**What is a Computer Network?**

"A Computer Network is defined as a set of two or more computers that are linked together?either via wired cables or wireless networks i.e., WiFi?with the purpose of communicating, exchanging, sharing or distributing data, files and resources."

Computer Networks are built using a collection of hardware (such as **routers, switches, hubs, and so forth)** and networking software (such as **operating systems, firewalls, or corporate applications).**

Though one can also define the computer networks based on their geographic location, a **LAN (local area network)** connects computers in a definite physical dimension, such as **home or within an office.**

In contrast, a **MAN (Metropolitan area network)** connects computers ranging between multiple buildings in a city.

The **Internet** is the most significant example of **WAN (Wide Area Network),** connecting billions of networking devices across the world.

One can also describe the concept of computer networking by its communicating protocols, the physical arrangement of its networking elements, how it manages network traffic, and it's functioning.

Computer networks are globally used by businesses, the entertainment industry, education in the research field for communication and transferring their data from source to destination node.

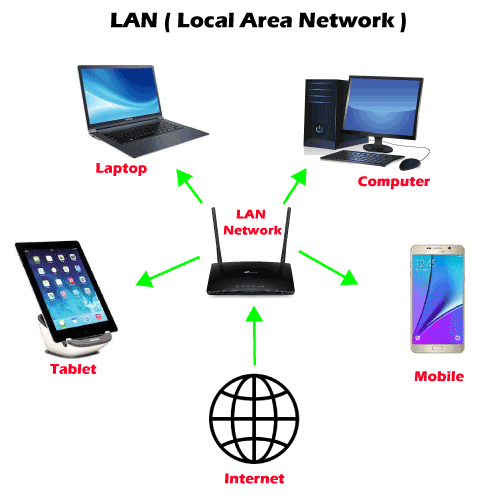
All the other technologies, including the **internet, Google search, instant messaging apps, online video streaming, social media, email, cloud kitchen, cloud data storage,** etc., all exist because of computer networks.

## **Computer Network Types**

Below are the most common computer network types that are frequently used these days:

* **LAN [Local Area Network}**
* **WLAN [Wireless local area network]**
* **CAN [Campus Area Network]**
* **MAN [Metropolitan Area Network]**
* **PAN [Personal Area Network]**
* **SAN [Storage Area Network]**
* **VPN [Virtual Private Network]**
* **WAN [ Wide Area Network]**

### **1. LAN**



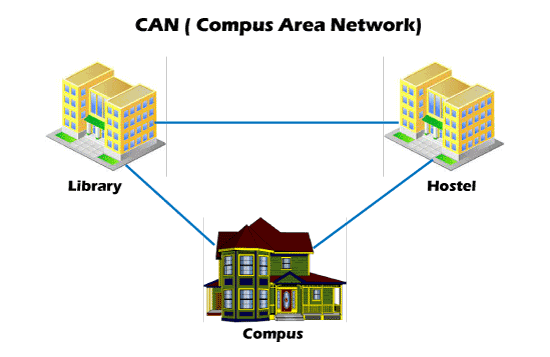
**LAN or Local Area Network** is a group of devices connecting the computers and other devices such as **switches, servers, printers,** etc., over a short distance such as office, home. The commonly used LAN is **Ethernet LAN.** This network is used as it allows the user to transfer or share data, files, and resources.

### **2. WLAN**



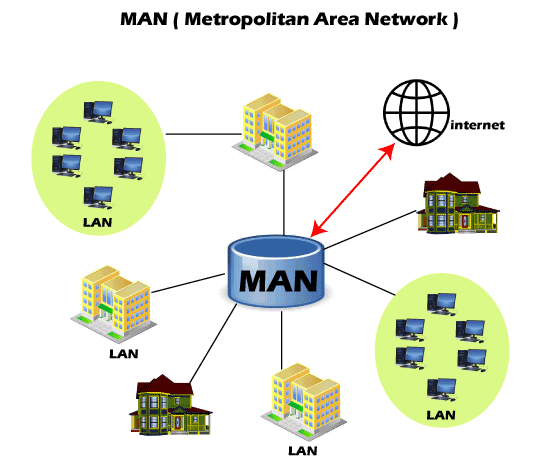
**WLAN or Wireless local area network** is similar to LAN with the difference that it uses wireless communication between devices instead of wired connections. WLAN typically involves a **Wi-Fi router or wireless access point for devices,** unlike **smartphones, laptops, desktops,** etc.

### **3. CAN**



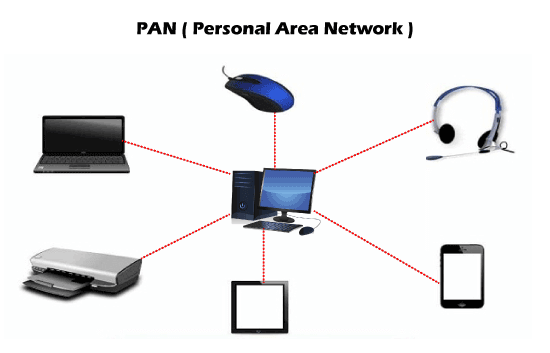
**CAN or Campus Area Network** is a closed corporate communication network. A CAN is a mobile network that may contain a private or public part. CANs are widely used **colleges, academies, and corporate sites.**

### **4. MAN**



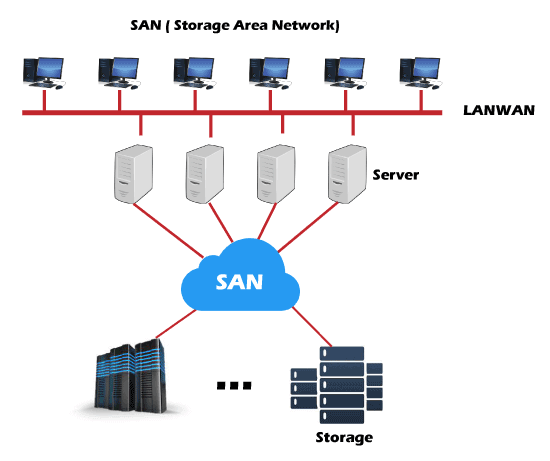
**MAN or Metropolitan Area Network** is typically a more extensive network when compared to LANs but is smaller than WANs. This network ranges between several buildings in the same city. Man networks are connected via fiber optic cable (usually high-speed connection). Cities and government bodies usually manage MANs.

### **5. PAN**



**PAN or Personal Area Network** is a type of network used personally and usually serves one person. This network usually connects devices unlike your smartphones, laptop, or desktop to sync content and share small files, unlike songs, photos, videos, calendars, etc. These devices connect via **wireless networks such as Wi-Fi, Bluetooth, Infrared, etc.**

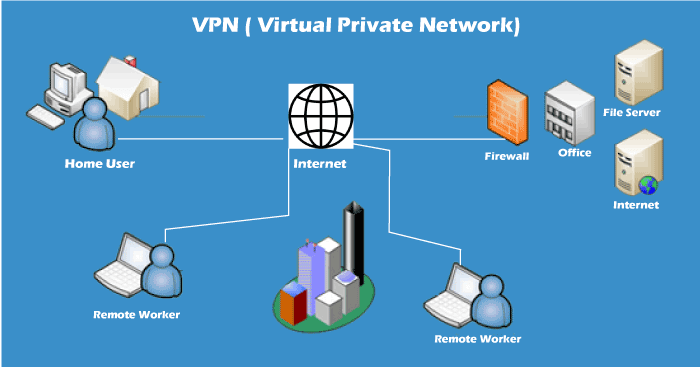
### **6. SAN**



**SAN or Storage Area Network** is a specialized high-speed network that stores and provides access to block-level storage. It is a dedicated shared network that is used for cloud data storage that appears and works like a storage drive.

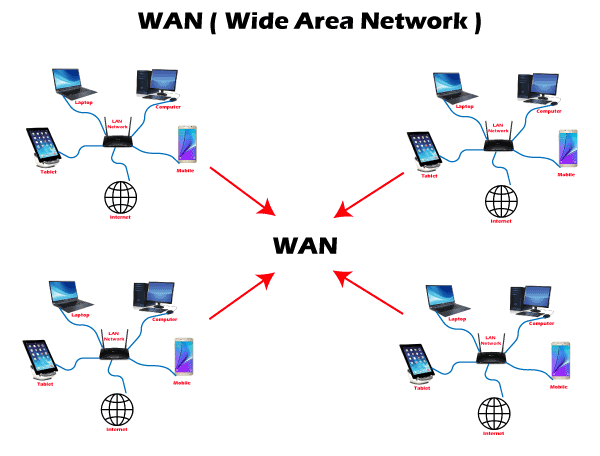
SAN consists of various **switches, servers, and disks array.** One of the advantages of SAN is that it is fault-tolerant, which means if any switch or server goes down, the data can still be accessed.

### **7. VPN**



**VPN or Virtual Private Network** is a secure tool that encrypts point-to-point Internet connection and hides the user's IP address and virtual location. It determines an encrypted network to boost user's online privacy so as their identity and data are inaccessible to hackers.

### **8. WAN**



**WAN or Wide Area Network** is the most significant network type connecting computers over a wide geographical area, such as a country, continent. WAN includes **several LANs, MANs, and CANs.** An example of WAN is the **Internet,** which connects billions of computers globally.

## **Computer Networks and the Internet**

The Internet is the major example of a WAN, which connects billions of computers globally. Internet follows standard protocols that facilitate communication between these network devices. Those protocols include:

1. **HTTP (Hypertext Transfer Protocol)**
2. **IP (Internet protocol or IP addresses)**
3. **TCP (Transmission Control Protocol)**
4. **UDP (User Datagram Protocol)**
5. **FTP (File Transfer Protocol)**

**ISPs (Internet Service Providers) NSPs (Network Service Providers)** effectively support the internet infrastructure. The infrastructure allows the transportation of data packets to the recipient device over the Internet.

Internet is a giant hub of information, but this information is not sent to every computer connected to the Internet. The protocols and infrastructure are responsible for managing to share the precise information the user has requested.

## **How do they work?**

1. The **Computer networks are formed by connecting multiple nodes** such as computers, desktops, routers, hubs, and switches with the help of either wired cables (Ethernet, data cables, fiber optics) or wireless networks (Bluetooth, Wi-Fi). This network connection enables the nodes to communicate and exchange data over the network.
2. Networks **follow communication protocols to send, receive, create or forward data.** Each note connected with a network is allocated a unique IP (Internet Protocol), the IP address used to identify a device and enables the other devices to identify it.
3. **Routers and Switches are the virtual or physical medium that supports and manages the communications** between networks. Routers examine the data packets to conclude the best route, following which the data can easily reach its destination node. In contrast, Switches connect the devices if there are multiple routes in a more extensive network and facilitate node-to-node communication, ensuring that the data packets traveling across the network reach their destination node.

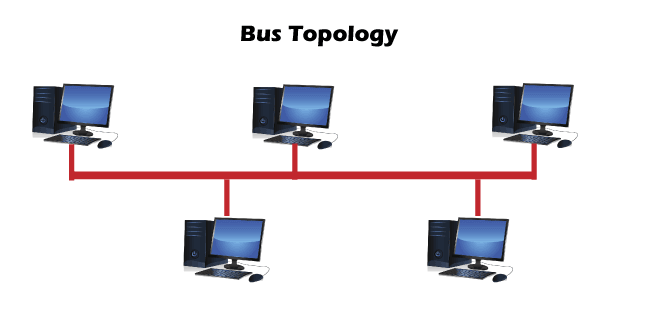
## **Network Topology**

**"Network topology is defined as the arrangement of computers or nodes of a computer network to establish communication among all."**

A node refers to a device that can transmit, receive, create, or store information. The nodes are connected via a network link that could be either wired (cables, Ethernet) or wireless (Bluetooth, Wi-Fi).

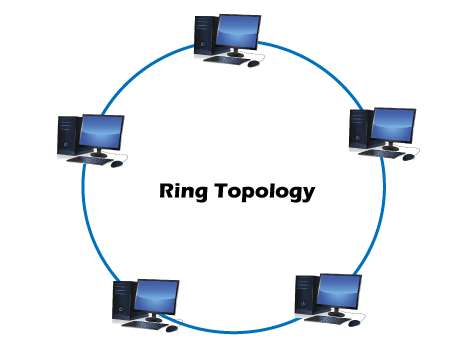
To help build a successful network in different situations, topologies are further classified into several types.  
Though there are several topologies but in this tutorial, we will discuss the commonly used ones, which are as follows:

### **1. Bus Topology**



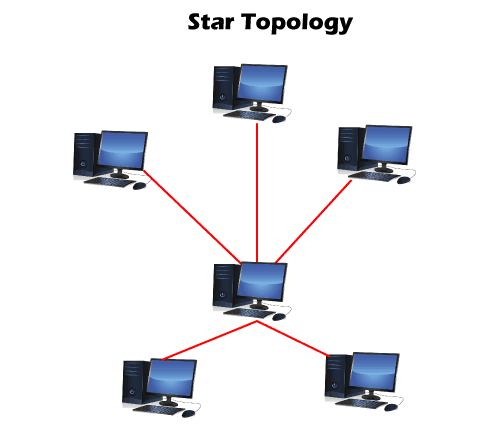
* A **Bus network topology** supports a common transmission medium where each node is directly connected with the main network cable.
* The data is transmitted through the main network cable and is received by all nodes simultaneously.
* A signal is generated through the source machine, which contains the address of the receiving machine. The signal travels in both the direction to all the nodes connected to the bus network until it reaches the destination node.
* Bus topology is not fault-tolerant and has a limited cable length.

### **2. Ring Topology**



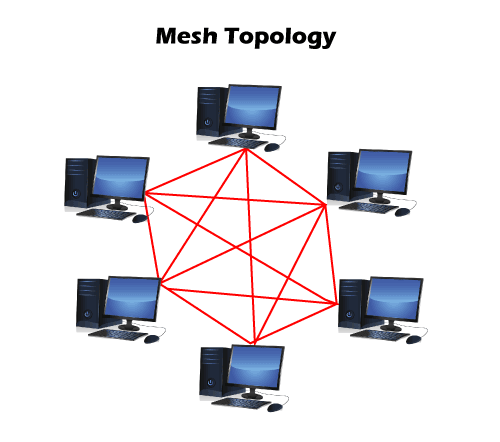
* A **Ring topology** is a modified version of bus topology where every node is connected in a closed-loop forming peer-to-peer LAN topology.
* Every node in a ring topology has precisely two connections. The Adjacent node pairs are connected directly, whereas the non-adjacent nodes are indirectly connected via various nodes.
* Ring topology supports a unidirectional communication pattern where sending and receiving of data occurs via **TOKEN.**

### **3. Star Topology**



* In a **Star network topology,** every node is connected using a single central hub or switch.
* The hub or switch performs the entire centralized administration. Each node sends its data to the hub, and later hub shares the received information to the destination device.
* Two or more-star topologies can be connected to each other with the help of a repeater.

### **4. Mesh Topology**



* In a **Mesh topology,** every node in the network connection is directly connected to one other forming overlapping connections between the nodes.
* This topology delivers better fault tolerance because if any network device fails, it won't affect the network, as other devices can transfer information.
* The Mesh networks self-configure and self-organize, finding the quickest, most secure way to transmit the data.
* One can form a full mesh topology by connecting every single node to another node in the network. **Full mesh** is expensive and is only used in the networks, which demands high data redundancy.
* Another type of mesh topology is **partial mesh topology,** where only a few devices are connected, and few are connected to the devices with which they share the most information. This mesh type is applicable in the networks, requiring less redundancy or a cost-effective network topology that is easy to execute.

Computer networking is the practice of connecting computers together to enable communication and data exchange between them.

Here are some basic concepts of computer networking:

**Network:**A network is a collection of computers and devices that are connected together to enable communication and data exchange.

**Nodes:**Nodes are devices that are connected to a network. These can include computers, servers, printers, routers, switches, and other devices.

**Protocol:**A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include TCP/IP, HTTP, and FTP.

**Topology:** Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include bus, star, ring, mesh, and tree.

**LAN:**A Local Area Network (LAN) is a network that covers a small area, such as an office or a home. LANs are typically used to connect computers and other devices within a building or a campus.

**WAN:**A Wide Area Network (WAN) is a network that covers a large geographic area, such as a city, country, or even the entire world. WANs are used to connect LANs together and are typically used for long-distance communication.

**IP Address**: An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.

**DNS:**The Domain Name System (DNS) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.

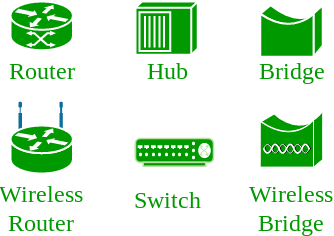
**Firewall:**A firewall is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.

These are just a few basic concepts of computer networking. Networking is a vast and complex field, and there are many more concepts and technologies involved in building and maintaining networks.

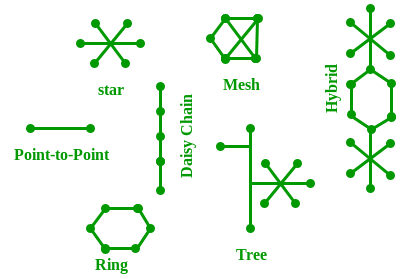
**Open system:** A system that is connected to the network and is ready for communication.

**Closed system:** A system that is not connected to the network and can’t be communicated with.

**Computer Network:**An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as **Network devices** and include things such as routers, switches, hubs, and bridges.



**Network Topology:**The layout arrangement of the different devices in a network. Common examples include Bus, Star, Mesh, Ring, and Daisy chain.



**OSI:** OSI stands for **Open Systems Interconnection**. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer. The OSI has been developed by the International Organization For Standardization and it is 7 layer architecture. Each layer of OSI has different functions and each layer has to follow different protocols.

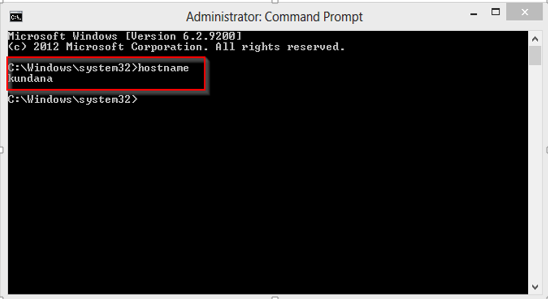
The 7 layers are:-

1. physical layer
2. Data link layer
3. Network layer
4. Transport layer
5. Session layer
6. Presentation layer
7. Application layer

**Protocol:**A protocol is a set of rules or algorithms which define the way how two entities can communicate across the network and there exists different protocol defined at each layer of the OSI model. Few of such protocols are TCP, IP, UDP, ARP, DHCP, FTP, and so on.

**UNIQUE IDENTIFIERS OF NETWORK**

**Host name:**Each device in the network is associated with a unique device name known as Hostname.   
Type “hostname” in the command prompt(Administrator Mode) and press ‘Enter’, this displays the hostname of your machine. 



**IP Address (Internet Protocol address):**  Also known as the Logical Address, the IP Address is the network address of the system across the network.   
To identify each device in the world-wide-web, the Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4) address as a unique identifier to each device on the Internet.   
The length of an IPv4 address is 32-bits, hence, we have 232 IP addresses available. The length of an IPv6 address is 128-bits.  
*Type “ipconfig” in the command prompt and press ‘Enter’, this gives us the IP address of the device.*

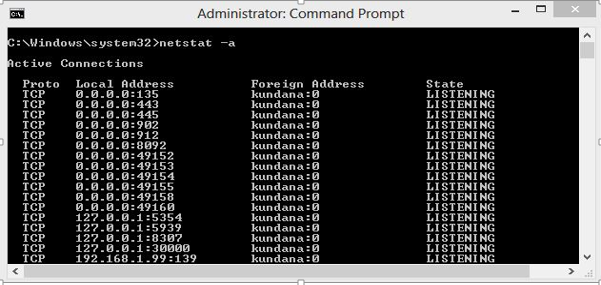
**MAC Address (Media Access Control address):**Also known as physical address, the MAC Address is the unique identifier of each host and is associated with its NIC (Network Interface Card).   
A MAC address is assigned to the NIC at the time of manufacturing.   
The length of the MAC address is : 12-nibble/ 6 bytes/ 48 bits   
*Type “ipconfig/all” in the command prompt and press ‘Enter’, this gives us the MAC address.*

**Port:**A port can be referred to as a logical channel through which data can be sent/received to an application. Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.

A port number is a 16-bit integer, hence, we have 216 ports available which are categorized as shown below: 

|  |  |
| --- | --- |
| **Port Types** | **Range** |
| **Well known Ports** | **0 – 1023** |
| **Registered Ports** | **1024 – 49151** |
| **Ephemeral Ports** | **49152 – 65535** |

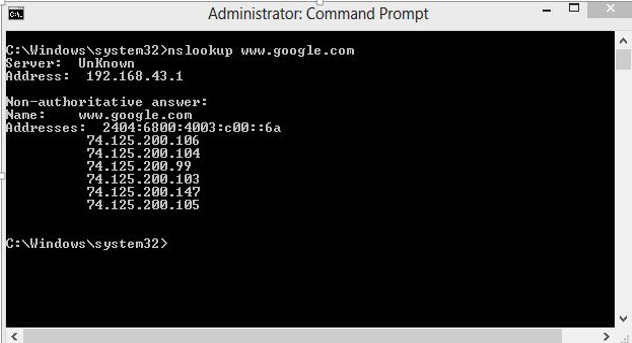
Number of post: 65,536   
Range: 0 – 65535   
*Type “****netstat -a****” in the command prompt and press ‘Enter’, this lists all the ports being used.*



**Socket:** The unique combination of IP address and Port number together are termed as Socket.

**Other related concepts**

**DNS Server:** DNS stands for **Domain Name system**. DNS is basically a server which translates web addresses or URLs (ex: www.google.com) into their corresponding IP addresses. We don’t have to remember all the IP addresses of each and every website. The command ‘**nslookup**’ gives you the IP address of the domain you are looking for. This also provides the information of our DNS Server. \



**RP:** ARP stands for **Address Resolution Protocol**.   
It is used to convert an IP address to its corresponding physical address(i.e., MAC Address).   
ARP is used by the Data Link Layer to identify the MAC address of the Receiver’s machine.

**RARP:** RARP stands for **Reverse Address Resolution Protocol**.   
As the name suggests, it provides the IP address of the device given a physical address as input. But RARP has become obsolete since the time DHCP has come into the picture.

**OSI Model Full Form in Computer Networking**

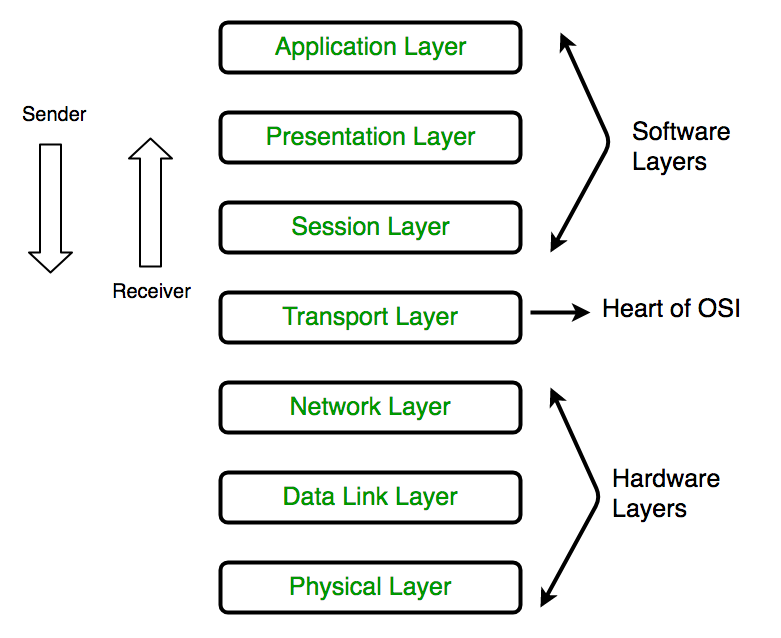
**OSI** stands for **Open Systems Interconnection.** The OSI model was developed by the International Organization for Standardization(ISO). It is a reference model for how applications communicate over a network. The OSI model characterizes computing functions into a universal set of rules and requirements to support interoperability between different products and software.

The OSI model can be considered a universal language for computer networking. It is based on the concept of divide and conquers, it splits up the communication system into 7 abstract layers, and the layer is stacked upon the previous layer.

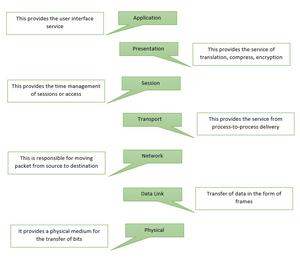
### Layers of OSI Model

OSI model has seven layers which are as follows:

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



### Functions of OSI model:



*Functions of OSI*

To learn more about layers, visit [Layers of OSI Model](https://www.geeksforgeeks.org/layers-of-osi-model/)

### Characteristics:

* It is the conceptual model that enables the diverse communication systems to communicate using the network.
* It was developed by the ISO (International Organization for Standardization) in 1984.
* It acts as an architecture for inter-computer communications.
* It is divided into 7 layers and each layer performs a particular task.
* Each layer is independent of the other and can perform its operations independently.

### Advantages:

* It is a layered model and each layer is independent. Thus, changes in one layer don’t affect the other layers.
* It divides the complex function into smaller parts.
* It is a generic model as it has the flexibility to adapt to many protocols.
* It supports both connection-oriented as well as connectionless services.
* It is more secure and adaptable than having all services bundled in a single layer.

### Disadvantages:

* It is purely a theoretical model and ignores the availability of resources and technologies. Hence, its practical implementation is somewhat restricted.
* It is very complex. The initial implementation was cumbersome, slow, and costly.
* The layers are interdependent, they can’t operate parallelly as they have to wait for the data/ packets from the predecessor layer.

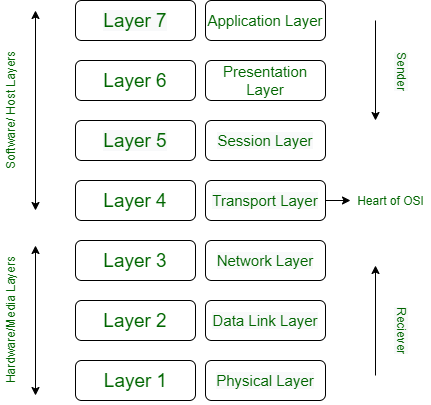
# How Communication happens using OSI model

[The Open System Interconnection (OSI) model](https://www.geeksforgeeks.org/layers-of-osi-model/) is a standard “**reference model”** created by an International Organization for Standardization (ISO) to describe how software and hardware components involved in network communication divide efforts and interact with each other.

The OSI model defines a seven-layer set of functional elements, from physical interrelations at level 1 (physical layer) up to layer 7 (application layer). Transmission Control Protocol (TCP) and Internet Protocol (IP) are two network standards that define the Internet. IP defines how computers can receive data from each other on a mutually connected set of networks. TCP defines how such networks can have more reliable channels of communication.

**Need of layers in the** **OSI model :**

1. The approach of establishing a link between two devices for communicating and sharing information is complex. Generating profitable communication takes many tasks. A network architecture needs to be developed to perform all these functions.
2. In network architecture, various tasks and functions are classified into related and manageable sets called LAYERS. Network architecture can be defined as a set of protocols that describe how each layer functions. Protocols are hidden in the OSI model and are easily changed as technology changes.
3. Intermediate systems require only a few layers and not all layers. Protocol layering enables us to design the system or device to which the consecutive layers are placed. It also allows services to be distinct from implementation.

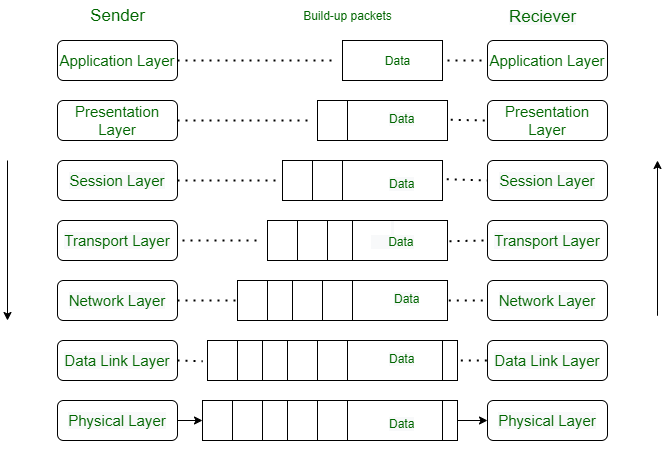


*A 7 Layer OSI/ISO reference Model*

**The reasons and advantages of using network architecture are as follows :**

1. The layered architecture provides variability to renovate and expand network services.
2. Management of new services and network infrastructure has become easier. It removes complications from the design process because the functions and their negotiation of each layer are distinguishable.
3. The number of layers, the names, and functions of the layers assigned to them can change from network to network. But for all networks, always the lower layer provides something Services of its upper layer.
4. The concept of layered architecture is a new way of looking at networks.
5. Logical segmentation allows parallel work on different tasks by different teams simultaneously.
6. Due to segmentation (layered structure), it is possible to break complex problems into simple and more feasible tasks.

**The communication process in the** **OSI/ISO model :**



*An exchange using ISO/OSI Model*

1. In higher layers, each layer of the sender adds its information to the message received from above that layer and moves the entire package just below the layer as shown in the figure.
2. Each layer added its information in the form of headers. Headers are added at the level of the messages (6, 5, 4, 3, and 2). A header is added at the Data Link layer (layer 2).
3. At the physical layer, communication is direct i.e. the sender sends a stream of bits to the receiver. At the physical layer (layer 1) the entire package is converted into a form that can be transferred to the receiver. On the receiver side, each process is accompanied layer-by-layer to receive and delete message data.
4. Always the upper OSI layers are implemented in the software (Transport layer, Session layer, Presentation layer, Application layer (4, 5,) and the lower layers are a combination of hardware and software (layer 2, 3), except for the physical layer which is mostly hardware. Layer 1, 2, and 3 (ie physical layer, data link layer, and network layer) are network support layers. They deal with physical aspects of moving data such as electrical specifications, physical connections, physical address, and transport time and reliability from one device to another. Layer 4, Transport layer end to end ensures reliable data transmission.
5. Not all applications need to use seven layers. The lower three layers are sufficient for most applications. Each layer is made up of electronic circuits and/or software and has a separate existence from the rest of the layers.
6. Each layer is assumed to handle messages or data from the layers that are above or below it. This is done by following protocol rules.
7. Thus, each layer takes data from the adjacent layer, Handles it according to these rules, and then sends the processed data to the next layer on the other side.

# Physical Layer in OSI Model

Physical Layer is the bottom-most layer in the [**Open System Interconnection**](https://www.geeksforgeeks.org/layers-of-osi-model/)**(OSI) Model**which is a physical and electrical representation of the system. It consists of various network components such as power plugs, connectors, receivers, cable types, etc. Physical Layer sends data bits from one device(s) (like a computer) to another device(s). Physical Layer defines the types of encoding (that is how the 0’s and 1’s are encoded in a signal). Physical Layer is responsible for the communication of the unstructured raw data streams over a physical medium.

**Functions Performed by Physical Layer :**  
Following are some important and basic functions that are performed by the Physical Layer of the OSI Model –

1. Physical Layer maintains the data rate (how many bits a sender can send per second).
2. It performs Synchronization of bits.
3. It helps in Transmission Medium decision (direction of data transfer).
4. It helps in Physical Topology (Mesh, Star, Bus, Ring) decision (Topology through which we can connect the devices with each other).
5. It helps in providing Physical Medium and Interface decisions.
6. It provides two types of configuration Point to Point configuration and Multi-Point configuration.
7. It provides an interface between devices (like PC’s or computers) and transmission medium.
8. It has a protocol data unit in bits.
9. Hubs, Ethernet, etc. device is used in this layer.
10. This layer comes under the category of Hardware Layers (since the hardware layer is responsible for all the physical connection establishment and processing too).
11. It provides an important aspect called Modulation, which is the process of converting the data into radio waves by adding the information to an electrical or optical nerve signal.
12. It also provides Switching mechanism wherein data packets can be forward from one port (sender port) to the leading destination port.

# Presentation Layer in OSI model

**Introduction :** Presentation Layer is the 6th layer in the Open System Interconnection (OSI) model. This layer is also known as Translation layer, as this layer serves as a data translator for the network. The data which this layer receives from the Application Layer is extracted and manipulated here as per the required format to transmit over the network. The main responsibility of this layer is to provide or define the data format and encryption. The presentation layer is also called as Syntax layer since it is responsible for maintaining the proper syntax of the data which it either receives or transmits to other layer(s).

Application Layer

Present Layer=> Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Layer

Physical Layer

**Functions of Presentation Layer :**

Data from Application Layer <=> Presentation layer <=> Data from Session Layer

The presentation layer, being the 6th layer in the OSI model, performs several types of functions, which are described below-

* Presentation layer format and encrypts data to be sent across the network.
* This layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data efficiently and effectively.
* This layer manages the abstract data structures and allows high-level data structures (example- banking records), which are to be defined or exchanged.
* This layer carries out the encryption at the transmitter and decryption at the receiver.
* This layer carries out data compression to reduce the bandwidth of the data to be transmitted (the primary goal of data compression is to reduce the number of bits which is to be transmitted).
* This layer is responsible for interoperability (ability of computers to exchange and make use of information) between encoding methods as different computers use different encoding methods.
* This layer basically deals with the presentation part of the data.
* Presentation layer, carries out the data compression (number of bits reduction while transmission), which in return improves the data throughput.
* This layer also deals with the issues of string representation.
* The presentation layer is also responsible for integrating all the formats into a standardized format for efficient and effective communication.
* This layer encodes the message from the user-dependent format to the common format and vice-versa for communication between dissimilar systems.
* This layer deals with the syntax and semantics of the messages.
* This layer also ensures that the messages which are to be presented to the upper as well as the lower layer should be standardized as well as in an accurate format too.
* Presentation layer is also responsible for translation, formatting, and delivery of information for processing or display.
* This layer also performs serialization (process of translating a data structure or an object into a format that can be stored or transmitted easily).

**Features of Presentation Layer in the OSI model:** Presentation layer, being the 6th layer in the OSI model, plays a vital role while communication is taking place between two devices in a network.

List of features which are provided by the presentation layer are:

* Presentation layer could apply certain sophisticated compression techniques, so fewer bytes of data are required to represent the information when it is sent over the network.
* If two or more devices are communicating over an encrypted connection, then this presentation layer is responsible for adding encryption on the sender’s end as well as the decoding the encryption on the receiver’s end so that it can represent the application layer with unencrypted, readable data.
* This layer formats and encrypts data to be sent over a network, providing freedom from compatibility problems.
* This presentation layer also negotiates the Transfer Syntax.
* This presentation layer is also responsible for compressing data it receives from the application layer before delivering it to the session layer (which is the 5th layer in the OSI model) and thus improves the speed as well as the efficiency of communication by minimizing the amount of the data to be transferred.

**Working of Presentation Layer in the OSI model :**  
Presentation layer in the OSI model, as a translator, converts the data sent by the application layer of the transmitting node into an acceptable and compatible data format based on the applicable network protocol and architecture.  Upon arrival at the receiving computer, the presentation layer translates data into an acceptable format usable by the application layer. Basically, in other words, this layer takes care of any issues occurring when transmitted data must be viewed in a format different from the original format. Being the functional part of the OSI mode, the presentation layer performs a multitude (large number of) data conversion algorithms and character translation functions. Mainly, this layer is responsible for managing two network characteristics: protocol (set of rules) and architecture.

**Presentation Layer Protocols :**  
Presentation layer being the 6th layer, but the most important layer in the OSI model performs several types of functionalities, which makes sure that data which is being transferred or received should be accurate or clear to all the devices which are there in a closed network.  
Presentation Layer, for performing translations or other specified functions, needs to use certain protocols which are defined below –

* [**Apple Filing Protocol (AFP):**](https://www.geeksforgeeks.org/afp-fullform/) Apple Filing Protocol is the proprietary network protocol (communications protocol) that offers services to macOS or the classic macOS. This is basically the network file control protocol specifically designed for Mac-based platforms.
* **Lightweight Presentation Protocol (LPP):** Lightweight Presentation Protocol is that protocol which is used to provide ISO presentation services on the top of TCP/IP based protocol stacks.
* [**NetWare Core Protocol (NCP):**](https://www.geeksforgeeks.org/introduction-of-novell-netware/) NetWare Core Protocol is the network protocol which is used to access file, print, directory, clock synchronization, messaging, remote command execution and other network service functions.
* **Network Data Representation (NDR):** Network Data Representation is basically the implementation of the presentation layer in the OSI model, which provides or defines various primitive data types, constructed data types and also several types of data representations.
* **External Data Representation (XDR):** External Data Representation (XDR) is the standard for the description and encoding of data. It is useful for transferring data between computer architectures and has been used to communicate data between very diverse machines. Converting from local representation to XDR is called encoding, whereas converting XDR into local representation is called decoding.
* [**Secure Socket Layer (SSL):**](https://www.geeksforgeeks.org/secure-socket-layer-ssl/) The Secure Socket Layer protocol provides security to the data that is being transferred between the web browser and the server. SSL encrypts the link between a web server and a browser, which ensures that all data passed between them remains private and free from attacks.

# Application Layer in OSI Model

**Introduction :**  
The Application Layer is topmost layer in the Open System Interconnection (OSI) model. This layer provides several ways for manipulating the data (information) which actually enables any type of user to access network with ease. This layer also makes a request to its bottom layer, which is presentation layer for receiving various types of information from it. The Application Layer interface directly interacts with application and provides common web application services. This layer is basically highest level of open system, which provides services directly for application process.

Present Layer=> Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Layer

Physical Layer

**Functions of Application Layer :**  
The Application Layer, as discussed above, being topmost layer in OSI model, performs several kinds of functions which are requirement in any kind of application or communication process.  
Following are list of functions which are performed by Application Layer of OSI Model –

Data from User <=> Application layer <=> Data from Presentation Layer

* Application Layer provides a facility by which users can forward several emails and it also provides a storage facility.
* This layer allows users to access, retrieve and manage files in a remote computer.
* It allows users to log on as a remote host.
* This layer provides access to global information about various services.
* This layer provides services which include: e-mail, transferring files, distributing results to the user, directory services, network resources and so on.
* It provides protocols that allow software to send and receive information and present meaningful data to users.
* It handles issues such as network transparency, resource allocation and so on.
* This layer serves as a window for users and application processes to access network services.
* Application Layer is basically not a function, but it performs application layer functions.
* The application layer is actually an abstraction layer that specifies the shared protocols and interface methods used by hosts in a communication network.
* Application Layer helps us to identify communication partners, and synchronizing communication.
* This layer allows users to interact with other software applications.
* In this layer, data is in visual form, which makes users truly understand data rather than remembering or visualize the data in the binary format (0’s or 1’s).
* This application layer basically interacts with Operating System (OS) and thus further preserves the data in a suitable manner.
* This layer also receives and preserves data from it’s previous layer, which is Presentation Layer (which carries in itself the syntax and semantics of the information transmitted).
* The protocols which are used in this application layer depend upon what information users wish to send or receive.
* This application layer, in general, performs host initialization followed by remote login to hosts.

**Working of Application Layer in the OSI model :**  
In the OSI model, this application layer is narrower in scope.   
The application layer in the OSI model generally acts only like the interface which is responsible for communicating with host-based and user-facing applications. This is in contrast with TCP/IP protocol, wherein the layers below the application layer, which is Session Layer and Presentation layer, are clubbed together and form a simple single layer which is responsible for performing the functions, which includes controlling the dialogues between computers, establishing as well as maintaining as well as ending a particular session, providing data compression and data encryption and so on.

At first, client sends a command to server and when server receives that command, it allocates port number to client. Thereafter, the client sends an initiation connection request to server and when server receives request, it gives acknowledgement (ACK) to client through client has successfully established a connection with the server and, therefore, now client has access to server through which it may either ask server to send any types of files or other documents or it may upload some files or documents on server itself.

**Features provided by Application Layer Protocols :**  
To ensure smooth communication, application layer protocols are implemented the same on source host and destination host.  
The following are some of the features which are provided by Application layer protocols-

* The Application Layer protocol defines process for both parties which are involved in communication.
* These protocols define the type of message being sent or received from any side (either source host or destination host).
* These protocols also define basic syntax of the message being forwarded or retrieved.
* These protocols define the way to send a message and the expected response.
* These protocols also define interaction with the next level.

[**Application Layer Protocols:**](https://www.geeksforgeeks.org/protocols-application-layer/) The application layer provides several protocols which allow any software to easily send and receive information and present meaningful data to its users.  
The following are some of the protocols which are provided by the application layer.

* [**TELNET:**](https://www.geeksforgeeks.org/introduction-to-telnet/) Telnet stands for Telecommunications Network. This protocol is used for managing files over the Internet. It allows the Telnet clients to access the resources of Telnet server. Telnet uses port number 23.
* [**DNS:**](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/) DNS stands for Domain Name System. The DNS service translates the domain name (selected by user) into the corresponding IP address. For example- If you choose the domain name as www.abcd.com, then DNS must translate it as 192.36.20.8 (random IP address written just for understanding purposes). DNS protocol uses the port number 53.
* [**DHCP:**](https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/) DHCP stands for Dynamic Host Configuration Protocol. It provides IP addresses to hosts. Whenever a host tries to register for an IP address with the DHCP server, DHCP server provides lots of information to the corresponding host. DHCP uses port numbers 67 and 68.
* [**FTP:**](https://www.geeksforgeeks.org/file-transfer-protocol-ftp-in-application-layer/) FTP stands for File Transfer Protocol. This protocol helps to transfer different files from one device to another. FTP promotes sharing of files via remote computer devices with reliable, efficient data transfer. FTP uses port number 20 for data access and port number 21 for data control.
* [**SMTP:**](https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp/) SMTP stands for Simple Mail Transfer Protocol. It is used to transfer electronic mail from one user to another user. SMTP is used by end users to send emails with ease. SMTP uses port numbers 25 and 587.
* [**HTTP:**](https://www.geeksforgeeks.org/http-full-form/) HTTP stands for Hyper Text Transfer Protocol. It is the foundation of the World Wide Web (WWW). HTTP works on the client server model. This protocol is used for transmitting hypermedia documents like HTML. This protocol was designed particularly for the communications between the web browsers and web servers, but this protocol can also be used for several other purposes. HTTP is a stateless protocol (network protocol in which a client sends requests to server and server responses back as per the given state), which means the server is not responsible for maintaining the previous client’s requests. HTTP uses port number 80.
* [**NFS:**](https://www.geeksforgeeks.org/network-file-system-nfs/) NFS stands for Network File System. This protocol allows remote hosts to mount files over a network and interact with those file systems as though they are mounted locally. NFS uses the port number 2049.
* [**SNMP:**](https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/) SNMP stands for Simple Network Management Protocol. This protocol gathers data by polling the devices from the network to the management station at fixed or random intervals, requiring them to disclose certain information. SNMP uses port numbers 161 (TCP) and 162 (UDP).