**WEEK-2**

**What is a network?**

A computer network is a group of interconnected devices that are designed to communicate and share information with each other.

## Advantages of Uses of Computer Networks

Here are the advantages uses of a computer network:

* Improved communication and collaboration.
* Cost savings through resource sharing.
* Better data management and security.
* Increased flexibility with remote access.
* Enhanced productivity and efficiency

## Disadvantages of Uses of Computer Networks

Here are the disadvantages uses of a computer network:

* Security risks and potential for data breaches.
* Technical issues and maintenance challenges.
* Increased vulnerability to viruses and malware.
* Potential for decreased privacy and confidentiality.

**Uses of computer networks**

1. **Resource sharing:** Networks allow users to share resources such as printers, scanners, and files, which can improve efficiency and reduce costs.
2. **Communication:** Computer networks enable individuals and organizations to communicate with each other using various methods such as email, messaging, and video conferencing.
3. Information Access
4. Centralized management
5. **Remote access:** Networks enable users to access information and resources from anywhere in the world, providing greater flexibility and convenience.
6. **Collaboration:** Networks facilitate collaboration by enabling users to work together on projects, share ideas, and provide feedback in real time.
7. **E-commerce:** Computer networks are used extensively in e-commerce, enabling businesses to sell products and services online and process payments securely.
8. **Education:** Networks are used in educational institutions to facilitate distance learning, provide access to educational resources, and enable collaboration among students and teachers.
9. **Entertainment:** Networks are used for entertainment purposes such as online gaming, streaming movies and music, and social media.

**Types of networks**

1. Local Area Network (LAN)

LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol.

Private addresses are unique in relation to other computers on the local network.

By definition, the connections must be high-speed and relatively inexpensive hardware (Such as hubs, network adapters, and Ethernet cables). LANs cover a smaller geographical area (Size is limited to a few kilometres) and are privately owned. One can use it for an office building, home, hospital, school, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted-pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

Routers are found at the boundary of a LAN, connecting them to the larger WAN.

Early LANs had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN. The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. LAN has a range up to 2km. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. The fault tolerance of a LAN is more and there is less congestion in this network. For example A bunch of students playing Counter-Strike in the same room (without internet).

#### **Advantages:**

* Provides fast data transfer rates and high-speed communication.
* Easy to set up and manage.
* Can be used to share peripheral devices such as printers and scanners.
* Provides increased security and fault tolerance compared to WANs.

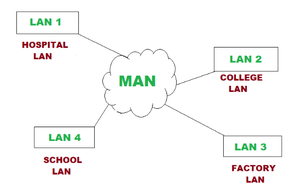
#### **Disadvantages:**

* Limited geographical coverage.
* Limited scalability and may require significant infrastructure upgrades to accommodate growth.
* May experience congestion and network performance issues with increased usage.

1. Metropolitan Area Network (MAN)

### Metropolitan Area Network (MAN) –

MAN or Metropolitan area Network covers a larger area than that covered by a LAN and a smaller area as compared to WAN. MAN has a range of 5-50km. It connects two or more computers that are apart but reside in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need high-speed connectivity. Speeds of MAN range in terms of Mbps. It’s hard to design and maintain a Metropolitan Area Network.



The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN are moderate. Devices used for transmission of data through MAN are Modem and Wire/Cable. Examples of a MAN are part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

#### **Advantages:**

* Provides high-speed connectivity over a larger geographical area than LAN.
* Can be used as an ISP for multiple customers.
* Offers higher data transfer rates than WAN in some cases.

#### **Disadvantages:**

* Can be expensive to set up and maintain.
* May experience congestion and network performance issues with increased usage.
* May have limited fault tolerance and security compared to LANs.

1. Wide Area Network (WAN)

### Wide Area Network (WAN) –

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. WAN has a range of above 50 km. A WAN could be a connection of LAN connecting to other LANs via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high-speed and relatively expensive.

There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long-distance transmission, the noise and error tend to be more in WAN.

WAN’s data rate is slow about a 10th LAN’s speed since it involves increased distance and increased number of servers and terminals etc. The speed of WAN ranges from a few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for the transmission of data through WAN are Optic wires, Microwaves, and Satellites. An example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is a dial-up line that connects a home computer to the Internet.

#### **Advantages:**

* Covers large geographical areas and can connect remote locations.
* Provides connectivity to the internet.
* Offers remote access to resources and applications.
* Can be used to support multiple users and applications simultaneously.

#### **Disadvantages:**

* Can be expensive to set up and maintain.
* Offers slower data transfer rates than LAN or MAN.
* May experience higher latency and longer propagation delays due to longer distances and multiple network hops.
* May have lower fault tolerance and security compared to LANs.

1. Personal Area Network (PAN)

It is the smallest network of computers.

Bluetooth or other infrared-enabled devices could be used to connect devices.

It has a 10-metre range of connectivity.

It can cover up to 30 feet in diameter.

PAN network enables a single person's personal devices to connect with each other.

**Network Topologies**

A network topology refers to how devices are connected in a network.

1. Bus

In bus network topology, all computers and network devices are connected to a single cable called bus. The bus cable acts as the shared communication medium for all the devices in the network.

When a device wants to transmit data, it sends the data on the bus cable. All other devices receive and check whether they are the intended recipients. The intended recipient accepts the data while others discard it.

Bus topology is inexpensive, easy to implement, and adds devices easily. However, it can be difficult to troubleshoot and isolate faults. Also, if the main bus cable fails, the entire network fails.

1. Ring

In ring network topology, all nodes are connected to form a circle. Each node is connected to the next node through a point-to-point link.

[Data](https://intellipaat.com/blog/what-is-data/) travels circularly from one node to the next until it reaches the intended recipient. Nodes can transmit data only after receiving a token, a special kind of data packet.

Ring topology provides equal access to the network for all nodes. However, failure of any link can bring down the entire network. Adding or removing nodes also disrupts the network.

1. Star

In a star network topology, all nodes are connected to a central device called a hub through a point-to-point link. The hub acts as a central node that manages and controls the entire network.

All data transmitted between nodes passes through the hub. The hub ensures that the data is directed to the intended recipient.

Star topology is easy to set up and expand, and faults are easily isolated. However, the hub represents a single point of failure. If the hub goes down, the entire network suffers. Star topology also provides limited bandwidth since all data flows through the hub.

1. Mesh

Every node in a mesh topology is linked to every other node. Point-to-point linkages connect the nodes to one another. Multiple links between nodes in the network can increase redundancy.

Data travels across the network using the shortest path available. If a link fails, the network automatically routes traffic through alternate paths.

Mesh topology is highly fault-tolerant and provides a lot of bandwidth. However, it is difficult and expensive to implement because the number of connections grows exponentially with the number of nodes.

1. Tree

A tree topology combines the characteristics of bus and star topologies. It consists of groups of star-configured workstations connected to a bus backbone cable.

Tree topology allows the expansion of a star network while still maintaining a bus structure. However, the backbone cable remains a single point of failure. Tree topology can be difficult to configure and wire.

1. Hybrid

A hybrid network topology combines two or more network topologies to get the benefits of each topology. For example, a star-bus topology consists of stars connected to a bus, while a star-ring topology has stars connected in a ring.

A hybrid topology offers outstanding efficiency, flexibility, and fault tolerance. However, execution and solving issues can be challenging. The implementation of various topologies may also result in increased costs.

|  |  |  |
| --- | --- | --- |
| **Topology** | **Pros** | **Cons** |
| **Bus** | Inexpensive Simple to expand        Easy to implement | Prone to faults Limited scalability Difficult to isolate faults |
| **Ring** | Equal access Deterministic    Avoid collision | Fault in any link affects whole network Difficult to add or remove nodes |
| **Mesh** | Redundant     Fault-tolerant   Highly scalable | Very expensive Difficult to setup and configure the number of links grows exponentially with nodes |
| **Star** | Easy to setup      Easy to expand        Fault isolation | Hub is a single point of failure Limited bandwidth |
| **Tree** | Expansion of star Some fault tolerance Low-cost | Bus cable is a single point of failure Difficult to configure |
| **Hybrid** | Flexibility Fault tolerance High performance | Complex Costly to implement Difficult to troubleshoot |

## **Use Cases of Different Network Topologies**

The optimal network topology for an organization depends on its size, budget, and needs. Here are some examples of where different topologies may be suitable:

* **Bus topology**  
  Suitable for small networks where ease of installation and low cost are significant factors. Used in old Ethernet networks.
* **Ring topology**  
  Useful for applications where data integrity and determinism are crucial such as token-based networks. Used in FDDI (Fiber Distributed Data Interface) networks.
* **Mesh topology**  
  Implemented where availability and bandwidth are critical as in air traffic control systems. Used in mobile ad hoc networks (MANETs) and wireless mesh networks.
* **Star topology**  
  Well suited for most modern Ethernet LANs where ease of installation and management are important. Used in most common office networks and Wi-Fi networks.
* **Tree topology**  
  Appropriate where a bus network needs to be expanded while still maintaining a bus structure. Used to some extent in modern Ethernet networks.
* **Hybrid topology**  
  Suitable for large, complex networks where high performance and availability are essential. Used in some wide area networks (WANs) and backbone networks.

## **Applications of Different Network Topologies**

The type of network topology used depends on the application and use case. Some examples of where different topologies are applied:

* **Bus topology**  
   Bus topology is best suited for small, simple networks with limited nodes. The simplicity and low cost of bus topology make it useful for basic networks where high performance and availability are not major concerns.
  + Simple network for small organizations
  + Classic Ethernet networks
  + Low-cost networks where performance is not critical
* **Ring topology**  
  Ring topology is traditionally used in token-based networks such as FDDI (Fiber Distributed Data Interface) networks where determinism and reliability are important. The circular configuration provides redundancy and fault tolerance for specific types of applications.
  + Token Ring networks
  + FDDI networks
  + Circular networks with high-reliability requirements
* **Mesh topology**  
  Mesh topology is used in applications where network availability and bandwidth are crucial such as real-time mobile ad hoc networks and high-performance computing. The mesh configuration with multiple redundant connections provides fault tolerance and increased performance.
  + Mobile ad hoc networks (MANETs)
  + High performance computing clusters
  + Wireless mesh networks
  + Networks where availability and high bandwidth are critical
* **Star topology**  
  Star topology is popular for small to mid-size organizations because it is simple to set up, cost-effective and meets basic connectivity needs. Variations of star topology are used in most common wired and wireless networks including [Ethernet](https://intellipaat.com/blog/what-is-ethernet/) and Wi-Fi networks.
  + Most common modern Ethernet networks
  + Wireless networks (Wi-Fi)
  + Simple networks with limited nodes
* **Tree topology**  
  Tree topology is used to some extent in modern Ethernet networks to expand star topologies while retaining a basic bus configuration. It provides more fault tolerance than a star while being simpler than a mesh topology.
  + Expansion of Ethernet-based star topologies
  + Networks that require a simple bus structure with some fault tolerance
* **Hybrid topology**  
  Hybrid topology is suitable for demanding enterprise networks where a combination of multiple topologies is needed to meet goals for performance, availability, reliability and cost. The mix of topologies provides flexibility, scalability and redundancy for mission-critical networking.
  + Backbone networks requiring very high availability
  + Complex networks where flexibility and performance are essential
  + Large enterprise networks

### OSI Model

The OSI (Open Systems Interconnection) model is a conceptual framework for understanding how computer networks work. It is composed of seven layers, each of which serves a specific purpose in the communication process.

### 7. Application layer

The application layer is the topmost layer in the OSI model. The layer establishes communication between the application on the network and the end user using it by defining the protocols for successful user interaction. An excellent example of this layer is that of web browsers.

Application layer protocols allow the software to direct data flow and present it to the user. Some of the known protocols include Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and[File Transfer Protocol (FTP)](https://www.spiceworks.com/tech/networking/articles/what-is-ftp/).

**Key functions:**

* The application layer provides user interfaces (UI) that are key to user interaction
* Supports a variety of applications such as e-mail and remote file transfer

In summary, layer 7 ensures effective communication between applications on different computing systems and networks.

### 6. Presentation layer

The presentation layer is often referred to as a syntax or translation layer as it translates the application data into a network format. This layer also encrypts and decrypts data before transmitting it over the network. For instance, layer 6 encrypts data from the application and decrypts it at the recipient’s end, ensuring secure data transmission. Moreover, this layer is known to compress data received from layer 7 to reduce the overall size of the data transferred.

**Key functions:**

* Performs data translation based on the application’s data semantics
* Encrypts and decrypts sensitive data transferred over communication channels
* Performs data compression to reduce the number of bits in exchanged data

In summary, layer 6 ensures that the communicated information is in the desired format as required by the receiving application.

### 5. Session layer

The session layer establishes a communication session between communicating entities. The session is maintained at a sufficient time interval to ensure efficient data transmission and avoid wasting computing resources.

This OSI layer is also responsible for data synchronization to maintain smooth data flow. This implies that in situations where large volumes of data are sent at once, layer 5 can break down the data into smaller chunks by adding checkpoints.

For example, let’s say you want to send a 500-page document to another person. In this case, this layer can add checkpoints at 50 or 100 pages. This is in case a document transfer is interrupted due to network or system failure. Once the system failure issue is resolved, the document transfer resumes from the last checkpoint. Such a system saves time by not restarting the file transfer from the beginning.

**Key functions:**

* Opens maintains, and closes communication sessions
* Enables data synchronization by adding checkpoints to data streams

In summary, layer 5 establishes, maintains, synchronizes, and terminates sessions between end-user applications.

### 4. Transport layer

The transport layer allows safe message transfer between the sender and the receiver. It divides the data received from the layer above into smaller segments. It also reassembles the data at the receiver side to allow the session layer to read it.

Layer 4 performs two critical functions: flow control and error control. Flow control implies regulating data transfer speeds. It ensures that the communicating device with a good network connection does not send data at higher rates, which is difficult for devices with slower connections to handle. Error control refers to the error-checking functionality to ensure the completeness of data. In incomplete data cases, this layer requests the system to resend the incomplete data.

Examples of transport layer protocols include[transmission control protocol (TCP) and user datagram protocol (UDP)](https://www.spiceworks.com/tech/networking/articles/tcp-vs-udp/).

**Key functions:**

* Ensures completeness of each message exchanged between source and destination
* Maintains proper data transmission through flow control and error control
* Performs data segmentation and reassembling of data

In summary, layer 4 is responsible for transmitting an entire message from a sender application to a receiver application.

### 3. Network layer

The network layer enables the communication between multiple networks. It receives data segments from the layer above, further broken down into smaller packets at the sender side. On the receiver side, this layer reassembles the data together.

The network layer also handles routing functionality, wherein the data transmission is accomplished by choosing the best possible route or path that connects different networks and ensures efficient data transfer. This network layer uses[internet protocol (IP)](https://www.spiceworks.com/tech/networking/articles/what-is-ipv6/) for data delivery.

**Key functions:**

* Handles routing to recognize suitable routes from sender to receiver
* Performs logical addressing that assigns unique names to each device operating over the network

In summary, layer 3 is responsible for dividing segmented data into network packets, reassembling them at the recipient’s side, and identifying the shortest yet most suitable and secure path for transmitting data packets.

### 2. Data link layer

The data link layer transmits data between two nodes that are directly connected or are operating over the same network architecture. Typically, this layer takes data packets from layer 3 and breaks them down into frames before sending them to the destination.

Layer 2 is divided into two sub-layers: media access control (MAC) and logical link control (LLC). The MAC layer encapsulates data frames transmitted through the network connecting media such as wires or cables. In situations where such data transmission fails, LLC helps manage packet retransmission.

The well-known data link layer protocol includes the Address Resolution Protocol (ARP) that translates IP addresses to MAC addresses to establish communication between systems whose addresses vary in bit length (32 bits vs. 48 bits).

**Key functions:**

* Detects damaged or lost frames and retransmits them
* Performs framing where data received from layer 3 is further subdivided into smaller units called frames
* Updates headers of created frames by adding the MAC address of the sending device and receiving device

In summary, layer 2 is responsible for setting up and terminating physical connections between participating network nodes.

### 1. Physical layer

The last OSI layer is the physical layer that manages physical hardware and network components such as cables, switches, or routers that transmit data.

In the context of data, layer 1 transmits data in the form of ones and zeros. Technically, this layer picks up bits from the sender end, encodes them into a signal, sends the signal over the network, and decodes the signal at the receiver end. Thus, without layer 1, communicating data bits across network devices through physical media is not possible.

**Key functions:**

* Synchronizes data bits
* Enables modulation (conversion of a signal from one form to another for data transmission)
* Defines data transmission rate (bits/sec)
* Outlines the arrangement of network devices across different[network topologies](https://www.spiceworks.com/tech/networking/articles/what-is-network-topology/) such as bus, tree, star, or mesh topology
* Defines transmission modes such as simple or half-duplex mode

In summary, layer 1 is responsible for transmitting data bits of 0s and 1s between network systems via electrical, mechanical, or procedural interfaces.

### TCP/IP Model

The TCP/IP (Transmission Control Protocol/Internet Protocol) model is a widely used networking model that provides a framework for communication over the internet. It is composed of four layers, each with its own set of protocols and functions.

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.

## What is the Difference between TCP and IP?

[TCP](https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp/) and[IP](https://www.geeksforgeeks.org/what-is-an-ip-address/) are different protocols of Computer Networks. The basic difference between TCP (Transmission Control Protocol) and IP (Internet Protocol) is in the transmission of data. In simple words, IP finds the destination of the mail and TCP has the work to send and receive the mail. UDP is another protocol, which does not require IP to communicate with another computer. IP is required by only TCP. This is the basic difference between TCP and IP.

## How Does the TCP/IP Model Work?

Whenever we want to send something over the internet using the TCP/IP Model, the TCP/IP Model divides the data into packets at the sender’s end and the same packets have to be recombined at the receiver’s end to form the same data, and this thing happens to maintain the accuracy of the data. TCP/IP model divides the data into a 4-layer procedure, where the data first go into this layer in one order and again in reverse order to get organized in the same way at the receiver’s end.

For more, you can refer to [TCP/IP in Computer Networking](https://www.geeksforgeeks.org/tcp-ip-in-computer-networking/).

## Layers of TCP/IP Model

1. Application Layer
2. [Transport Layer(TCP/UDP)](https://www.geeksforgeeks.org/tcp-and-udp-in-transport-layer/)
3. Network/Internet Layer(IP)
4. [Data Link Layer (MAC)](https://www.geeksforgeeks.org/data-link-layer/)
5. Physical Layer

### ****1. Physical 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.

### 2. Data Link Layer

The packet’s network protocol type, in this case, TCP/IP, is identified by the data-link layer. Error prevention and “framing” are also provided by the data-link 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.

### 3. 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.

### 4. 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.

### 5. 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.

The host-to-host layer is a layer in the OSI (Open Systems Interconnection) model that is responsible for providing communication between hosts (computers or other devices) on a network. It is also known as the transport layer.

Some common use cases for the host-to-host layer include:

1. **Reliable Data Transfer:** The host-to-host layer ensures that data is transferred reliably between hosts by using techniques like error correction and flow control. For example, if a packet of data is lost during transmission, the host-to-host layer can request that the packet be retransmitted to ensure that all data is received correctly.
2. **Segmentation and Reassembly:** The host-to-host layer is responsible for breaking up large blocks of data into smaller segments that can be transmitted over the network, and then reassembling the data at the destination. This allows data to be transmitted more efficiently and helps to avoid overloading the network.
3. **Multiplexing and Demultiplexing:** The host-to-host layer is responsible for multiplexing data from multiple sources onto a single network connection, and then demultiplexing the data at the destination. This allows multiple devices to share the same network connection and helps to improve the utilization of the network.
4. **End-to-End Communication:** The host-to-host layer provides a connection-oriented service that allows hosts to communicate with each other end-to-end, without the need for intermediate devices to be involved in the communication.

**Example:** Consider a network with two hosts, A and B. Host A wants to send a file to host B. The host-to-host layer in host A will break the file into smaller segments, add error correction and flow control information, and then transmit the segments over the network to host B. The host-to-host layer in host B will receive the segments, check for errors, and reassemble the file. Once the file has been transferred successfully, the host-to-host layer in host B will acknowledge receipt of the file to host A.

In this example, the host-to-host layer is responsible for providing a reliable connection between host A and host B, breaking the file into smaller segments, and reassembling the segments at the destination. It is also responsible for multiplexing and demultiplexing the data and providing end-to-end communication between the two hosts.

## Other Common Internet Protocols

TCP/IP Model covers many Internet Protocols. The main rule of these Internet Protocols is how the data is validated and sent over the Internet. Some Common Internet Protocols include:

* **HTTP (Hypertext Transfer Protocol):**[HTTP](https://www.geeksforgeeks.org/http-full-form/) takes care of Web Browsers and Websites.
* **FTP (File Transfer Protocol):**[FTP](https://www.geeksforgeeks.org/file-transfer-protocol-ftp-in-application-layer/) takes care of how the file is to be sent over the Internet.
* **SMTP (Simple Mail Transfer Protocol):**[SMTP](https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp/) is used to send and receive data.

## Difference between TCP/IP and OSI Model

| **TCP/IP** | **OSI** |
| --- | --- |
| TCP refers to Transmission Control Protocol. | OSI refers to Open Systems Interconnection. |
| TCP/IP uses both the session and presentation layer in the application layer itself. | OSI uses different session and presentation layers. |
| TCP/IP follows connectionless a horizontal approach. | OSI follows a vertical approach. |
| The Transport layer in TCP/IP does not provide assurance delivery of packets. | In the OSI model, the transport layer provides assurance delivery of packets. |
| Protocols cannot be replaced easily in TCP/IP model. | While in the OSI model, Protocols are better covered and are easy to replace with the technology change. |
| TCP/IP model network layer only provides connectionless (IP) services. The transport layer (TCP) provides connections. | Connectionless and connection-oriented services are provided by the network layer in the OSI model. |

### Network Devices

These are physical devices that allow hardware on a computer network to communicate and interact with one another. Example: Hub, Switch, Router, etc.

Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

**1. Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

**2. Hub** – A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.  In other words, the [collision domain](https://en.wikipedia.org/wiki/Collision_domain) of all hosts connected through Hub remains one.  Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

**Types of Hub**

* **Active Hub:-**These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring centre. These are used to extend the maximum distance between nodes.
* **Passive Hub:-**These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.
* **Intelligent Hub:-**It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

**3. Bridge** – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

**Types of Bridges**

* **Transparent Bridges:-**These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
* **Source Routing Bridges:-**In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

**4. Switch** – A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.  In other words, the switch divides the collision domain of hosts, but the [broadcast domain](https://en.wikipedia.org/wiki/Broadcast_domain) remains the same.

#### **Types of Switch**

1. Unmanaged switches: These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.
2. Managed switches: These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.
3. Smart switches: These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.
4. Layer 2 switches: These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.
5. Layer 3 switches: These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.
6. PoE switches: These switches have Power over Ethernet capabilities, which allows them to supply power to network devices over the same cable that carries data.
7. Gigabit switches: These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.
8. Rack-mounted switches: These switches are designed to be mounted in a server rack and are suitable for use in data centers or other large networks.
9. Desktop switches: These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.
10. Modular switches: These switches have modular design, which allows for easy expansion or customization. They are suitable for large networks and data centers.

**5. Routers** – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

**6. Gateway** – A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.

**7. Brouter** – It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks and working as the bridge, it is capable of filtering local area network traffic.

**8. NIC**– NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN.  It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

### Network Protocols

Network protocols define how data is transmitted, received, and processed between devices. They are essential for ensuring that devices can communicate with each other.

### Wireless Networks

A wireless network is a type of computer network that uses radio waves instead of physical cables to connect devices. Wireless networks are commonly used for internet access, as well as for sharing files, printers, and other resources between devices.