**UNIT – 1 : Introduction**

**Overview of Networks, Circuit switching to packet switching principles, Protocols, protocol architecture, Reference Models, TCP/IP Model. Design Issues for the layers.**

**What is a Computer Network?**

A computer network is a system that connects many independent computers to share information (data) and resources. The integration of computers and other different devices allows users to communicate more easily. A computer network is a collection of two or more computer systems that are linked together. A network connection can be established using either  [cable](https://www.geeksforgeeks.org/what-is-coaxial-cable/) or [wireless media.](https://www.geeksforgeeks.org/wired-and-wireless-networking/) Hardware and software are used to connect computers and tools in any network.

**What Do Computer Networks Do?**

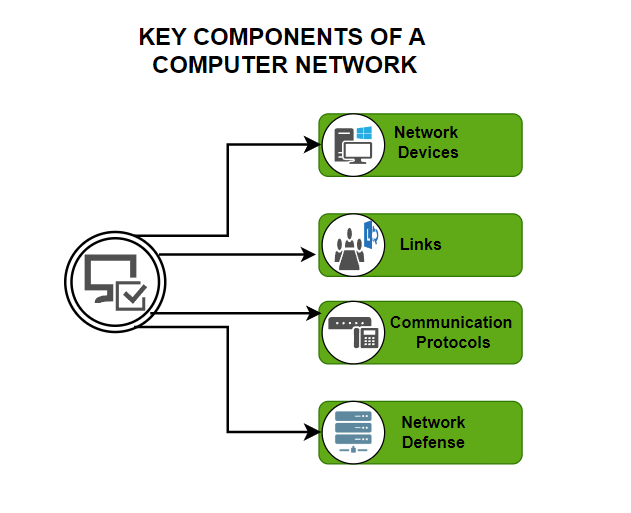
Computer Networks are one of the important aspects of Computer Science. In the early days, it is used for data transmission on[telephone lines](https://www.geeksforgeeks.org/introduction-to-telephone-network/) and had a very limited use, but nowadays, it is used in a variety of places.

Computer Networks help in providing better connectivity that helps nowadays. Modern computer networks have the following functionality:

* Computer Networks help in operating virtually
* Computer Networks integrate on a large scale
* Computer Networks respond very quickly in case of conditions change
* Computer Networks help in providing data security

**Key Components of a Computer Network**

In simple terms, a computer network is made up of **two main parts**: devices (called nodes) and connections (called links). The links connect the devices to each other. The rules for how these connections send information are called communication protocols. The starting and ending points of these communications are often called ports**.**



**Key Components of Computer Network**

**1.Network Devices**

Basic hardware interconnecting network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers, are used in all networks. In addition, a mechanism for connecting these building parts is necessary, which is usually galvanic cable and optical cable are less popular (“optical fiber”)The following are the network devices :

**NIC (Network Interface Card):**A network card, often known as a network adapter or [NIC](https://www.geeksforgeeks.org/nic-full-form) (network interface card), is computer hardware that enables computers to communicate via a network. It offers physical access to networking media and, in many cases, MAC addresses serve as a low-level addressing scheme. Each network interface card has a distinct identifier. This is stored on a chip that is attached to the card.

**Repeater:**A [repeater](https://www.geeksforgeeks.org/repeaters-in-computer-network/) is an electrical device that receives a signal, cleans it of unwanted noise, regenerates it, and retransmits it at a higher power level or to the opposite side of an obstruction, allowing the signal to travel greater distances without degradation. In the majority of twisted pair Ethernet networks, Repeaters are necessary for cable lengths longer than 100 meters in some systems. Repeaters are based on physics.

**Hub:**A [hub](https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways) is a device that joins together many twisted pairs or fiber optic Ethernet devices to give the illusion of a formation of a single network segment. The device can be visualized as a multiport repeater. A network hub is a relatively simple broadcast device. Any packet entering any port is regenerated and [broadcast](https://www.geeksforgeeks.org/what-is-broadcast-domain/) out on all other ports, and hubs do not control any of the traffic that passes through them. Packet collisions occur as a result of every packet being sent out through all other ports, substantially impeding the smooth flow of communication.

**Bridges:**[Bridges](https://www.geeksforgeeks.org/bridges-local-internetworking-device/) broadcast data to all the ports but not to the one that received the transmission. Bridges, on the other hand, learn which MAC addresses are reachable through specific ports rather than copying messages to all ports as hubs do. Once a port and an address are associated, the bridge will only transport traffic from that address to that port.

**Switches:**A switch differs from a hub in that it only forwards frames to the ports that are participating in the communication, rather than all of the ports that are connected. The collision domain is broken by a switch, yet the switch depicts itself as a broadcast domain. Frame-forwarding decisions are made by switches based on MAC addresses.

**Routers:**Routers are networking devices that use headers and forwarding tables to find the optimal way to forward data packets between networks. A router is a computer networking device that links two or more computer networks and selectively exchanges data packets between them. A router can use address information in each data packet to determine if the source and destination are on the same network or if the data packet has to be transported between networks. When numerous routers are deployed in a wide collection of interconnected networks, the routers share target system addresses so that each router can develop a table displaying the preferred pathways between any two systems on the associated networks.

**Gateways:**To provide system compatibility, a [gateway](https://www.geeksforgeeks.org/what-is-the-difference-between-an-api-and-an-api-gateway/) may contain devices such as protocol translators, impedance-matching devices, rate converters, fault isolators, or signal translators. It also necessitates the development of administrative procedures that are acceptable to both networks. By completing the necessary protocol conversions, a protocol translation/mapping gateway joins networks that use distinct network protocol technologies.

**2.Links**

Links are the ways information travels between devices, and they can be of two types:

**Wired:**Communication done in a wired medium**.** Copper wire, twisted pair, or fiber optic cables are all options. A wired network employs wires to link devices to the Internet or another network, such as laptops or desktop PCs.

**Wireless:**Wireless means without wire, media that is made up of electromagnetic waves (EM Waves) or infrared waves. Antennas or sensors will be present on all wireless devices. For data or voice communication, a wireless network uses radio frequency waves rather than wires.

**3.Communication Protocols**

A communication protocol is a set of rules that all devices follow when they share information. Some common protocols are TCP/IP, IEEE 802, Ethernet, wireless LAN, and cellular standards. TCP/IP is a model that organizes how communication works in modern networks. It has four functional layers for these communication links:

**Network Access Layer**: This layer controls how data is physically transferred, including how hardware sends data through wires or fibers.

**Internet Layer**: This layer packages data into understandable packets and ensures it can be sent and received.

**Transport Layer**: This layer keeps the communication between devices steady and reliable.

**Application Layer**: This layer allows high-level applications to access the network to start data transfer.

Most of the modern internet structure is based on the TCP/IP model, although the similar seven-layer OSI model still has a strong influence.

IEEE 802 is a group of standards for local area networks (LAN) and metropolitan area networks (MAN). The most well-known member of the IEEE 802 family is wireless LAN, commonly known as WLAN or Wi-Fi.

**4.Network Defense**

While nodes, links, and protocols are the building blocks of a network, a modern network also needs strong defenses. Security is crucial because huge amounts of data are constantly being created, moved, and processed. Some examples of network defense tools are firewalls, intrusion detection systems ([IDS](https://www.geeksforgeeks.org/intrusion-detection-system-ids/)), intrusion prevention systems ([IPS](https://www.geeksforgeeks.org/intrusion-prevention-system-ips/)), network access control ([NAC](https://www.geeksforgeeks.org/what-is-network-access-control/)), content filters, proxy servers, anti-DDoS devices, and load balancers.

How Does a Computer Network Work?

Computer Networks simply work using nodes and links. Data communication equipment is simply termed as Nodes. For example, [Modems](https://www.geeksforgeeks.org/what-is-modem/), Hubs, Switches, etc. whereas links in Computer networks can be referred to as a connection between two nodes. We have several types of links like cable wires, [optical fibers](https://www.geeksforgeeks.org/fiber-optics-and-types), etc.

Whenever a Computer Network is working, nodes have the work of sending and receiving data via the links. Computer Network provides some set of protocols that help in following the rules and protocols.

**Criteria of a Good Network**

**Performance:**It can be measured in many ways, including transmit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of the network depends on a number of factors, including the number of users, the type of medium & Hardware.

**Reliability:**In addition to accuracy is measured by frequency of failure, the time it takes a link to recover from failure, and the network’s robustness in catastrophe.

**Security:** Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data loss.

**Goals of Computer Networking**

Programs do not have to execute on a single system because of resource and load sharing

Reduced costs – Multiple machines can share printers, tape drives, and other peripherals

Reliability – If one machine fails, another can take its place

Scalability (it’s simple to add more processors or computers)

Communication and mail (people living apart can work together)

Information Access (remote information access, access to the internet, e-mail, video conferencing, and online shopping)

Entertainment that is interactive (online games, videos, etc.)

Social Networking

**Types of Computer Networks**

Division Based on Area Covered

**Local Area Network (LAN):** A [LAN](https://www.geeksforgeeks.org/lan-full-form) is a network that covers an area of around 10 kilometers. For example, a college network or an office network. Depending upon the needs of the organization, a LAN can be a single office, building, or Campus. We can have two PCs and one printer in-home office or it can extend throughout the company and include audio and video devices. Each host in LAN has an identifier, an address that defines hosts in LAN. A packet sent by the host to another host carries both the source host’s and the destination host’s address.

**Metropolitan Area Network (MAN):**[MAN](https://www.geeksforgeeks.org/man-full-form-in-computer-networking) refers to a network that covers an entire city. For example: consider the cable television network.

**Wide Area Network (WAN):** [WAN](https://www.geeksforgeeks.org/wan-full-form) refers to a network that connects countries or continents. For example, the Internet allows users to access a distributed system called www from anywhere around the globe.WAN interconnects connecting devices such as switches, routers, or modems. A LAN is normally privately owned by an organization that uses it. We see two distinct examples of WANs today: point-to-point WANs and Switched WANs

**Point To Point**: Connects two connecting devices through transmission media.

**Switched:** A switched WAN is a network with more than two ends.

Based on Types of Communication

**Point To Point networks:**[Point-to-Point networking](https://www.geeksforgeeks.org/differences-between-point-to-point-and-multi-point-communication/) is a type of data networking that establishes a direct link between two networking nodes.  
A direct link between two devices, such as a computer and a printer, is known as a point-to-point connection.

**Multipoint**: is the one in which more than two specific devices share links. In the multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection.

**Broadcast networks:**In[broadcast networks](https://www.geeksforgeeks.org/types-of-broadcast-network/), a signal method in which numerous parties can hear a single sender. Radio stations are an excellent illustration of the “Broadcast Network” in everyday life. The radio station is a sender of data/signal in this scenario, and data is only intended to travel in one direction. Away from the radio transmission tower, to be precise.

Based on the Type of Architecture

**P2P Networks:**Computers with similar capabilities and configurations are referred to as peers. The “peers” in a[peer-to-peer](https://www.geeksforgeeks.org/what-is-p2p-peer-to-peer-process/) network are computer systems that are connected to each other over the Internet. Without the use of a central server, files can be shared directly between systems on the network.

**Client-Server Networks:**Each computer or process on the network is either a client or a server in a client-server architecture (client/server). The client asks for services from the server, which the server provides. Servers are high-performance computers or processes that manage disc drives (file servers), printers (print servers), or network traffic (network servers)

**Hybrid Networks:**The hybrid model uses a combination of client-server and peer-to-peer architecture. Eg: Torrent.

**Types of Computer Network Architecture**

Computer Network Architecture is of two types. These types are mentioned below.

**Client-Server Architecture:**[Client-Server Architecture](https://www.geeksforgeeks.org/client-server-model) is basically the architecture where the clients and the server are connected as two clients can communicate with each other and the devices present work as servers in the network.

**Peer-to-Peer Architecture:**[Peer-to-Peer Architecture](https://www.geeksforgeeks.org/what-is-p2ppeer-to-peer-process), computers are connected to each other and each computer is equally capable of working as there is no central server here. Each device present here can be used as a client or server.

Types of Enterprise Computer Networks

There are three main types of Enterprise Computer Networks which are mentioned below.

**Local Area Network (LAN):**[Local Area Networks](https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan) are small-scale networks used in small companies or as test networks. It has a limited size.

**Wide Area Networks (WAN):**[Wide Area Networks](https://www.geeksforgeeks.org/difference-between-lan-and-wan) are networks that are used for a larger area than local area networks and are used for long-distance communication.

**Service Provider Networks:**Service Provider Networks are the networks that help in wireless communication, high-speed internet access, etc.

Key Objectives of Creating and Deploying a Computer Network

No industry—whether it’s education, retail, finance, tech, government, or healthcare—can function without well-designed computer networks. The larger the organization, the more complex the network becomes. Before starting the challenging job of creating and setting up a computer network, here are some key objectives to consider.

1. Resource Sharing

Today’s enterprises are spread across the globe, with critical assets being shared across departments, geographies, and time zones. Clients are no more bound by location. A network allows data and hardware to be accessible to every pertinent user. This also helps with interdepartmental data processing. For example, the marketing team analyzes customer data and product development cycles to enable executive decisions at the top level.

2. Resource Availability & Reliability

A network ensures that resources are not stuck in isolated areas and can be accessed from multiple locations. High reliability comes from having various sources of supply. Important resources are backed up across multiple machines, so they remain accessible even if there are hardware problems.

3. Performance Management

As a company grows, its workload increases. Adding one or more processors to the network boosts the overall performance of the system and allows it to handle this growth. Storing data in well-designed databases can significantly speed up searching and retrieving information.

4.Cost Savings

Big mainframe computers are costly, so it’s smarter to add processors strategically throughout the system. This boosts performance and saves money. Networks let employees access information quickly, saving operational time and costs. Centralized network administration means fewer investments are needed for IT support**.**

5. Increased Storage Capacity

Network-attached storage devices are great for employees who handle lots of data. For instance, the data science team doesn’t each need their own data storage for the large number of records they process. Centralized repositories are more efficient. As businesses deal with record amounts of customer data, the ability to expand storage capacity is crucial**.**

6. Streamlined Collaboration & Communication

Networks greatly influence how companies operate daily. Employees can share files, see each other’s work, sync calendars, and exchange ideas more efficiently. Internal messaging systems like Slack facilitate easy flow of information and conversations within modern enterprises. However, emails remain the formal mode of communication with clients, partners, and vendors.

7. Reduction of Errors

Networks decrease errors by ensuring everyone gets information from one source, even if they’re in different places. [Backed-up](https://www.geeksforgeeks.org/backup-and-restore/)data ensures consistency and continuity. Standard versions of customer and employee manuals can be easily accessed by many people without much trouble**.**

8. Secured Remote Access

Computer networks offer flexibility, which is crucial during uncertain times like now when natural disasters and pandemics are affecting the world. A secure network guarantees that users can access and work on sensitive data safely, even when they’re not at the company’s location. Mobile devices registered to the network can also provide multiple layers of authentication, ensuring that unauthorized users can’t access the system.

**What is Network Topology?**

The structure of the network and how each component is connected to the others are defined by the network topology. Different types of network topology are mentioned below:

**Bus Topology**

Every computer and network device is connected to a single cable in a [bus topology](https://www.geeksforgeeks.org/types-of-network-topology) network. Linear Bus topology is defined as having exactly two terminals.

Advantages

Installation is simple

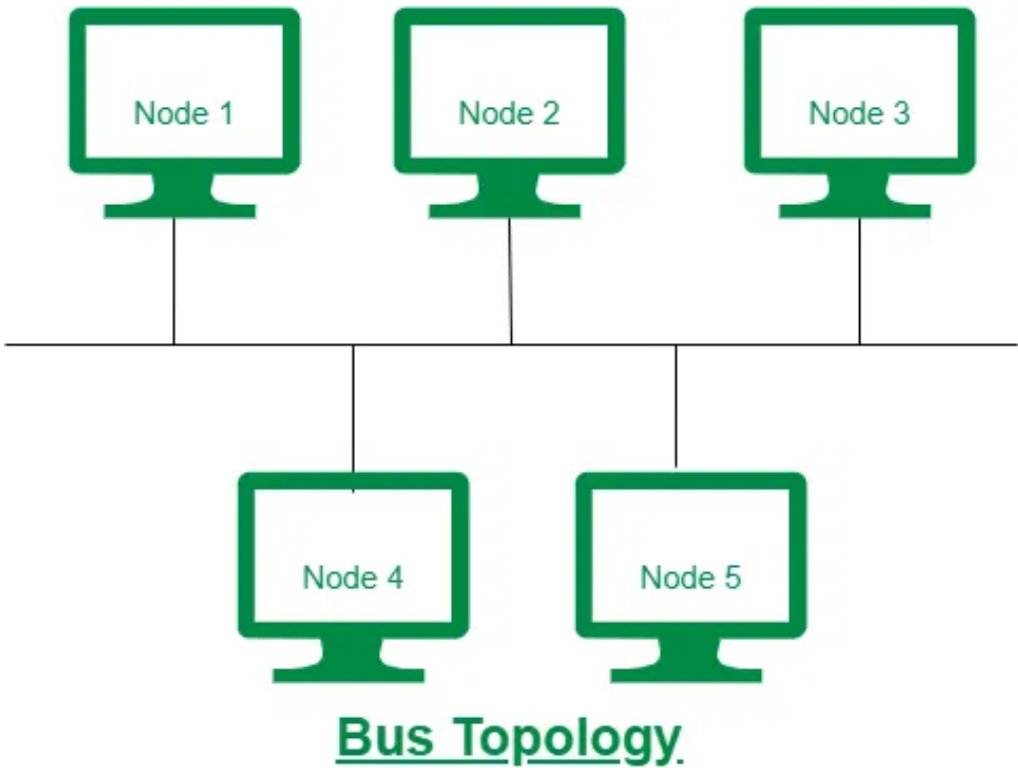
Compared to mesh, star, and tree topologies, the bus utilizes less cabling

Disadvantages

Difficulty in reconfiguring and isolating faults

A bus cable malfunction or break interrupts all communication

For more, you can refer to the [Advantages and Disadvantages of Bus Topology.](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-bus-topology)



**Ring Topology**

The topology is named ring topology because one computer is connected to another, with the final one being connected to the first. Exactly two neighbors for each device. A signal is passed along the ring in one direction. Each ring incorporates a repeater.

Advantages

Data transmission is relatively straightforward because packets only move in one direction

There is no requirement for a central controller to manage communication between nodes

Easy installation & Reconfiguration

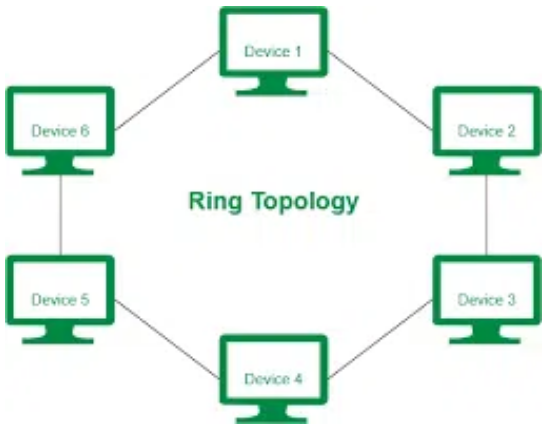
Simplified Faulty connections

Disadvantages

In a Unidirectional Ring, a data packet must traverse through all nodes

All computers must be turned on in order for them to connect with one another

For more, you can refer to the [Advantages and Disadvantages of Ring Topology.](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-ring-topology)



**Star Topology**

Each device in a star topology has a dedicated point-to-point link to a central controller, which is commonly referred to as the HUB. There is no direct connection between the devices. Traffic between the devices is not allowed in this topology. As an exchange, the controller is used.

Advantages

When attaching or disconnecting devices, there are no network interruptions

It’s simple to set up and configure

Identifying and isolating faults is simple

Less Expensive than mesh

Easy to install & configure

Disadvantages

Nodes attached to the hub, switch, or concentrator is failed if they fail

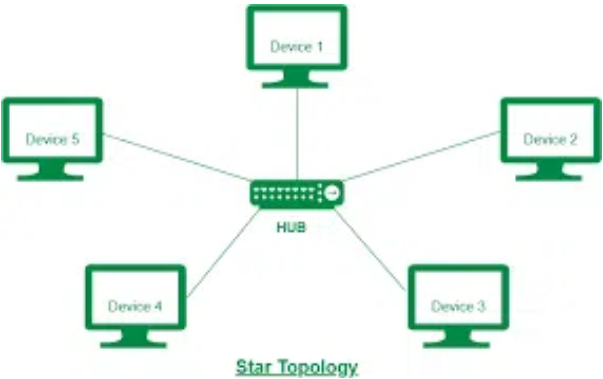
Because of the expense of the hubs, it is more expensive than linear bus topologies

More cable is required compared to a bus or ring

Too much dependency on Hub

For more, you can refer to the[Advantages and Disadvantages of Star Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-star-topology).

**Example:** Used in high-speed LANs



**Mesh Topology**

Every device in a mesh topology has dedicated point-to-point connectivity to every other device. The term “dedicated” refers to the fact that the link exclusively transports data between the two devices it links. To connect n devices, a fully connected mesh network contains n \*(n-1)/2 physical channels.

Advantages

Data can be sent from multiple devices at the same time. This topology can handle a lot of traffic.

Even if one of the connections fails, a backup is always available. As a result, data transit is unaffected.

Physical boundaries prevent other users from gaining access to messages.

Point to Point links make fault transmission & fault isolation easy.

Disadvantages

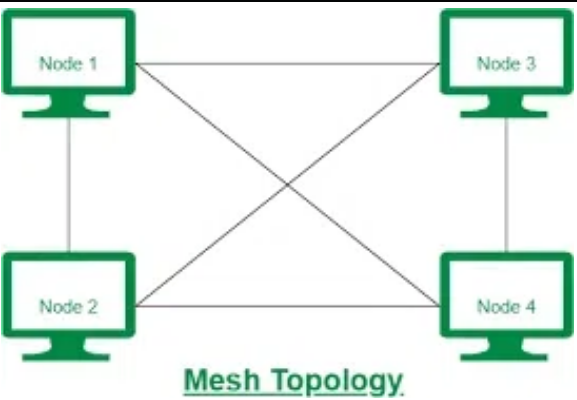
The amount of cabling and the number of I/O ports that are necessary.

The sheer bulk of wiring can be greater than the available space can accommodate.

It is difficult to install and reconfigure.

For more, you can refer to the [Advantages and Disadvantages of Mesh Topology](https://www.geeksforgeeks.org/advantage-and-disadvantage-of-mesh-topology).

**Example:**  connection of telephone regional office in which each regional office needs to be connected to every other regional office.



**Tree Topology**

The topology of a tree is similar to that of a star. Nodes in a tree, like those in a star, are connected to a central hub that manages network traffic. It has a root node, which is connected to all other nodes, producing a hierarchy. Hierarchical topology is another name for it. The number of Star networks is connected via Bus in Tree Topology.

Advantages

Network expansion is both possible and simple.

We partition the entire network into pieces (star networks) that are easier to manage and maintain.

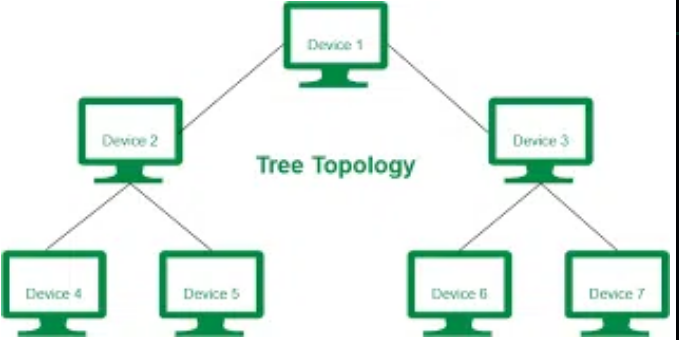
Other segments are unaffected if one segment is damaged.

Disadvantages

Tree topology relies largely on the main bus cable because of its basic structure, and if it fails, the entire network is handicapped.

Maintenance becomes more challenging when more nodes and segments are added.

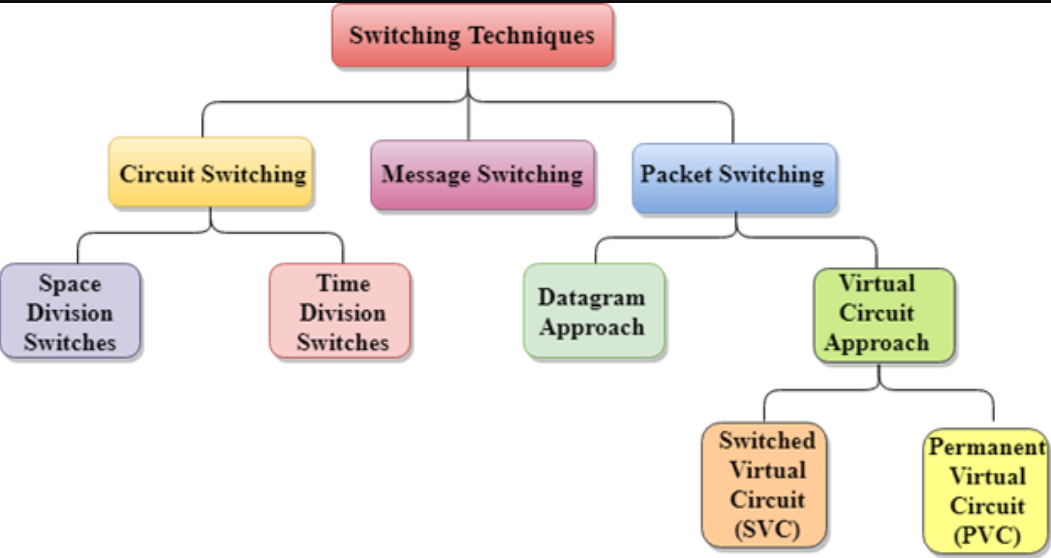
For more, you can refer to the [Advantages and Disadvantages of Tree Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-tree-topology).

****

**Switching**

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

****

**Circuit Switching** is a type of switching, in which a connection is established between the source and destination. This connection receives the complete bandwidth of the network until the data is transferred completely while **Packet Switching** in computer networks is a method of transferring data to a network in the form of packets. To transfer the file fast and efficiently over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called **Packet.**

**What is Circuit Switching?**

[Circuit switching](https://www.geeksforgeeks.org/circuit-switching-in-computer-network/) is a communication method where a dedicated communication path, or circuit, is established between two devices before data transmission begins. The circuit remains dedicated to the communication for the duration of the session, and no other devices can use it while the session is in progress. Circuit switching is commonly used in voice communication and some types of data communication.

**Advantages of Circuit Switching**

* **Guaranteed bandwidth:** Circuit switching provides a dedicated path for communication, ensuring that bandwidth is guaranteed for the duration of the call.
* **Low latency:** Circuit switching provides low latency because the path is predetermined, and there is no need to establish a connection for each packet.
* **Predictable performance:** Circuit switching provides predictable performance because the bandwidth is reserved, and there is no competition for resources.
* **Suitable for real-time communication:** Circuit switching is suitable for real-time communication, such as voice and video, because it provides low latency and predictable performance.

**Disadvantages of Circuit Switching**

* **Inefficient use of bandwidth:**Circuit switching is inefficient because the bandwidth is reserved for the entire duration of the call, even when no data is being transmitted.
* **Limited scalability:** Circuit switching is limited in its scalability because the number of circuits that can be established is finite, which can limit the number of simultaneous calls that can be made.
* **High cost:** Circuit switching is expensive because it requires dedicated resources, such as hardware and bandwidth, for the duration of the call.

**What is Packet Switching?**

[Packet switching](https://www.geeksforgeeks.org/packet-switching-and-delays-in-computer-network/)is a communication method where data is divided into smaller units called packets and transmitted over the network. Each packet contains the source and destination addresses, as well as other information needed for routing. The packets may take different paths to reach their destination, and they may be transmitted out of order or delayed due to network congestion.

**Advantages of Packet Switching**

* **Efficient use of bandwidth:**Packet switching is efficient because bandwidth is shared among multiple users, and resources are allocated only when data needs to be transmitted.
* **Flexible**: Packet switching is flexible and can handle a wide range of data rates and packet sizes.
* **Scalable:** Packet switching is highly scalable and can handle large amounts of traffic on a network.
* **Lower cost:** Packet switching is less expensive than circuit switching because resources are shared among multiple users.

**Disadvantages of Packet Switching**

* **Higher latency:**Packet switching has higher [latency](https://www.geeksforgeeks.org/what-is-latency/)than circuit switching because packets must be routed through multiple nodes, which can cause delay.
* **Limited QoS:** Packet switching provides limited QoS guarantees, meaning that different types of traffic may be treated equally.
* **Packet loss:** Packet switching can result in packet loss due to [congestion](https://www.geeksforgeeks.org/congestion-control-in-computer-networks/)on the network or errors in transmission.
* **Unsuitable for real-time communication:** Packet switching is not suitable for real-time communication, such as voice and video, because of the potential for latency and packet loss.

**Similarities**

* Both methods involve the transmission of data over a network.
* Both methods use a [physical layer](https://www.geeksforgeeks.org/physical-layer-in-osi-model/) of the [OSI model](https://www.geeksforgeeks.org/open-systems-interconnection-model-osi/) for transmission of data.
* Both methods can be used to transmit voice, video, and data.
* Both methods can be used in the same network infrastructure.
* Both methods can be used for both wired and wireless networks.

Difference between Circuit Switching and Packet Switching

| Circuit Switching | Packet Switching |
| --- | --- |
| In-circuit switching has there are 3 phases:  i) Connection Establishment.  ii) Data Transfer.  iii) Connection Released. | In Packet switching directly data transfer takes place. |
| In-circuit switching, each data unit knows the entire path address which is provided by the source. | In Packet switching, each data unit just knows the final destination address intermediate path is decided by the routers. |
| In-Circuit switching, data is processed at the source system only | In Packet switching, data is processed at all intermediate nodes including the source system. |
| The delay between data units in circuit switching is uniform. | The delay between data units in packet switching is not uniform. |
| Resource reservation is the feature of circuit switching because the path is fixed for data transmission. | There is no resource reservation because bandwidth is shared among users. |
| Circuit switching is more reliable. | Packet switching is less reliable. |
| Wastage of resources is more in Circuit Switching | Less wastage of resources as compared to Circuit Switching |
| It is not a store and forward technique. | It is a store and forward technique. |
| Transmission of the data is done by the source. | Transmission of the data is done not only by the source but also by the intermediate routers. |
| Congestion can occur during the connection establishment phase because there might be a case where a request is being made for a channel but the channel is already occupied. | Congestion can occur during the data transfer phase, a large number of packets comes in no time. |
| Circuit switching is not convenient for handling bilateral traffic. | Packet switching is suitable for handling bilateral traffic. |
| In-Circuit switching, the charge depends on time and distance, not on traffic in the network. | In Packet switching, the charge is based on the number of bytes and connection time. |
| Recording of packets is never possible in circuit switching. | Recording of packets is possible in packet switching. |
| In-Circuit Switching there is a physical path between the source and the destination | In Packet Switching there is no physical path between the source and the destination |
| Circuit Switching does not support store and forward transmission | Packet Switching supports store and forward transmission |
| Call setup is required in circuit switching. | No call setup is required in packet switching. |
| In-circuit switching each packet follows the same route. | In packet switching packets can follow any route. |
| The circuit switching network is implemented at the physical layer. | Packet switching is implemented at the datalink layer and network layer |
| Circuit switching requires simple protocols for delivery. | Packet switching requires complex protocols for delivery. |

**Protocols and Protocol Architecture**

## What is Network Protocol?

A network protocol is a set of rules that govern data communication between different devices in the network. It determines what is being communicated, how it is being communicated, and when it is being communicated. It permits connected devices to communicate with each other, irrespective of internal and structural differences.

## How do Network Protocols Work?

It is essential to understand how devices communicate over a network by recognizing network protocols. The [Open Systems Interconnection (OSI),](https://www.geeksforgeeks.org/open-systems-interconnection-model-osi/) the most widely used model, illustrates how computer systems interact with one another over a network. The communication mechanism between two network devices is shown by seven different layers in the OSI model. Every layer in the OSI model works based on different network protocols. At every layer, one or more protocols are there for network communication. To enable network-to-network connections, the Internet Protocol (IP), for instance, routes data by controlling information like the source and destination addresses of data packets. It is known as a network layer protocol.

## Types of Network Protocols

In most cases, communication across a network like the [Internet](https://www.geeksforgeeks.org/internet-and-its-services/) uses the [OSI model](https://www.geeksforgeeks.org/layers-of-osi-model/). The OSI model has a total of seven layers. Secured connections, network management, and [network communication](https://www.geeksforgeeks.org/network-and-communication/)are the three main tasks that the [network protocol](https://www.geeksforgeeks.org/elements-of-network-protocol/) performs. The purpose of protocols is to link different devices.

The protocols can be broadly classified into three major categories:

* Network Communication
* Network Management
* Network Security

## ****1. Network Communication****

Communication protocols are really important for the functioning of a network. They are so crucial that it is not possible to have computer networks without them. These protocols formally set out the rules and formats through which data is transferred. These protocols handle syntax, semantics, error detection, synchronization, and authentication. Below mentioned are some network communication protocol:

### **Hypertext Transfer Protocol(HTTP)**

It is a layer 7 protocol that is designed for transferring a hypertext between two or more systems.[HTTP](https://www.geeksforgeeks.org/http-full-form/) works on a [client-server model](https://www.geeksforgeeks.org/client-server-model/), most of the data sharing over the web is done through using HTTP.

### **Transmission Control Protocol(TCP)**

[TCP](https://www.geeksforgeeks.org/tcp-ip-model/) layouts a reliable stream delivery by using sequenced acknowledgment. It is a [connection-oriented](https://www.geeksforgeeks.org/connection-oriented-service/)protocol i.e., it establishes a connection between applications before sending any [data](https://www.geeksforgeeks.org/what-is-data/). It is used for communicating over a network. It has many applications such as [emails](https://www.geeksforgeeks.org/email-protocols/), [FTP](https://www.geeksforgeeks.org/file-transfer-protocol-ftp/), streaming media, etc.

### **User Datagram Protocol(UDP)**

It is a connectionless protocol that lay-out a basic but unreliable message service. It adds no [flow control](https://www.geeksforgeeks.org/flow-control-in-data-link-layer/), reliability, or [error-recovery](https://www.geeksforgeeks.org/what-is-error-recovery/)functions. [UPD](https://www.geeksforgeeks.org/user-datagram-protocol-udp/) is functional in cases where reliability is not required. It is used when we want faster transmission, for [multicasting and broadcasting](https://www.geeksforgeeks.org/difference-between-broadcast-and-multicast/) connections, etc.

### **Border Gateway Protocol(BGP)**

[BGP](https://www.geeksforgeeks.org/border-gateway-protocol-bgp/)is a routing protocol that controls how packets pass through the router in an independent system one or more networks run by a single organization and connect to different networks. It connects the endpoints of a [LAN](https://www.geeksforgeeks.org/lan-full-form/) with other LANs and it also connects endpoints in different LANs to one another.

### **Address Resolution Protocol(ARP)**

[ARP](https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/) is a protocol that helps in mapping logical addresses to the physical addresses acknowledged in a local network. For mapping and maintaining a correlation between these logical and physical addresses a table known as ARP cache is used.

### **Internet Protocol(IP)**

It is a protocol through which data is sent from one host to another over the internet. It is used for addressing and routing data packets so that they can reach their destination.

### **Dynamic Host Configuration Protocol(DHCP)**

it’s a protocol for network management and it’s used for the method of automating the process of configuring devices on IP networks. A [DHCP](https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/) server automatically assigns an [IP address](https://www.geeksforgeeks.org/what-is-an-ip-address/)and various other configurational changes to devices on a network so they can communicate with other IP networks. it also allows devices to use various services such as [NTP,](https://www.geeksforgeeks.org/network-time-protocol-ntp/)[DNS](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/), or any other protocol based on [TCP or UDP](https://www.geeksforgeeks.org/differences-between-tcp-and-udp/).

## ****2. Network Management****

These protocols assist in describing the procedures and policies that are used in monitoring, maintaining, and managing the computer network. These protocols also help in communicating these requirements across the network to ensure stable communication. Network management protocols can also be used for [troubleshooting](https://www.geeksforgeeks.org/how-to-troubleshoot-common-http-error-codes/) connections between a host and a client.

### **Internet Control Message Protocol(ICMP)**

It is a layer 3 protocol that is used by network devices to forward operational information and error messages. [ICMP](https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/) is used for reporting congestions, network errors, diagnostic purposes, and timeouts.

### **Simple Network Management Protocol(SNMP)**

It is a layer 7 protocol that is used for managing nodes on an IP network. There are three main components in the SNMP protocol i.e., [SNMP](https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/) agent, SNMP manager, and managed device. SNMP agent has the local knowledge of management details, it translates those details into a form that is compatible with the SNMP manager. The manager presents data acquired from SNMP agents, thus helping in monitoring network glitches, and network performance, and troubleshooting them.

### **Gopher**

It is a type of file retrieval protocol that provides downloadable files with some description for easy management, retrieving, and searching of files. All the files are arranged on a remote computer in a stratified manner. Gopher is an old protocol and it is not much used nowadays.

### **File Transfer Protocol(FTP)**

[FTP](https://www.geeksforgeeks.org/file-transfer-protocol-ftp/) is a Client/server protocol that is used for moving files to or from a host computer, it allows users to download [files, programs](https://www.geeksforgeeks.org/difference-between-program-and-file/), [web pages](https://www.geeksforgeeks.org/web-pages/), and other things that are available on other services.

### Post Office Protocol**(POP3)**

It is a protocol that a local mail client uses to get email messages from a remote email server over a TCP/IP connection. Email servers hosted by ISPs also use the [POP3](https://www.geeksforgeeks.org/what-is-pop3-post-office-protocol-version-3/) protocol to hold and receive emails intended for their users. Eventually, these users will use email client software to look at their mailbox on the remote server and to download their emails. After the email client downloads the emails, they are generally deleted from the servers.

### **Telnet**

It is a protocol that allows the user to connect to a remote computer program and to use it i.e., it is designed for remote connectivity. [Telnet](https://www.geeksforgeeks.org/introduction-to-telnet/) creates a connection between a host machine and a remote endpoint to enable a remote session.

## ****3. Network Security****

These protocols secure the data in passage over a network. These protocols also determine how the network secures data from any unauthorized attempts to extract or review data. These protocols make sure that no unauthorized devices, users, or services can access the network data. Primarily, these protocols depend on encryption to secure data.

### **Secure Socket Layer(SSL)**

It is a network security protocol mainly used for protecting sensitive data and securing internet connections. SSL allows both server-to-server and client-to-server communication. All the data transferred through[SSL](https://www.geeksforgeeks.org/secure-socket-layer-ssl/) is encrypted thus stopping any unauthorized person from accessing it.

### **Hypertext Transfer Protocol(HTTPS)**

It is the secured version of HTTP. this protocol ensures secure communication between two computers where one sends the request through the [browser](https://www.geeksforgeeks.org/browser-developer-tools/) and the other fetches the data from the [web server](https://www.geeksforgeeks.org/web-server-and-its-type/).

### **Transport Layer Security(TLS)**

It is a security protocol designed for [data security](https://www.geeksforgeeks.org/data-security/) and privacy over the internet, its functionality is encryption, checking the integrity of data i.e., whether it has been tampered with or not, and authentication. It is generally used for encrypted communication between servers and web apps, like a web browser loading a website, it can also be used for encryption of messages, emails, and [VoIP](https://www.geeksforgeeks.org/voice-over-internet-protocol-voip/).

## Some Other Protocols

### Internet Message Access Protocol (IMAP)

* ICMP protocol is used to retrieve message from the mail server. By using ICMP mail user can view and manage mails on his system.

### Session Initiation Protocol (SIP)

* SIP is used in video, voice, and messaging application. This protocol is used to initiating, Managing, Terminating the session between two users while they are communicating.

### Real-Time Transport Protocol (RTP)

* This protocol is used to forward audio, video over IP network. This protocol is used with SIP protocol to send audio, video at real-time.

### Rout Access Protocol (RAP)

* RAP is used in network management. It helps to user for accessing the nearest router for communication. RAP is less efficient as compared to [SNMP](https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/).

### Point To Point Tunnelling Protocol (PPTP)

* It is used to implement VPN ( Virtual Private Network ). PPTP protocol append PPP frame in IP datagram for transmission through IP based network.

### Trivial File Transfer Protocol (TFTP)

* TFTP is the simplified version of FTP. TFTP is also used to transfer file over internet

### Resource Location Protocol (RLP)

* RLP is used to assign the resource such as server, printer, or other devices over the internet to the user. It is used to locate the resource to the client for broadcast query.

**Reference Models**

**In computer networks, reference models give a conceptual framework that standardizes communication between heterogeneous networks.**

**The two popular reference models are −**

* **OSI Model**
* **TCP/IP Protocol Suite**

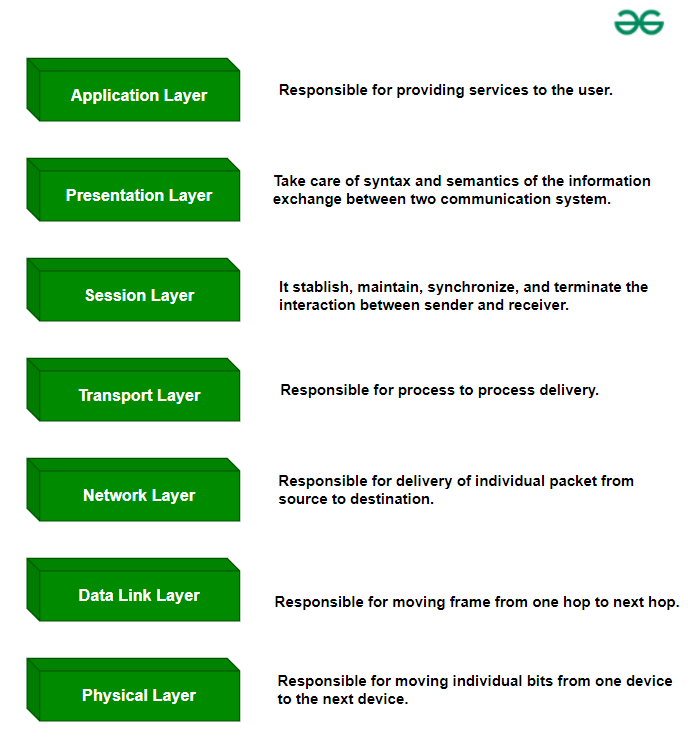
**What is OSI Model? – Layers of OSI Model**

**OSI stands for Open Systems Interconnection, where open stands to say non-proprietary. It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe. The OSI reference model was developed by ISO – ‘International Organization for Standardization‘, in the year 1984.**

**The OSI model provides a theoretical foundation for understanding network communication. However, it is usually not directly implemented in its entirety in real-world networking hardware or software. Instead, specific protocols and technologies are often designed based on the principles outlined in the OSI model to facilitate efficient data transmission and networking operations**

**What is OSI Model?**

**The OSI model, created in 1984 by**[**ISO**](https://www.geeksforgeeks.org/iso-9000-certification-in-software-engineering)**, is a reference framework that explains the process of transmitting data between computers. It is divided into seven layers that work together to carry out specialised network functions, allowing for a more systematic approach to networking.**

****

***OSI Model***

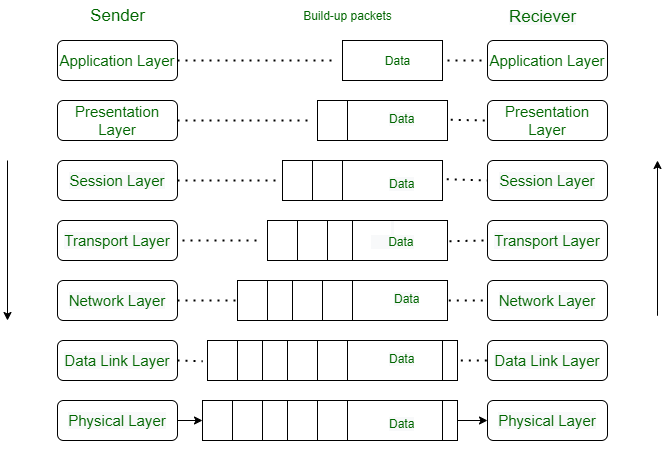
**Data Flow In OSI Model**

**When we transfer information from one device to another, it travels through 7 layers of OSI model. First data travels down through 7 layers from the sender’s end and then climbs back 7 layers on the receiver’s end.**

**Data flows through the OSI model in a step-by-step process:**

* **Application Layer: Applications create the data.**
* **Presentation Layer: Data is formatted and encrypted.**
* **Session Layer: Connections are established and managed.**
* **Transport Layer: Data is broken into segments for reliable delivery.**
* **Network Layer: Segments are packaged into packets and routed.**
* **Data Link Layer: Packets are framed and sent to the next device.**
* **Physical Layer: Frames are converted into bits and transmitted physically.**

**Each layer adds specific information to ensure the data reaches its destination correctly, and these steps are reversed upon arrival.**

****

**Let’s look at it with an Example:**

**Luffy sends an e-mail to his friend Zoro.**

**Step 1: Luffy interacts with e-mail application like Gmail, outlook, etc. Writes his email to send. (This happens in Layer 7: Application layer)**

**Step 2: Mail application prepares for data transmission like encrypting data and formatting it for transmission. (This happens in Layer 6: Presentation Layer)**

**Step 3: There is a connection established between the sender and receiver on the internet. (This happens in Layer 5: Session Layer)**

**Step 4: Email data is broken into smaller segments. It adds sequence number and error-checking information to maintain the reliability of the information. (This happens in Layer 4: Transport Layer)**

**Step 5: Addressing of packets is done in order to find the best route for transfer. (This happens in Layer 3: Network Layer)**

**Step 6: Data packets are encapsulated into frames, then MAC address is added for local devices and then it checks for error using error detection. (This happens in Layer 2: Data Link Layer)**

**Step 7: Lastly Frames are transmitted in the form of electrical/ optical signals over a physical network medium like ethernet cable or WiFi.**

**After the email reaches the receiver i.e. Zoro, the process will reverse and decrypt the e-mail content. At last, the email will be shown on Zoro’s email client.**

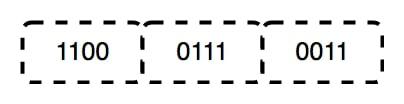
**What Are The 7 Layers of The OSI Model?**

**The OSI model consists of seven abstraction layers arranged in a top-down order:**

1. [**Physical Layer**](https://www.geeksforgeeks.org/physical-layer-in-osi-model)
2. [**Data Link Layer**](https://www.geeksforgeeks.org/data-link-layer)
3. [**Network Layer**](https://www.geeksforgeeks.org/network-layer-services-packetizing-routing-and-forwarding)
4. [**Transport Layer**](https://www.geeksforgeeks.org/transport-layer-responsibilities)
5. [**Session Layer**](https://www.geeksforgeeks.org/session-layer-in-osi-model)
6. [**Presentation Layer**](https://www.geeksforgeeks.org/presentation-layer-in-osi-model)
7. [**Application Layer**](https://www.geeksforgeeks.org/application-layer-in-osi-model)

**Physical Layer – Layer 1**

**The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.**

****

**Functions of the Physical Layer**

* **Bit Synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.**
* **Bit Rate Control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.**
* **Physical Topologies: Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.**
* **Transmission Mode: Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.**

***Note:***

* ***Hub, Repeater, Modem, and Cables are Physical Layer devices.***
* ***Network Layer, Data Link Layer, and Physical Layer are also known as Lower Layers or Hardware Layers.***

**Data Link Layer (DLL) – Layer 2**

**The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its**[**MAC address**](https://www.geeksforgeeks.org/mac-address-in-computer-network)**.   
The Data Link Layer is divided into two sublayers:**

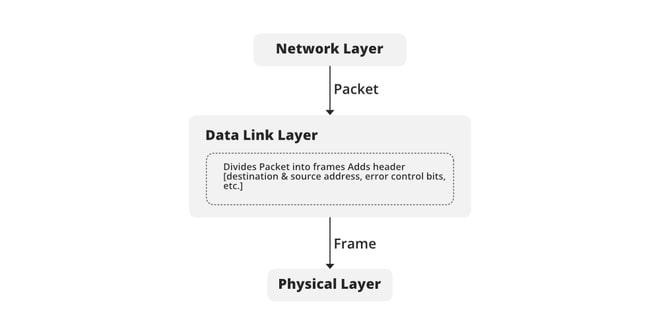
* [**Logical Link Control (LLC)**](https://www.geeksforgeeks.org/logical-link-control-llc-protocol-data-unit)
* [**Media Access Control (MAC)**](https://www.geeksforgeeks.org/introduction-of-mac-address-in-computer-network)

**The packet received from the Network layer is further divided into frames depending on the frame size of the NIC(Network Interface Card). DLL also encapsulates Sender and Receiver’s MAC address in the header.**

**The Receiver’s MAC address is obtained by placing an**[**ARP(Address Resolution Protocol)**](https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works)**request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.**

**Functions of the Data Link Layer**

* **Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.**
* **Physical Addressing: After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.**
* **Error Control: The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.**
* **Flow Control: The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.**
* **Access Control: When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.**

****

***Note:***

* ***Packet in the Data Link layer is referred to as Frame.***
* ***Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.***
* ***Switch & Bridge are Data Link Layer devices.***

**Network Layer – Layer 3**

**The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver’s**[**IP address**](https://www.geeksforgeeks.org/what-is-an-ip-address)**es are placed in the header by the network layer.**

**Functions of the Network Layer**

* **Routing: The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.**
* **Logical Addressing: To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender & receiver’s IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.**

***Note:***

* ***Segment in the Network layer is referred to as Packet.***
* ***Network layer is implemented by networking devices such as routers and switches.***

**Transport Layer – Layer 4**

**The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the end-to-end delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.**

**At the sender’s side: The transport layer receives the formatted data from the upper layers, performs Segmentation, and also implements Flow and error control to ensure proper data transmission. It also adds Source and Destination**[**port number**](https://www.geeksforgeeks.org/what-is-ports-in-networking)**s in its header and forwards the segmented data to the Network Layer.**

***Note: The sender needs to know the port number associated with the receiver’s application.***

***Generally, this destination port number is configured, either by default or manually. For example, when a web application requests a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.***

**At the receiver’s side: Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.**

**Functions of the Transport Layer**

* **Segmentation and Reassembly: This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.**
* **Service Point Addressing: To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.**

**Services Provided by Transport Layer**

* [**Connection-Oriented Service**](https://www.geeksforgeeks.org/connection-oriented-service)
* [**Connectionless Service**](https://www.geeksforgeeks.org/connection-less-service)

**1. Connection-Oriented Service: It is a three-phase process that includes:**

* **Connection Establishment**
* **Data Transfer**
* **Termination/disconnection**

**In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.**

**2. Connectionless service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.**

***Note:***

* ***Data in the Transport Layer is called Segments.***
* ***Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.***
* ***The transport layer is called as Heart of the OSI model.***
* ***Device or Protocol Use : TCP, UDP  NetBIOS, PPTP***

**Session Layer – Layer 5**

**This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.**

**Functions of the Session Layer**

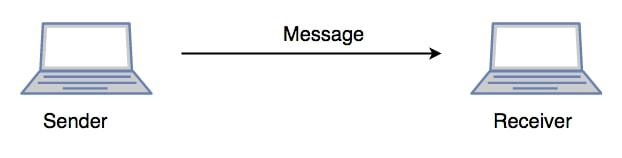
* **Session Establishment, Maintenance, and Termination: The layer allows the two processes to establish, use, and terminate a connection.**
* **Synchronization: This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.**
* **Dialog Controller: The session layer allows two systems to start communication with each other in half-duplex or full-duplex.**

***Note:***

* ***All the below 3 layers(including Session Layer) are integrated as a single layer in the***[***TCP/IP***](https://www.geeksforgeeks.org/tcp-ip-model)***model as the “Application Layer”.***
* ***Implementation of these 3 layers is done by the network application itself. These are also known as Upper Layers or Software Layers.***
* ***Device or Protocol Use :  NetBIOS, PPTP.***

**Example**

**Let us consider a scenario where a user wants to send a message through some Messenger application running in their browser. The “Messenger” here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, optionally encrypted (if the data is sensitive), and converted into bits (0’s and 1’s) so that it can be transmitted.**

****

***Communication in Session Layer***

**Presentation Layer – Layer 6**

**The presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.**

**Functions of the Presentation Layer**

* **Translation: For example,**[**ASCII to EBCDIC**](https://www.geeksforgeeks.org/difference-between-ascii-and-ebcdic)**.**
* **Encryption/ Decryption: Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.**
* **Compression: Reduces the number of bits that need to be transmitted on the network.**

**Note: Device or Protocol Use:  JPEG, MPEG, GIF.**

**Application Layer – Layer 7**

**At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.**

**Example: Application – Browsers,**[**Skype**](https://www.geeksforgeeks.org/introduction-to-skype)**Messenger, etc.**

***Note: The application Layer is also called Desktop Layer.***

***Device or Protocol Use :***[***SMTP***](https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp)***.***

**Functions of the Application Layer**

**The main functions of the application layer are given below.**

* **Network Virtual Terminal (NVT): It allows a user to log on to a remote host.**
* **File Transfer Access and Management(FTAM): This application allows a user to  
  access files in a remote host, retrieve files in a remote host, and manage or  
  control files from a remote computer.**
* **Mail Services: Provide email service.**
* **Directory Services: This application provides distributed database sources  
  and access for global information about various objects and services.**

***Note: The OSI model acts as a reference model and is not implemented on the Internet because of its late invention. The current model being used is the TCP/IP model.***

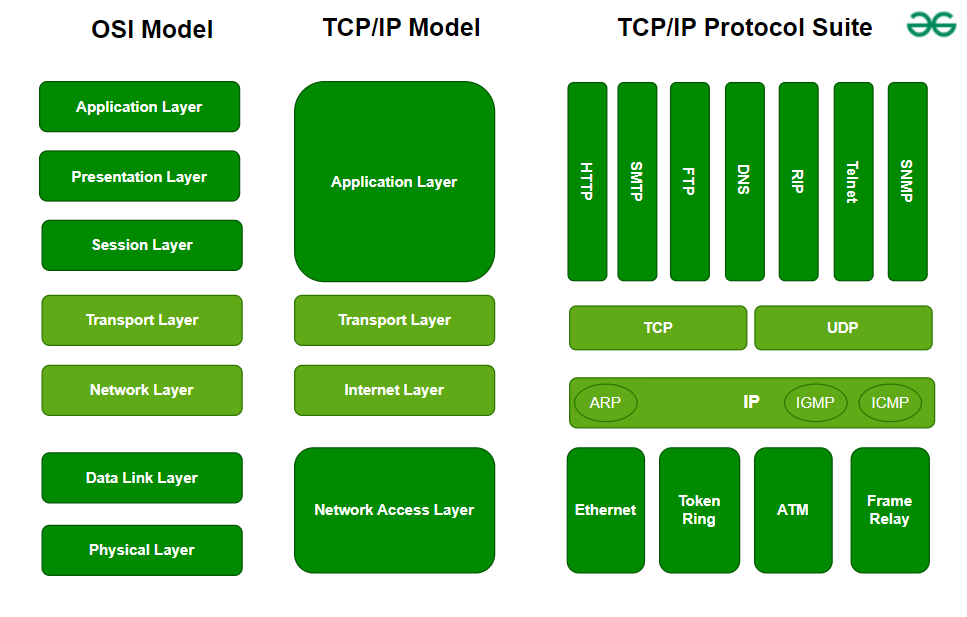
****

**OSI vs TCP/IP Model**

**TCP/IP protocol ( Transfer Control Protocol/Internet Protocol ) was created by U.S. Department of Defense’s Advanced Research Projects Agency (ARPA) in 1970s.**

**Some key differences between the OSI model and the**[**TCP/IP Model**](https://www.geeksforgeeks.org/tcp-ip-model)**are:**

* **TCP/IP model consists of 4 layers but OSI model has 7 layers. Layers 5,6,7 of the OSI model are combined into the Application Layer of TCP/IP model and OSI layers 1 and 2 are combined into Network Access Layers of TCP/IP protocol.**
* **The TCP/IP model is older than the OSI model, hence it is a foundational protocol that defines how should data be transferred online.**
* **Compared to the OSI model, the TCP/IP model has less strict layer boundaries.**
* **All layers of the TCP/IP model are needed for data transmission but in the OSI model, some applications can skip certain layers. Only layers 1,2 and 3 of the OSI model are necessary for data transmission.**

****

**Advantages of OSI Model**

* It divides network communication into 7 layers which makes it easier to understand and troubleshoot.
* It standardizes network communications, as each layer has fixed functions and protocols.
* Diagnosing network problems is easier with the OSI model.
* It is easier to improve with advancements as each layer can get updates separately.

**Disadvantages of OSI Model**

* Complexity: The OSI Model has seven layers, which can be complicated and hard to understand for beginners.
* Not Practical: In real-life networking, most systems use a simpler model called the Internet protocol suite (TCP/IP), so the OSI Model isn’t always directly applicable.
* Slow Adoption: When it was introduced, the OSI Model was not quickly adopted by the industry, which preferred the simpler and already-established TCP/IP model.
* Overhead: Each layer in the OSI Model adds its own set of rules and operations, which can make the process more time-consuming and less efficient.
* Theoretical: The OSI Model is more of a theoretical framework, meaning it’s great for understanding concepts but not always practical for implementation.

**TCP/IP Model**

**The TCP/IP model is a fundamental framework for computer networking. It stands for Transmission Control Protocol/Internet Protocol, which are the core protocols of the Internet. This model defines how data is transmitted over networks, ensuring reliable communication between devices. It consists of four layers: the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer. Each layer has specific functions that help manage different aspects of network communication, making it essential for understanding and working with modern networks.**

**TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model. In this article, we are going to discuss the TCP/IP model in detail.**

**What Does TCP/IP Do?**

**The main work of TCP/IP is to transfer the data of a computer from one device to another. The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end.**

**Layers of TCP/IP**

**1. Network Access Layer**

**It is a group of applications requiring network communications. This layer is responsible for generating the data and requesting connections. It acts on behalf of the sender and the Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.**

**The packet’s network protocol type, in this case, TCP/IP, is identified by network access layer. Error prevention and “framing” are also provided by this layer.**[**Point-to-Point Protocol (PPP)**](https://www.geeksforgeeks.org/point-to-point-protocol-ppp-frame-format)**framing and Ethernet IEEE 802.2 framing are two examples of data-link layer protocols.**

**2. Internet Layer**

**This layer parallels the functions of OSI’s Network layer. It defines the protocols which are responsible for the logical transmission of data over the entire network. The main protocols residing at this layer are as follows:**

* **IP:**[**IP**](https://www.geeksforgeeks.org/what-is-an-ip-address)**stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.**
* **ICMP:**[**ICMP**](https://www.geeksforgeeks.org/difference-between-icmp-and-igmp)**stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.**
* **ARP:**[**ARP**](https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works)**stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP.**

**The Internet Layer is a layer in the Internet Protocol (IP) suite, which is the set of protocols that define the Internet. The Internet Layer is responsible for routing packets of data from one device to another across a network. It does this by assigning each device a unique IP address, which is used to identify the device and determine the route that packets should take to reach it.**

**Example: Imagine that you are using a computer to send an email to a friend. When you click “send,” the email is broken down into smaller packets of data, which are then sent to the Internet Layer for routing. The Internet Layer assigns an IP address to each packet and uses routing tables to determine the best route for the packet to take to reach its destination. The packet is then forwarded to the next hop on its route until it reaches its destination. When all of the packets have been delivered, your friend’s computer can reassemble them into the original email message.**

**In this example, the Internet Layer plays a crucial role in delivering the email from your computer to your friend’s computer. It uses IP addresses and routing tables to determine the best route for the packets to take, and it ensures that the packets are delivered to the correct destination. Without the Internet Layer, it would not be possible to send data across the Internet.**

**3. Transport Layer**

**The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error. End-to-end communication is referred to as such. Transmission Control Protocol (TCP) and User Datagram Protocol are transport layer protocols at this level (UDP).**

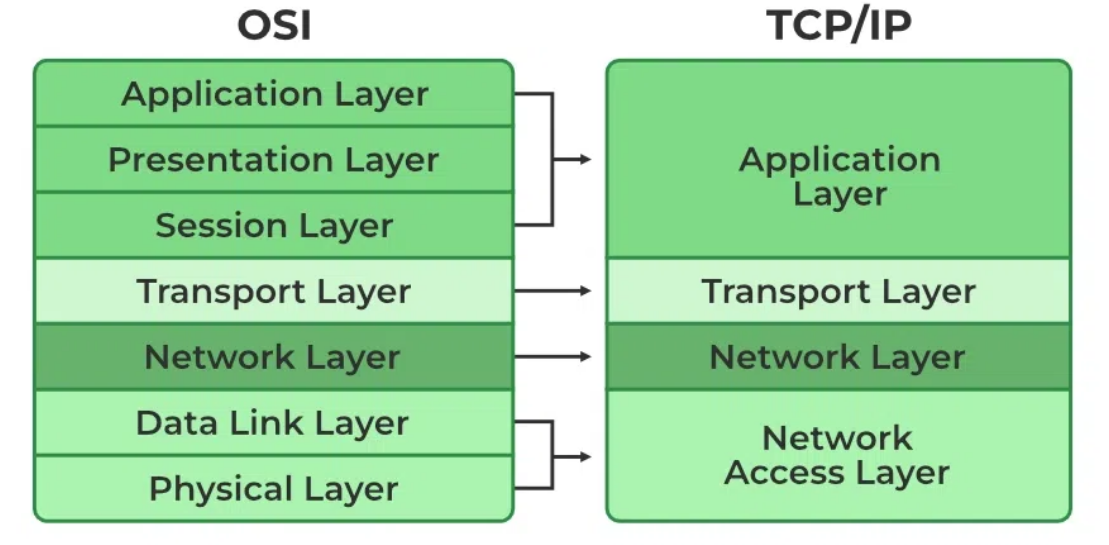
* **TCP: Applications can interact with one another using**[**TCP**](https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp)**as though they were physically connected by a circuit. TCP transmits data in a way that resembles character-by-character transmission rather than separate packets. A starting point that establishes the connection, the whole transmission in byte order, and an ending point that closes the connection make up this transmission.**
* **UDP: The datagram delivery service is provided by**[**UDP**](https://www.geeksforgeeks.org/user-datagram-protocol-udp)**, the other transport layer protocol. Connections between receiving and sending hosts are not verified by UDP. Applications that transport little amounts of data use UDP rather than TCP because it eliminates the processes of establishing and validating connections.**

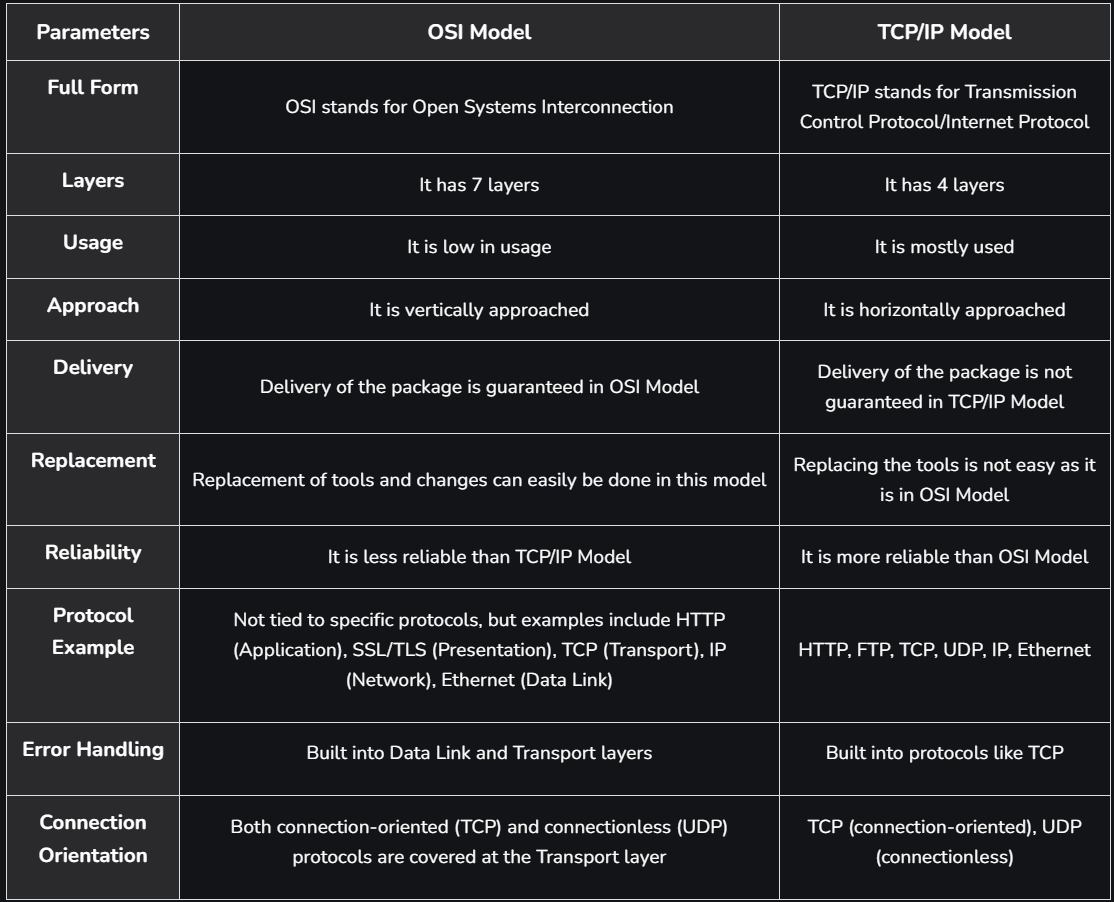
**4. Application Layer**

**This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The three main protocols present in this layer are:**

* **HTTP and HTTPS:**[**HTTP**](https://www.geeksforgeeks.org/difference-between-http-and-https-2)**stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and carry out bank transactions.**
* **SSH:**[**SSH**](https://www.geeksforgeeks.org/introduction-to-sshsecure-shell-keys)**stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.**
* **NTP:**[**NTP**](https://www.geeksforgeeks.org/network-time-protocol-ntp)**stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.**

**Difference between TCP/IP and OSI Model**

****

****

**Advantages of TCP/IP Model**

* Interoperability: The TCP/IP model allows different types of computers and networks to communicate with each other, promoting compatibility and cooperation among diverse systems.
* Scalability: TCP/IP is highly scalable, making it suitable for both small and large networks, from local area networks (LANs) to wide area networks (WANs) like the internet.
* Standardization: It is based on open standards and protocols, ensuring that different devices and software can work together without compatibility issues.
* Flexibility: The model supports various routing protocols, data types, and communication methods, making it adaptable to different networking needs.
* Reliability: TCP/IP includes error-checking and retransmission features that ensure reliable data transfer, even over long distances and through various network conditions.

**Disadvantages of TCP/IP Model**

* Complex Configuration: Setting up and managing a TCP/IP network can be complex, especially for large networks with many devices. This complexity can lead to configuration errors.
* Security Concerns: TCP/IP was not originally designed with security in mind. While there are now many security protocols available (such as SSL/TLS), they have been added on top of the basic TCP/IP model, which can lead to vulnerabilities.
* Inefficiency for Small Networks: For very small networks, the overhead and complexity of the TCP/IP model may be unnecessary and inefficient compared to simpler networking protocols.
* Limited by Address Space: Although IPv6 addresses this issue, the older IPv4 system has a limited address space, which can lead to issues with address exhaustion in larger networks.
* Data Overhead: TCP, the transport protocol, includes a significant amount of overhead to ensure reliable transmission. This can reduce efficiency, especially for small data packets or in networks where speed is crucial.

**Design Issues for the layers**

A number of design issues exist for the layer to layer approach of computer networks. Some of the main design issues are as follows −

**Reliability**

Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not distorted.

**Scalability**

Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

**Addressing**

At a particular time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.

**Error Control**

Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

**Flow Control**

If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

**Resource Allocation**

Computer networks provide services in the form of network resources to the end users. The main design issue is to allocate and deallocate resources to processes. The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

**Statistical Multiplexing**

It is not feasible to allocate a dedicated path for each message while it is being transferred from the source to the destination. So, the data channel needs to be multiplexed, so as to allocate a fraction of the bandwidth or time to each host.

**Routing**

There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

**Security**

A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

Designing layers in a computer network involves several considerations to ensure efficient, reliable, and scalable communication between devices. Each layer of a network architecture serves a specific purpose and has its own set of design issues. Here’s a breakdown of common design issues associated with different layers of a computer network:

**1. Physical Layer**

Media Choice: Selecting between wired (e.g., Ethernet, fiber optic) and wireless (e.g., Wi-Fi, Bluetooth) media based on factors like distance, bandwidth requirements, and environmental conditions.

Signal Integrity: Ensuring that signals are transmitted with minimal distortion and interference, which involves considering signal attenuation, noise, and crosstalk.

Bandwidth and Speed: Choosing appropriate hardware and media that can handle the required data transfer speeds and bandwidth.

**2. Data Link Layer**

Error Detection and Correction: Implementing mechanisms to detect and correct errors in the transmitted data, such as checksums, CRC (Cyclic Redundancy Check), and error correction codes.

Frame Synchronization: Ensuring that data frames are correctly synchronized between sender and receiver, which involves dealing with frame delimiters and alignment.

Flow Control: Managing the rate of data transmission between devices to prevent overwhelming slower devices or networks, using protocols like sliding window or acknowledgments.

MAC Addressing: Designing efficient MAC (Media Access Control) address schemes and handling issues related to MAC address conflicts and uniqueness.

**3. Network Layer**

Routing and Forwarding: Developing efficient routing algorithms and protocols to determine the best path for data to travel across the network, and managing issues related to routing table updates and convergence.

Addressing: Implementing addressing schemes (e.g., IP addressing) that ensure unique identification of devices and effective communication, including handling subnetting and address allocation.

Scalability: Designing the network to scale with increasing numbers of devices and traffic, which includes handling issues like IP address exhaustion and hierarchical routing.

**4. Transport Layer**

Connection Management: Managing the establishment, maintenance, and termination of connections, including handling issues related to connection setup and teardown.

Reliability: Ensuring reliable data transfer through mechanisms like retransmission of lost packets, acknowledgment of received packets, and in-order delivery of data.

Flow Control: Managing data flow between sender and receiver to prevent buffer overflow and ensure efficient use of network resources.

**5. Session Layer**

Session Management: Handling the establishment, management, and termination of sessions between applications, including dealing with session state and synchronization.

Checkpointing and Recovery: Implementing mechanisms to save the state of a session and recover from interruptions or failures, ensuring data consistency and continuity.

**6. Presentation Layer**

Data Translation: Ensuring that data is correctly translated between different formats and representations, such as character encoding and data compression.

Encryption and Decryption: Implementing security measures to protect data confidentiality and integrity through encryption and decryption processes.

**7. Application Layer**

Protocol Design: Designing application-level protocols that define how applications communicate over the network, including handling issues related to protocol efficiency and robustness.

Interoperability: Ensuring that applications from different vendors or running on different platforms can communicate effectively, which involves standardizing interfaces and data formats.

Security: Implementing security measures to protect data from unauthorized access, including authentication, authorization, and data encryption.

**General Design Issues Across Layers**

Scalability: Ensuring that the network design can handle growth in terms of the number of devices, traffic volume, and geographic expansion.

Reliability and Fault Tolerance: Designing the network to handle failures and recover gracefully, including implementing redundancy and failover mechanisms.

Performance: Optimizing network performance by minimizing latency, maximizing throughput, and managing congestion.

Security: Addressing security concerns at all layers to protect against various types of attacks, including unauthorized access, data breaches, and denial-of-service attacks.

Designing a network involves careful consideration of these issues at each layer to create a robust, efficient, and secure communication system.