UNIT-1

What is a Computer Network?

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

Components Of Computer Network:

Major components of a computer network are:

NIC(National interface card)

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

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

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

Hub

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

Switches

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

Cables and connectors

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

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

Router

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

Modem

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

Uses Of Computer Network

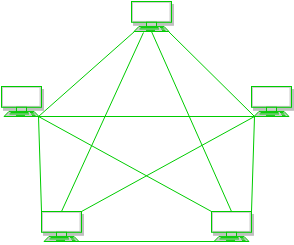
* **Resource sharing:** Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
* **Server-Client model:** Computer networking is used in the **server-client model**. A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

Network Topology

The arrangement of a network which comprises of nodes and connecting lines via sender and receiver is referred as network topology. The various network topologies are :

**a) Mesh Topology :**

In mesh topology, every device is connected to another device via particular channel.



**Figure 1** : Every device is connected with another via dedicated channels. These channels are known as links.

* If suppose, N number of devices are connected with each other in mesh topology, then total number of ports that is required by each device is ​ N-1. In the Figure 1, there are 5 devices connected to each other, hence total number of ports required is 4.
* If suppose, N number of devices are connected with each other in mesh topology, then total number of dedicated links required to connect them is NC2 i.e. N(N-1)/2. In the Figure 1, there are 5 devices connected to each other, hence total number of links required is 5\*4/2 = 10.

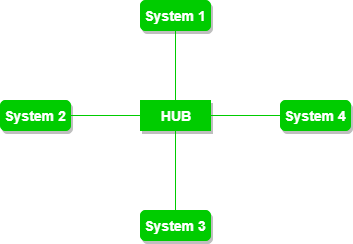
**Advantages of this topology :**

* It is robust.
* Fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
* Provides security and privacy.

**Problems with this topology :**

* Installation and configuration is difficult.
* Cost of cables are high as bulk wiring is required, hence suitable for less number of devices.
* Cost of maintenance is high.

**b) Star Topology :**

****

​ In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node. The hub can be passive ​in nature i.e. not intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as active ​hubs. Active hubs have repeaters in them.

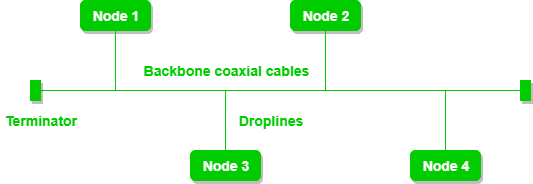
**Advantages of this topology :**

* If N devices are connected to each other in star topology, then the number of cables required to connect them is N. So, it is easy to set up.
* Each device require only 1 port i.e. to connect to the hub.

**Problems with this topology :**

* If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
* Cost of installation is high.
* Performance is based on the single concentrator i.e. hub.

**c) Bus Topology :**

****

​ Bus topology is a network type in which every computer and network device is connected to single cable. It transmits the data from one end to another in single direction. No bi-directional feature is in bus topology.

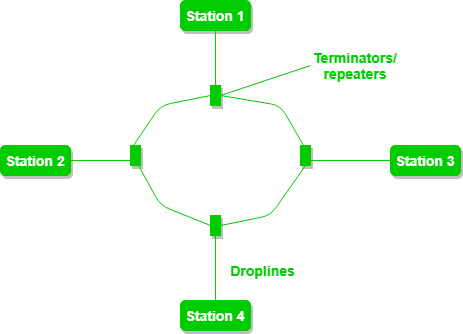
**Advantages of this topology :**

* If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1 ​which is known as backbone cable and N drop lines are required.
* Cost of the cable is less as compared to other topology, but it is used to built small networks.

**Problems with this topology :**

* If the common cable fails, then the whole system will crash down.
* If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD etc.

**d) Ring Topology :** In this topology, it forms a ring connecting a devices with its exactly two neighbouring devices.

  
  
The following operations takes place in ring topology are :

1. One station is known as **monitor** station which takes all the responsibility to perform the operations.
2. To transmit the data, station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques : **Early token release** releases the token just after the transmitting the data and **Delay token release** releases the token after the acknowledgement is received from the receiver.

**Advantages of this topology :**

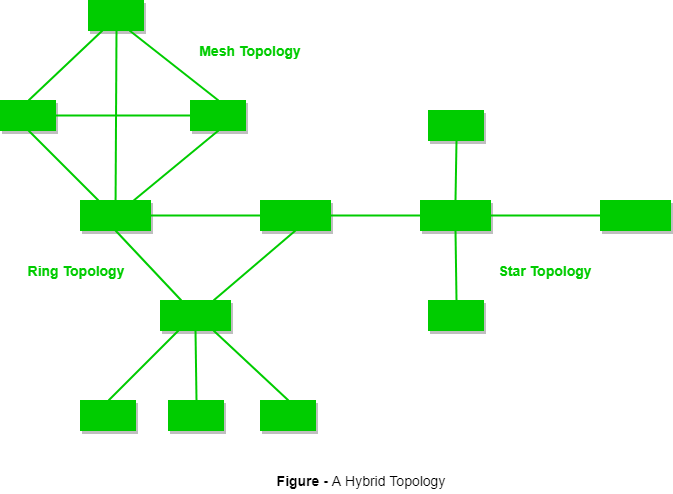
* The possibility of collision is minimum in this type of topology.
* Cheap to install and expand.

**Problems with this topology :**

* Troubleshooting is difficult in this topology.
* Addition of stations in between or removal of stations can disturb the whole topology.

**e) Hybrid Topology :**

​This topology is a collection of two or more topologies which are described above. This is a scalable topology which can be expanded easily. It is reliable one but at the same it is a costly topology.



**Network protocols**

Network protocols are sets of established rules that dictate how to format, transmit and receive [data](https://searchdatamanagement.techtarget.com/definition/data) so computer network devices -- from [servers](https://whatis.techtarget.com/definition/server) and routers to [endpoints](https://whatis.techtarget.com/definition/endpoint-device) -- can communicate regardless of the differences in their underlying infrastructures, designs or standards.To successfully send and receive information, devices on both sides of a communication exchange must accept and follow protocol conventions. Support for network protocols can be built into software, hardware or both.

Standardized network protocols provide a common language for network devices. Without them, computers wouldn't know how to engage with each other. As a result, except for specialty networks built around a specific architecture, few networks would be able to function, and the internet as we know it wouldn't exist. Virtually all network end users rely on network protocols for connectivity.

**Types of protocols**

Networks have three types of protocols -- communication, such as [Ethernet](https://searchnetworking.techtarget.com/definition/Ethernet); management, such as the Simple Mail Transfer Protocol ([SMTP](https://whatis.techtarget.com/definition/SMTP-Simple-Mail-Transfer-Protocol)); and security, such as Secure Shell ([SSH](https://searchsecurity.techtarget.com/definition/Secure-Shell)).

Falling into these three broad categories are thousands of network protocols that uniformly handle an extensive variety of defined tasks, including [authentication](https://searchsecurity.techtarget.com/definition/authentication), [automation](https://searchnetworking.techtarget.com/definition/network-automation), correction, [compression](https://searchstorage.techtarget.com/definition/compression), [error handling](https://searchsoftwarequality.techtarget.com/definition/error-handling), file retrieval, [file transfer](https://searchnetworking.techtarget.com/definition/file-transfer), link [aggregation](https://whatis.techtarget.com/definition/aggregate), routing, [semantics](https://whatis.techtarget.com/definition/semantics), synchronization and [syntax](https://whatis.techtarget.com/definition/syntax).

**IP: Internet Protocol**  
The Internet Protocol is where it all begins. IP is responsible for basic networking. The core of the IP protocol works with Internet addresses and every computer on a TCP/ IP network must have a numeric address.

**FTP: File Transfer Protocol**  
Where would be without FTP? The oldest (its 42 years old this year!) and frankly the best known of all protocols outside of IP. The original specification for FTP was compiled by [Abhay Bhushan](https://dora.iitk.ac.in/dora/abhay-bhushan-profile) and published April 16th, 1971. There have been many updates including the very latest which allows the protocol to support

**SSH: Secure Shell**  
SSH and FTP are often mentioned in the same breath. Invented in 1995 Secure Shell’s definition is “a cryptographic network protocol for secure data communication”. SSH allows for remote command-line login and remote execution. It has many of the functions of FTP but is more secure. The latest versions are referred to as SSH-1 and SSH-2.

**SSL: Secure Sockets Layer**  
SSL allows security by allowing applications to encrypt data that go from a client to a matching server (for example).

**TELNET (telnet)**  
The telnet (written in small caps) lets you connect to a remote computer and work as if you were sitting in front of your computer, no matter how far away you are. This is another old technology, first invented in 1969. By default, telnet does not encrypt data sent over the network so use with caution!

**SMTP: Simple Mail Transfer Protocol**  
The Simple Mail Transfer Protocol is the protocol for Internet email. It transfers email amongst computers. The majority of computers in the wild understand SMTP, but some do not.

**POP3: Post Office Protocol**  
The [Post Office Protocol](https://www.techopedia.com/definition/5383/post-office-protocol-pop) (latest version is ‘3’) provides basic client/ server features that help the user download email from a POP3 email server to a computer (be it mobile or a desktop). The main purpose of the protocol is to allow users to access their email more freely.

**HTTP: Hyper Text Transfer Protocol**  
OK, if you don’t know this one then we really recommend you start your training from the basics! HTTP is the key protocol for being able to transfer data across the Internet. HTTP allows the transfer of HyperText Markup Language (HTML) and other related scripting languages (like CSS) to travel from servers to browsers.

**HTTPS: Hypertext Transfer Protocol Secure**  
Think of HTTPS and a secure version of HTTP. The Hypertext Transfer Protocol Secure (HTTPS) protocol facilitates secure communication over a network. Strictly speaking, HTTPS is a layer on top of HTTP using SSL (see above).

**SIP: Session Initiation Protocol**  
We wanted to include SIP as our tenth protocol owing to an excellent Hacker Hotshot session we had recently titled: “Learn How To Crack SIP Authentication & Listen To VoIP Calls In 15-Minutes!”.

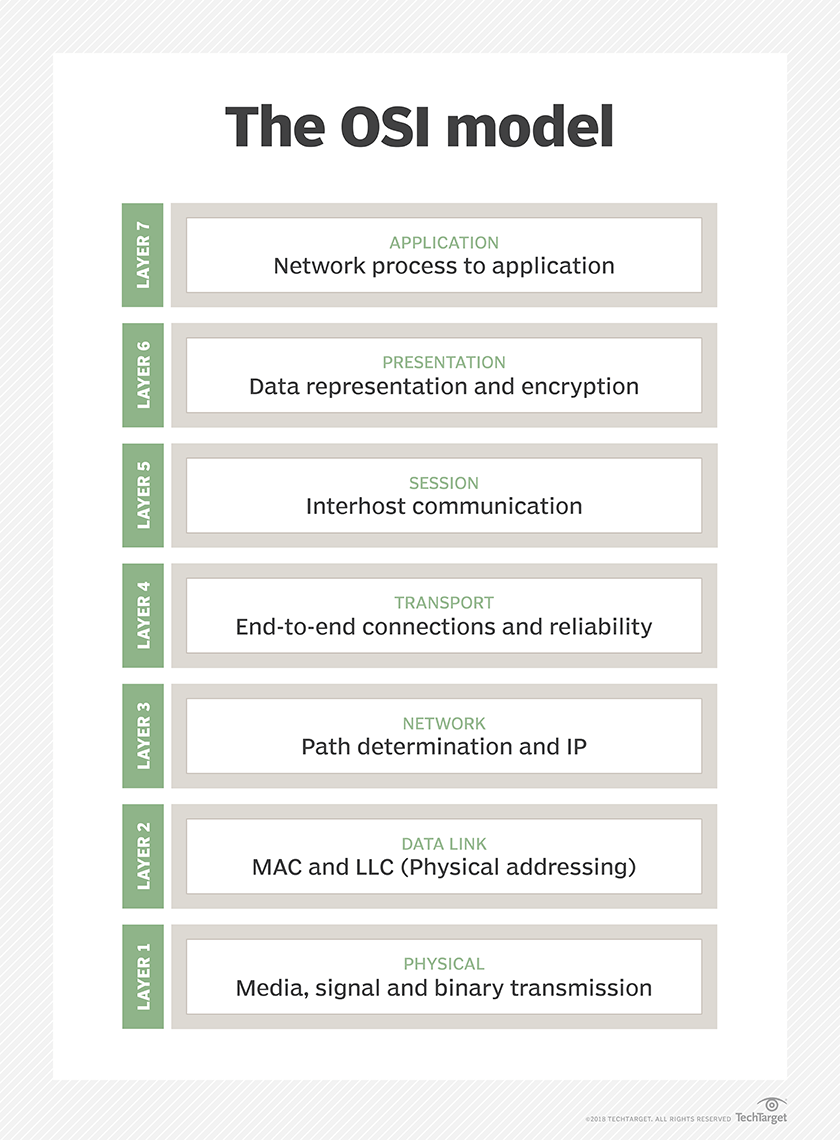
**OSI model (Open Systems Interconnection)**

OSI (Open Systems Interconnection) is a reference model for how applications communicate over a [network](https://searchnetworking.techtarget.com/definition/network). A reference model is a conceptual framework for understanding relationships. The purpose of the OSI reference model is to guide vendors and developers so the digital communication products and software programs they create can [interoperate](https://searchmicroservices.techtarget.com/definition/interoperability), and to facilitate a clear framework that describes the functions of a networking or telecommunication system. Most vendors involved in telecommunications make an attempt to describe their products and services in relation to the OSI model. And although it is useful for guiding discussion and evaluation, OSI is rarely actually implemented as-is. That's because few network products or standard tools keep related functions together in well-defined layers, as is the case in the OSI model. The [TCP/IP](https://searchnetworking.techtarget.com/definition/TCP-IP) protocol suite, which defines the internet, does not map cleanly to the OSI model.

### History of the OSI model

Developed by representatives of major computer and telecommunication companies beginning in 1983, OSI was originally intended to be a detailed specification of actual [interfaces](https://whatis.techtarget.com/definition/interface). Instead, the committee decided to establish a common reference model that others could then use to develop detailed interfaces, which, in turn, could become [standards](https://whatis.techtarget.com/definition/standard) governing the transmission of data packets. The OSI architecture was officially adopted as an international standard by the International Organization for Standardization ([ISO](https://searchdatacenter.techtarget.com/definition/ISO)) in 1984.

### How the OSI model works



IT professionals use OSI to model or trace how data is sent or received over a network. This model breaks down data transmission over a series of seven layers, each of which is responsible for performing specific tasks concerning sending and receiving data.

The main concept of OSI is that the process of communication between two endpoints in a network can be divided into seven distinct groups of related functions, or layers. Each communicating user or program is on a device that can provide those seven layers of function.

In this architecture, each layer serves the layer above it and, in turn, is served by the layer below it. So, in a given message between users, there will be a flow of data down through the layers in the source computer, across the network, and then up through the layers in the receiving computer. Only the application layer, at the top of the stack, doesn’t provide services to a higher-level layer.

The seven layers of function are provided by a combination of applications, [operating systems](https://whatis.techtarget.com/definition/operating-system-OS), network card device drivers and networking hardware that enable a system to transmit a signal over a network Ethernet or fiber optic cable or through [Wi-Fi](https://searchmobilecomputing.techtarget.com/definition/Wi-Fi) or other [wireless protocols](https://searchmobilecomputing.techtarget.com/definition/IEEE-802-Wireless-Standards-Fast-Reference).

**7 layers of the OSI model**

The seven Open Systems Interconnection layers are:

* 1. [Layer 7: The application layer](https://searchnetworking.techtarget.com/definition/Application-layer): Enables the user (human or software) to interact with the application or network whenever the user elects to read messages, transfer files or perform other network-related activities. Web browsers and other internet-connected apps, such as Outlook and Skype, use Layer 7 application protocols.
  2. [Layer 6: The presentation layer](https://searchnetworking.techtarget.com/definition/presentation-layer): Translates or formats data for the application layer based on the semantics or syntax that the application accepts. This layer is also able to handle the encryption and decryption that the application layer requires.
  3. [Layer 5: The session layer](https://searchnetworking.techtarget.com/definition/Session-layer): Sets up, coordinates and terminates conversations between applications. Its services include authentication and reconnection after an interruption. This layer determines how long a system will wait for another application to respond. Examples of session layer protocols include [X.225](https://whatis.techtarget.com/definition/ITU-X225), AppleTalk and Zone Information Protocol (ZIP).
  4. [Layer 4: The transport layer](https://searchnetworking.techtarget.com/definition/Transport-layer): Is responsible for transferring data across a network and provides error-checking mechanisms and data flow controls. It determines how much data to send, where it gets sent and at what rate. The Transmission Control Protocol is the best known example of the transport layer.
  5. [Layer 3: The network layer](https://searchnetworking.techtarget.com/definition/Network-layer): Primary function is to move data into and through other networks. Network layer protocols accomplish this by packaging data with correct network address information, selecting the appropriate network routes and forwarding the packaged data up the stack to the transport layer.
  6. [Layer 2: The data-link layer](https://searchnetworking.techtarget.com/definition/Data-Link-layer): The [protocol layer](https://searchnetworking.techtarget.com/definition/protocol) in a program that handles the moving of data into and out of a physical link in a network. This layer handles problems that occur as a result of bit transmission errors. It ensures that the pace of the data flow doesn’t overwhelm the sending and receiving devices. This layer also permits the transmission of data to Layer 3, the [network layer](https://searchnetworking.techtarget.com/definition/Network-layer), where it is addressed and routed.
  7. [Layer 1: The physical layer](https://searchnetworking.techtarget.com/definition/physical-layer): Transports data using electrical, mechanical or procedural interfaces. This layer is responsible for sending computer bits from one device to another along the network. It determines how physical connections to the network are set up and how bits are represented into predictable signals as they are transmitted either electrically, optically or via radio waves.

[**TCP/IP**](https://searchnetworking.techtarget.com/definition/TCP-IP)**suite**

A set of cooperating network protocols is called a protocol suite. The [TCP/IP](https://searchnetworking.techtarget.com/definition/TCP-IP) suite includes numerous protocols across layers -- such as the data, network, transport and application layers -- working together to enable internet connectivity. These include:

* Transmission Control Protocol ([TCP](https://searchnetworking.techtarget.com/definition/TCP)), which uses a set of rules to exchange messages with other internet points at the information packet level;
* User Datagram Protocol ([UDP](https://searchnetworking.techtarget.com/definition/UDP-User-Datagram-Protocol)), which acts as an alternative communication protocol to TCP and is used to establish low-[latency](https://whatis.techtarget.com/definition/latency) and loss-tolerating connections between applications and the Internet.
* Internet Protocol ([IP](https://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol)), which uses a set of rules to send and receive messages at the Internet address level; and
* additional network protocols that include the Hypertext Transfer Protocol ([HTTP](https://searchwindevelopment.techtarget.com/definition/HTTP)) and File Transfer Protocol ([FTP](https://searchenterprisewan.techtarget.com/definition/File-Transfer-Protocol)), each of which has defined sets of rules to exchange and display information.

Every packet transmitted and received over a network contains [binary](https://whatis.techtarget.com/definition/binary) data. Most protocols will add a header at the beginning of each packed in order to store information about the sender and the message's intended destination. Some protocols may also include a footer at the end with additional information. Network protocols process these headers and footers as part of the data moving among devices in order to identify messages of their own kind.

Network protocols are often set forth in an industry standard -- developed, defined and published by groups such as: