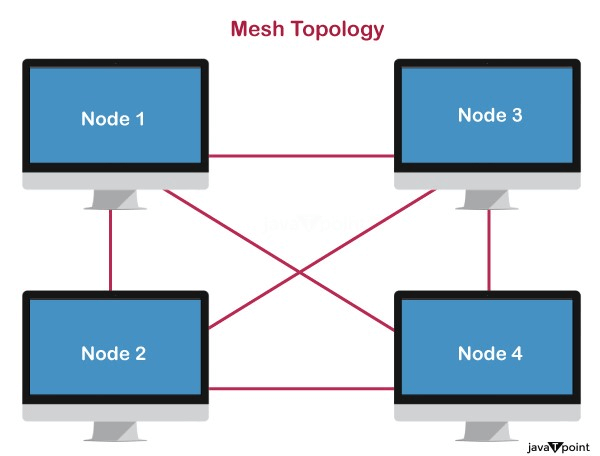
**Advantages of Tree topology**

* **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
* **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
* **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
* **Error detection:** Error detection and error correction are very easy in a tree topology.
* **Limited failure:** The breakdown in one station does not affect the entire network.
* **Point-to-point wiring:** It has point-to-point wiring for individual segments.

**Disadvantages of Tree topology**

* **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
* **High cost:** Devices required for broadband transmission are very costly.
* **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
* **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

**5) Mesh topology**

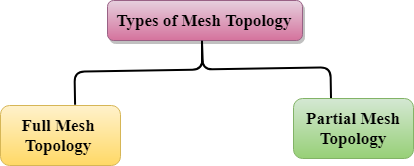


* Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
* There are multiple paths from one computer to another computer.
* It does not contain the switch, hub or any central computer which acts as a central point of communication.
* The Internet is an example of the mesh topology.
* Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
* Mesh topology is mainly used for wireless networks.
* Mesh topology can be formed by using the formula:  
  **Number of cables = (n\*(n-1))/2;**

Where n is the number of nodes that represents the network.

**Mesh topology is divided into two categories:**

* Fully connected mesh topology
* Partially connected mesh topology



* **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
* **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

**Advantages of Mesh topology:**

**Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

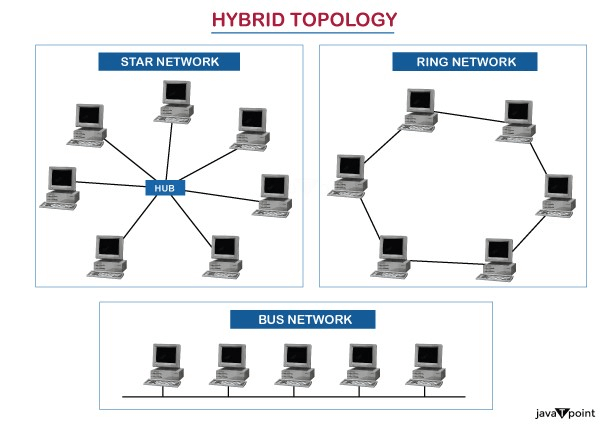
**Fast Communication:** Communication is very fast between the nodes.

**Easier Reconfiguration:** Adding new devices would not disrupt the communication between other devices.

**Disadvantages of Mesh topology**

* **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
* **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
* **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

6) Hybrid Topology



* The combination of various different topologies is known as **Hybrid topology**.
* A Hybrid topology is a connection between different links and nodes to transfer the data.
* When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

**Advantages of Hybrid Topology**

* **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
* **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
* **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
* **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

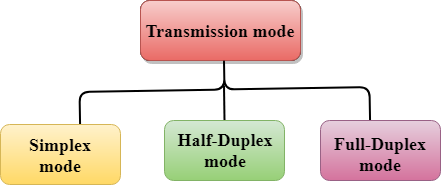
**Disadvantages of Hybrid topology**

* **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
* **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
* **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

**Transmission modes**

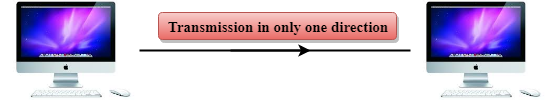
* The way in which data is transmitted from one device to another device is known as **transmission mode**.
* The transmission mode is also known as the communication mode.
* Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode.
* The transmission mode is defined in the physical layer.

The Transmission mode is divided into three categories:



* Simplex mode
* Half-duplex mode
* Full-duplex mode

**Simplex mode**



* In Simplex mode, the communication is unidirectional, i.e., the data flow in one direction.
* A device can only send the data but cannot receive it or it can receive the data but cannot send the data.
* This transmission mode is not very popular as mainly communications require the two-way exchange of data. The simplex mode is used in the business field as in sales that do not require any corresponding reply.
* The radio station is a simplex channel as it transmits the signal to the listeners but never allows them to transmit back.
* Keyboard and Monitor are the examples of the simplex mode as a keyboard can only accept the data from the user and monitor can only be used to display the data on the screen.
* The main advantage of the simplex mode is that the full capacity of the communication channel can be utilized during transmission.

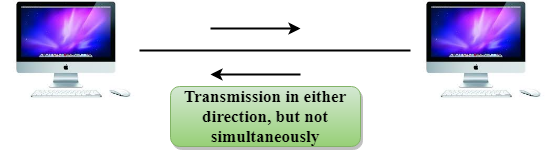
**Advantage of Simplex mode:**

* In simplex mode, the station can utilize the entire bandwidth of the communication channel, so that more data can be transmitted at a time.

**Disadvantage of Simplex mode:**

* Communication is unidirectional, so it has no inter-communication between devices.

Half-Duplex mode



* In a Half-duplex channel, direction can be reversed, i.e., the station can transmit and receive the data as well.
* Messages flow in both the directions, but not at the same time.
* The entire bandwidth of the communication channel is utilized in one direction at a time.
* In half-duplex mode, it is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data.
* A **Walkie-talkie** is an example of the Half-duplex mode. In Walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens. Speaking simultaneously will create the distorted sound which cannot be understood.

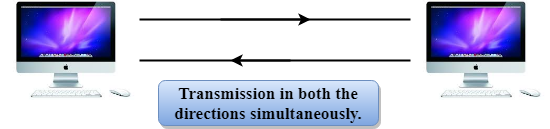
**Advantage of Half-duplex mode:**

* In half-duplex mode, both the devices can send and receive the data and also can utilize the entire bandwidth of the communication channel during the transmission of data.

**Disadvantage of Half-Duplex mode:**

* In half-duplex mode, when one device is sending the data, then another has to wait, this causes the delay in sending the data at the right time.

**Full-duplex mode**



* In Full duplex mode, the communication is bi-directional, i.e., the data flow in both the directions.
* Both the stations can send and receive the message simultaneously.
* Full-duplex mode has two simplex channels. One channel has traffic moving in one direction, and another channel has traffic flowing in the opposite direction.
* The Full-duplex mode is the fastest mode of communication between devices.
* The most common example of the full-duplex mode is a telephone network. When two people are communicating with each other by a telephone line, both can talk and listen at the same time.

**Advantage of Full-duplex mode:**

* Both the stations can send and receive the data at the same time.

**Disadvantage of Full-duplex mode:**

* If there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts.

**Differences b/w Simplex, Half-duplex and Full-duplex mode**

|  |  |  |  |
| --- | --- | --- | --- |
| **Basis for comparison** | **Simplex mode** | **Half-duplex mode** | **Full-duplex mode** |
| Direction of communication | In simplex mode, the communication is unidirectional. | In half-duplex mode, the communication is bidirectional, but one at a time. | In full-duplex mode, the communication is bidirectional. |
| Send/Receive | A device can only send the data but cannot receive it or it can only receive the data but cannot send it. | Both the devices can send and receive the data, but one at a time. | Both the devices can send and receive the data simultaneously. |
| Performance | The performance of half-duplex mode is better than the simplex mode. | The performance of full-duplex mode is better than the half-duplex mode. | The Full-duplex mode has better performance among simplex and half-duplex mode as it doubles the utilization of the capacity of the communication channel. |
| Example | Examples of Simplex mode are radio, keyboard, and monitor. | Example of half-duplex is Walkie-Talkies. | Example of the Full-duplex mode is a telephone network. |

**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.

**Benefits of Computer Network**

* Computer Networks have been put in place after a lot of decision-making and analysis, and it is expected to be the future of our evolution. That's why it is essential to know its advantages. The list of benefits of computer networks are:

**1. Enhancement of Communication and Information Availability:**

* By offering faster and more advanced methods to connect individuals, computer networks have revolutionized communication. Messaging, video calls, and file sharing have facilitated global user connectivity.
* Businesses with widespread offices and franchises can communicate and share information easily using networking techniques. Businesses and service industries alike have benefited from the ability to collaborate and receive fast feedback.
* Facebook is a prime example of a business that has boomed because of information availability and communication.

**2. Convenient Sharing of Resources:**

* Vast amounts of data production by large organizations can be a useful resource for current and future endeavours. Within these organizations, computer networks share resources, enabling effective data interchange and collaboration. This functionality is crucial for optimizing daily operations and ensuring that resources are available in several industries, including education, transportation, and hospitality.

**3. Easy File/Data Sharing:**

* The sharing of files and data sets is the most vital feature of a computer network. The computer present during the initial stages didn't even have this file-sharing feature. Now, with constant advancements, this feature has not only been present in the computer network but has also become much easier. Many industries and organizations are using computer networks for their operations, and computer networks have made information sharing easier because such organizations run on their data. It is very important to get such data to be transferred efficiently. Computer networks also save a lot of time, and it has been proven monetarily beneficial in the long run.

**4. Highly Flexible:**

* To accommodate consumers' changing requirements, modern technology must be adaptive and flexible. In this sense, computer networks shine, providing a variety of capabilities to accommodate users' desires for mobile and distant access. Because of their adaptability, computer networks have become a crucial part of our daily lives, boosting connectedness and ease.

**5. Affordable:**

* The computer network was rare among people twenty years ago because it was mainly used for commercial purposes and was expensive to install. With time and the rapid modernization of everything worldwide, networking devices became common among folks, and their cost decreased.
* The software now available in the computer world can be easily accessed and last very long on devices. The software and networking devices are available at very affordable rates and provide easy ways to transfer information across the network.
* **6. Increases Cost Efficiency:**
* Networking technology is constantly improving, which has prompted the creation of affordable software and apps. On the Internet, there are a lot of free or inexpensive software options that offer variety and long-term advantages. These techniques increase production, cut costs, and improve overall cost-effectiveness. VLC Media Player, Discord, WinRAR, and torrent clients are examples.
* **7. Networking Boosts Storage Capacity:**
* Users can access cloud storage options through computer networks, which maximize storage space at affordable prices. Cloud storage is crucial for effective data management in big businesses, where much data is produced daily. Users can access and upload the files they need online without using any local device storage. Google Drive, iCloud, and Dropbox are some well-known cloud storage providers.
* **8. Enhanced Security and Data Protection:**
* Advanced security mechanisms are available on computer networks to safeguard sensitive data. To protect their data from unauthorized access and online dangers, organizations might put in place firewalls, encryption mechanisms, and access controls. Additionally, data resilience may be ensured, and the threat of data loss due to hardware failures or disasters can be reduced by seamlessly integrating data backup and recovery solutions into network systems.
* Advertisement
* **9. Centralized Management and Control:**
* Centralized management and control of resources, devices, and security regulations are made possible via computer networks. Setting up configurations, implementing security patches, and troubleshooting problems are all made simpler by the ability of network administrators to monitor and administer the entire network from a single location.
* This centralized control makes network upkeep easier and less burdensome, which boosts the dependability and efficiency of the network. Additionally, it makes it possible to adopt uniform security procedures and standards across the whole network, improving both network and data security in general.
* **10. Scalability:**
* Businesses can quickly expand their infrastructure using computer networks to accommodate more users, devices, and data without experiencing significant disruptions. This adaptability permits effective expansion and upholds a solid network structure.

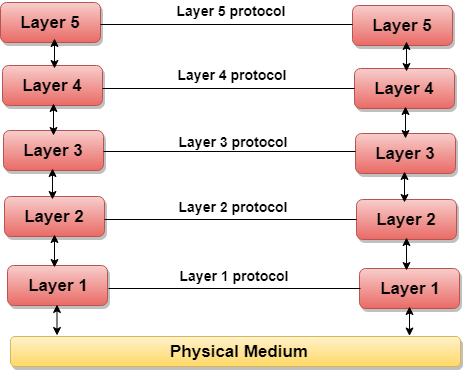
**Computer Network Models**

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.

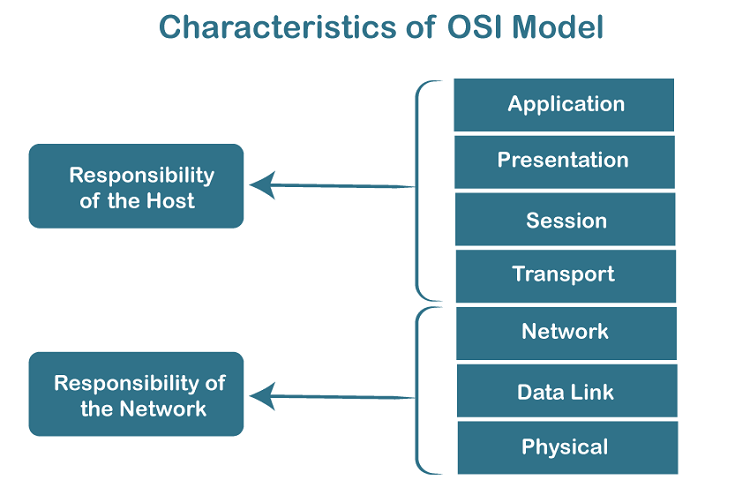
**Why do we require Layered architecture?**

* **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:**

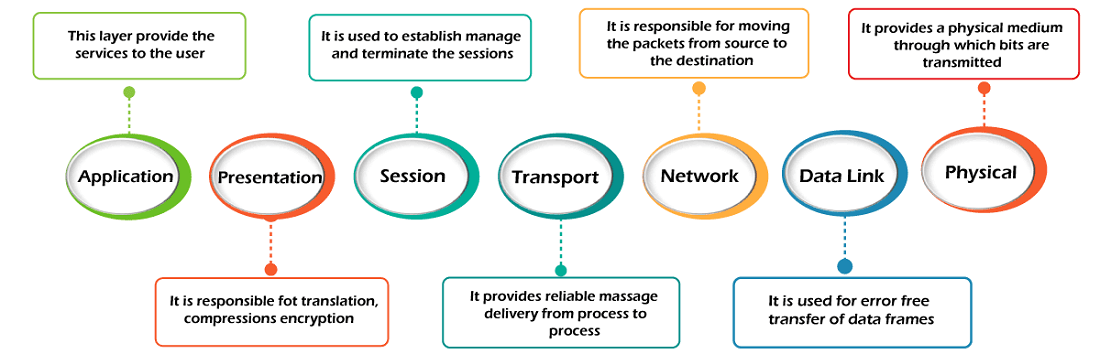


* The OSI model is divided into two layers: upper layers and lower layers.
* The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer 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.

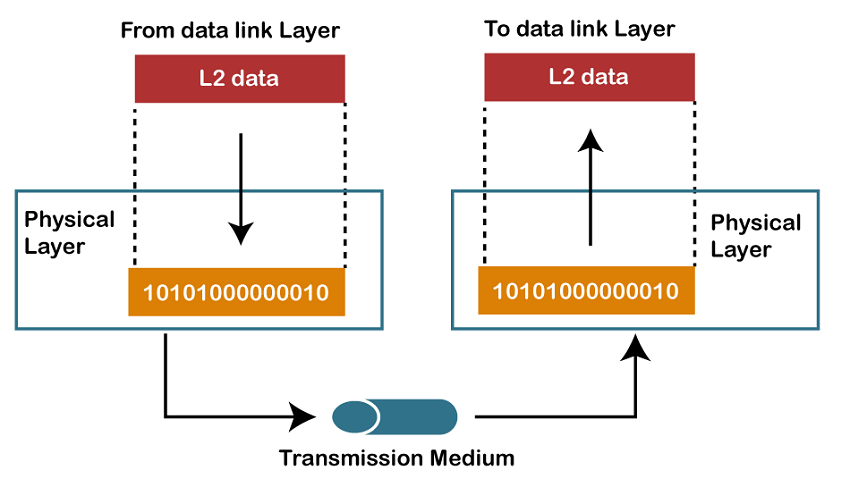
**7 Layers of OSI Model**

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

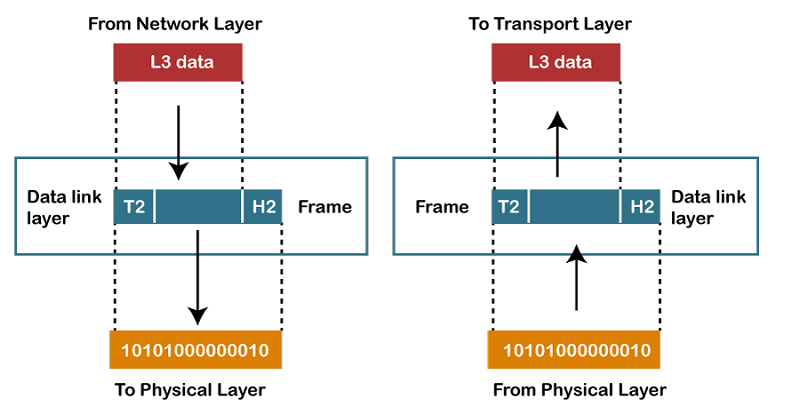


* The main functionality of the physical layer is to transmit the individual bits from one node to another node.
* It is the lowest layer of the OSI model.
* It establishes, maintains and deactivates the physical connection.
* It specifies the mechanical, electrical and procedural network interface specifications.

**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.

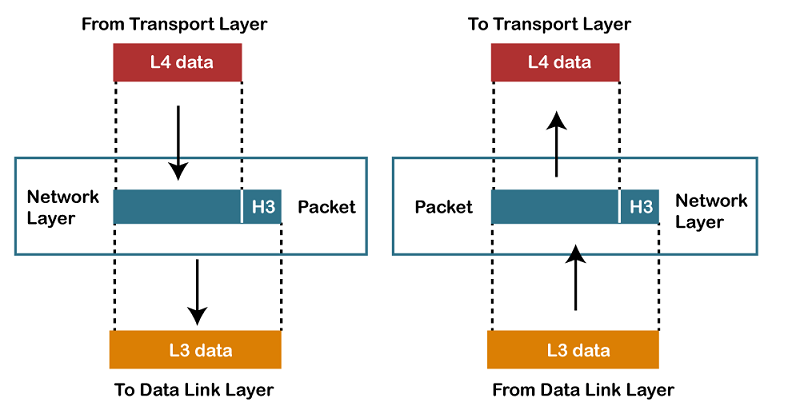
**Functions of the Data-link layer**

* **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**

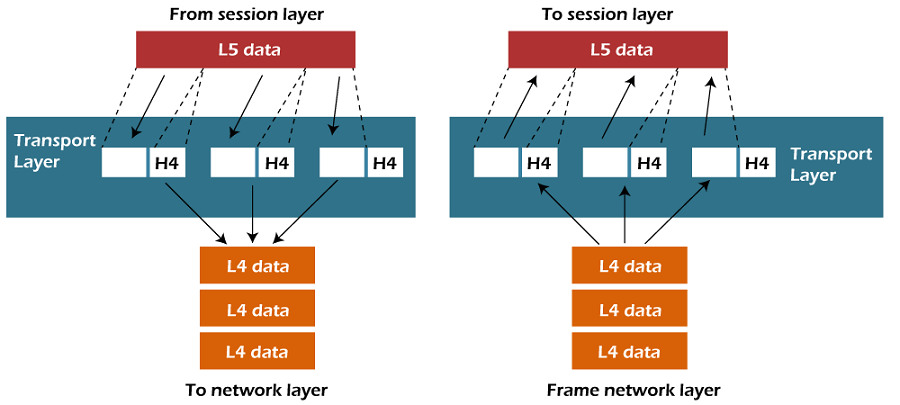


* It is a layer 3 that manages device addressing, tracks the location of devices on the network.
* It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
* The Data link layer is responsible for routing and 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.

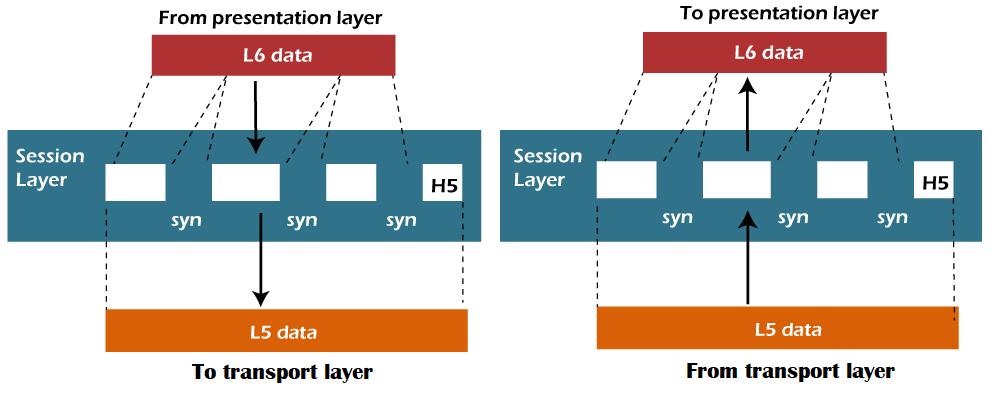
**The two protocols used in this layer are:**

* **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**

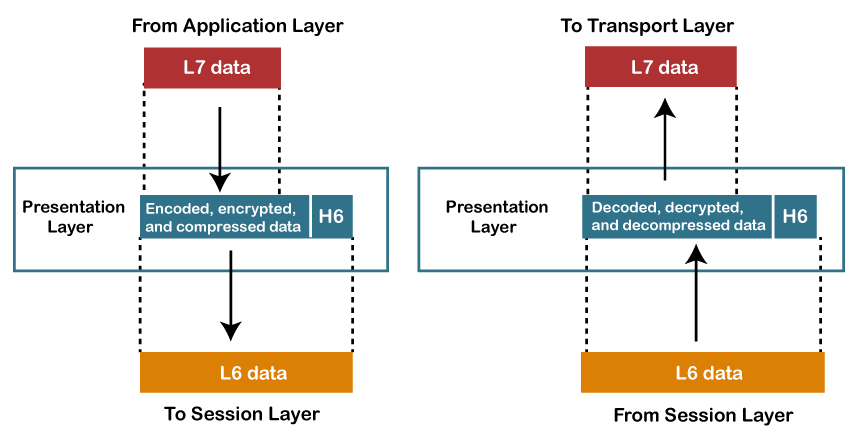


* It is a layer 3 in the OSI model.
* The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

**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**

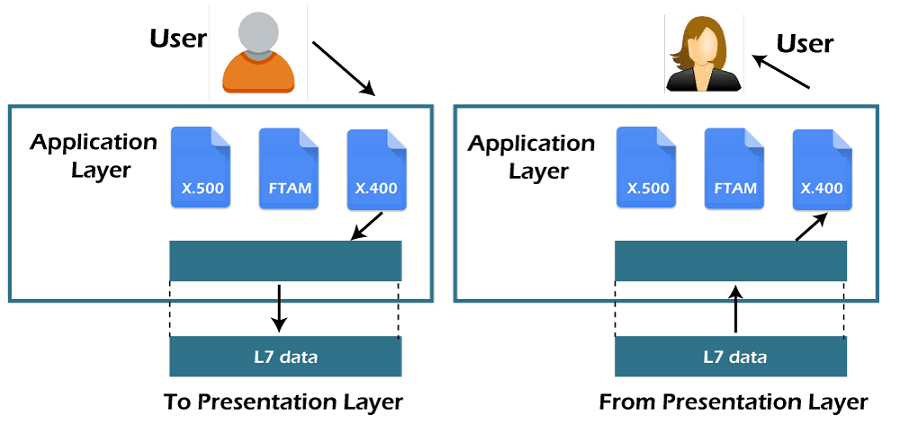


* A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
* It acts as a data translator for a network.
* This layer is a part of the operating system that converts the data from one presentation format to another format.
* The Presentation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



*TCP/IP* is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent. Whereas the OSI model specifies which functions belong to each of its layers, the layers of the *TCP/IP* protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system. The term *hierarchical*

means that each upper-level protocol is supported by one or more lower-level protocols.

At the transport layer, *TCP/IP* defines three protocols: Transmission Control

Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols that support data movement in this layer.

**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 / Network 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**

Advertisement

* 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**

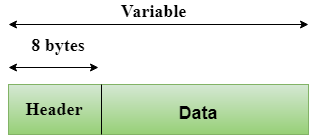
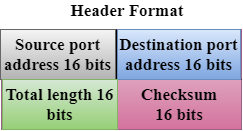
* **ICMP** stands for Internet Control Message Protocol.
* It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
* A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because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

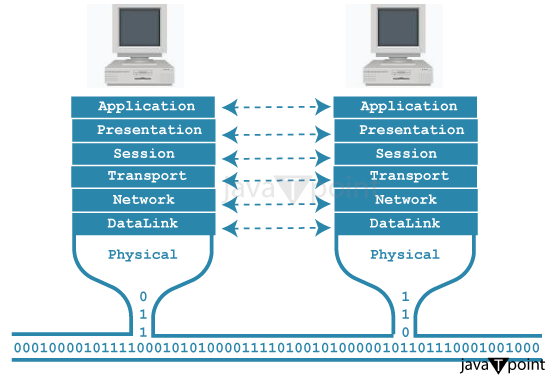
  


* **Transmission Control Protocol (TCP)**
  + It provides a full transport layer services to applications.
  + It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
  + TCP is a reliable protocol as it detects the error and retransmits the 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.
* Design Issues for the Layers of Computer Networks
* Introduction
* Computer networks are the lifelines of our digital era, supporting the flow of information, data, and communication across a wide range of devices and in an increasingly linked world. However, the complicated web of interconnected networks that enables our daily interactions and global connectedness is anything from simple. To ensure the seamless operation and scalability of computer networks, one must delve into the intricacies of design issues that span the layers of these intricate systems.
* 
* The design issues in computer network layers are not mere technical details; they are the foundation upon which the reliability, security, and efficiency of our digital interactions are built. In this comprehensive exploration, we will dissect the critical challenges that network architects and engineers must address to craft networks that function smoothly and adapt to the ever-evolving landscape of technology. In this read, we will look into the problems that might occur while designing the network.
* 1. Reliability
* Reliability is a cornerstone design issue in computer networks. Networks are composed of various components, and some of these components may be inherently unreliable, leading to potential data loss during transmission. Ensuring that data is transferred without distortion or corruption is paramount. ***Robust error detection and correction mechanisms*** are essential for preserving data integrity, especially in the face of unreliable communication channels.
* 2. Addressing
* Addressing is a fundamental aspect of network layers. In a network, numerous processes run on multiple machines, and each layer requires a mechanism to identify both senders and receivers accurately. Effectively assigning and managing addresses helps facilitate efficient communication, ensuring that data reaches its intended destination.
* 3. Error Control
* The inherent imperfections in physical communication circuits necessitate error control as a vital design issue. To safeguard data integrity, error-detecting and error-correcting codes are employed. However, it's imperative that both the sending and receiving ends reach a consensus on the specific error detection and correction codes to be used, ensuring effective data packet protection.
* 4. Flow Control
* Maintaining an equilibrium between data senders and receivers is essential to prevent data loss due to speed mismatches. A fast sender transmitting data to a slower receiver necessitates the implementation of a flow control mechanism. Several approaches are used, such as **increasing buffer sizes at receivers or slowing down the fast sender.** Additionally, the network should handle processes that cannot accommodate arbitrarily long messages by disassembling, transmitting, and reassembling messages as required.
* 5. Multiplexing and De-multiplexing
* Efficient data transmission on a network often involves transmitting data separately on the transmission medium. Setting up separate connections for every pair of communicating processes is neither practical nor cost-effective. To address this challenge, multiplexing is employed at the sender's end, allowing data from multiple sources to be combined into a single transmission stream. De-multiplexing is then performed at the receiver's end to separate and direct the data to the appropriate recipients.
* 6. Scalability
* As networks expand in size and complexity, new challenges inevitably arise. Scalability is crucial to ensuring that networks can continue to function effectively as they grow. The network's design should accommodate increasing sizes, reducing the risk of congestion and compatibility issues when new technologies are introduced. Scalability is a cornerstone for ensuring the network's long-term viability.
* 7. Routing
* Routing is a critical function within the network layer. When multiple paths exist between a source and destination, the network must select the most optimal route for data transmission. Various routing algorithms are utilized to make this determination, with the aim of minimizing cost and time, thereby ensuring efficient and reliable data transfer.
* 8. Confidentiality and Integrity
* The security of a network is critical. Confidentiality methods are critical for protecting against risks like eavesdropping and preventing unauthorized parties from accessing sensitive data. Data integrity is also crucial since it protects against tampering and unauthorized changes to messages during transmission.
* Advertisement
* 9. Service Quality (QoS):
* QoS refers to a network's ability to deliver varying levels of service to different types of traffic. Video streaming, VoIP, and data transmission all have varying bandwidth, latency, and reliability needs. It is a difficult challenge to ensure that the network can prioritize and distribute resources effectively to satisfy these objectives.
* 10. Network management:
* Network management includes monitoring and maintaining the health and performance of different network components such as routers, switches, and servers. Device configuration, fault detection, performance analysis, and security monitoring all need network management tools and protocols. Effective network administration is critical for detecting and resolving problems in real time, optimizing resource utilization, and maintaining a positive user experience.
* 11. Load Balancing:
* In scenarios where a network has multiple servers or paths to handle incoming traffic, load balancing becomes critical. The challenge is to distribute network traffic evenly across these resources to prevent overloads and optimize resource utilization. Load balancing can be achieved through hardware or software solutions, and it may require advanced algorithms to make intelligent decisions based on factors like server health and current traffic loads.
* 12. Network Topology Design:
* The choice of network topology can significantly impact the network's performance, scalability, and fault tolerance. Designing the right topology for a given scenario involves considering factors such as cost, reliability, ease of expansion, and fault tolerance. For example, a star topology might be suitable for a small office network, while a mesh or hybrid topology could be preferred for a large-scale data center.
* 13. Energy Efficiency:
* With increasing concerns about energy consumption and its environmental impact, designing energy-efficient networks is essential. This includes using energy-efficient hardware, optimizing network protocols, and implementing strategies for turning off or reducing power to unused network components during periods of low demand. Energy-efficient network design helps reduce operational costs and minimizes the carbon footprint.
* 14. Interoperability:
* It is a huge task to ensure that these components can function together seamlessly. Adherence to industry standards and protocols, as well as testing and certification processes, are used to achieve interoperability. It's crucial to ensure that data can flow smoothly between diverse network elements.
* 15. Virtualization and Network Function Virtualization (NFV):
* Network virtualization involves creating virtual instances of network components and services, such as virtual routers and firewalls. Managing these virtual networks, ensuring their security, and dynamically scaling resources to meet changing demands is a complex task. Network Function Virtualization (NFV) extends this concept by virtualizing network functions like firewalls and load balancers, enabling flexible and cost-effective service delivery.
* 16. Mobile and Wireless Networks:
* As the use of mobile devices and wireless connections continues to grow, designing networks that provide seamless connectivity as users move between different access points is a challenge. This involves implementing mobility management protocols, handover procedures, and efficient spectrum management to prevent interference and optimize wireless performance.
* 17. Legacy Systems Integration:
* Many existing networks include legacy systems and technologies that must be integrated with modern networking solutions. This can be complex because older systems may not support the latest standards and security protocols. Network designers must ensure compatibility while maintaining security during the integration process.
* 18. Disaster Recovery and Redundancy:
* Planning for network resilience in the face of disasters, equipment failures, or cyberattacks is critical. Redundancy, failover mechanisms, and disaster recovery strategies must be in place to maintain network continuity. This involves duplicating critical components, creating backup data centers, and implementing data backup and recovery solutions.
* 19. IoT and Edge Computing:
* With the proliferation of Internet of Things (IoT) devices and the adoption of edge computing, networks must handle a massive number of connected devices and process data at the edge of the network. This presents challenges related to device management, data processing, and ensuring security and privacy for IoT devices.
* 20. Compliance and Regulatory Issues:
* Networks often need to comply with specific regulations and industry-specific standards, such as data privacy laws (e.g., GDPR) or compliance requirements for industries like healthcare or finance. Meeting these requirements involves implementing security measures, data encryption, and auditing processes to ensure network compliance while avoiding legal and financial penalties.
* These problems reflect the evolving nature of computer networks and the diverse demands placed on them in a constantly changing technological landscape. Network designers must consider these challenges to create robust, efficient, and secure network architectures.

**OSI model defines the services, protocols, and interfaces as well as provides a proper distinction between them. It is protocol independent. In the TCP/IP model, services, protocols, and interfaces are not properly separated. It is protocol dependent.**

**Interfaces and Services** is a process that generally provides and gives a common technique for each layer to communicate with each other. Standard terminology basically required for layered networks to request and aim for the services are provided. Service is defined as a set of primitive operations. Services are provided by layer to each of layers above it. Below is diagram showing relation between layers at an interface.

**Let's see the differences between the OSI and TCP/IP model in a tabular form:**

|  |  |
| --- | --- |
| **OSI Model** | **TCP/IP Model** |
| It stands for **Open System Interconnection.** | It stands for **Transmission Control Protocol.** |
| OSI model has been developed by ISO (International Standard Organization). | It was developed by ARPANET (Advanced Research Project Agency Network). |
| It is an independent standard and generic protocol used as a communication gateway between the network and the end user. | It consists of standard protocols that lead to the development of an internet. It is a communication protocol that provides the connection among the hosts. |
| In the OSI model, the transport layer provides a guarantee for the delivery of the packets. | The transport layer does not provide the surety for the delivery of packets. But still, we can say that it is a reliable model. |
| This model is based on a vertical approach. | This model is based on a horizontal approach. |
| In this model, the session and presentation layers are separated, i.e., both the layers are different. | In this model, the session and presentation layer are not different layers. Both layers are included in the application layer. |
| It is also known as a reference model through which various networks are built. For example, the TCP/IP model is built from the OSI model. It is also referred to as a guidance tool. | It is an implemented model of an OSI model. |
| In this model, the network layer provides both connection-oriented and connectionless service. | The network layer provides only connectionless service. |
| Protocols in the OSI model are hidden and can be easily replaced when the technology changes. | In this model, the protocol cannot be easily replaced. |
| It consists of 7 layers. | It consists of 4 layers. |
| OSI model defines the services, protocols, and interfaces as well as provides a proper distinction between them. It is protocol independent. | In the TCP/IP model, services, protocols, and interfaces are not properly separated. It is protocol dependent. |
| The usage of this model is very low. | This model is highly used. |
| It provides standardization to the devices like router, motherboard, switches, and other hardware devices. | It does not provide the standardization to the devices. It provides a connection between various computers. |

**Line Configuration in Computer Networks**

A network is two or more devices connected through a link. A link is a communication pathway that transfers data from one device to another. Devices can be a computer, printer, or any other device that is capable to send and receive data. For visualization purposes, imagine any link as a line drawn between two points.

For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections:

1. **Point-to-Point Connection**
2. **Multipoint Connection**

**Point-to-Point:**

* Uses a dedicated link to connect two devices
* Simple and easy to set up
* Limited to two devices only
* Does not require a network interface card (NIC) or a hub/switch
* Can become complex and difficult to manage as the network grows

**Multipoint:**

* Uses a single link to connect three or more devices
* More complex than point-to-point configuration
* Can be more efficient and cost-effective for larger networks
* Devices share the same link, which can lead to collisions and lower performance
* Commonly used in LANs and MANs