Computer networking

[Basics of Computer Networking](https://www.geeksforgeeks.org/basics-computer-networking/)

[Computer Network Tutorial](https://www.javatpoint.com/computer-network-tutorial)

[Network and Communication](https://www.geeksforgeeks.org/network-and-communication/)

[Difference between Unicast, Broadcast and Multicast in Computer Network](https://www.geeksforgeeks.org/difference-between-unicast-broadcast-and-multicast-in-computer-network/)

**Computer networking**

Networking refers to the practice of connecting two or more devices or systems so that they can communicate with each other and exchange data or information. In the context of computing, networking often refers to the use of computer networks, which are collections of interconnected computers, servers, routers, and other devices that allow users to share resources, such as files, printers, and internet access.

Computer networking can be accomplished through wired or wireless connections and can be local or wide area in scale. Local area networks (LANs) typically connect devices within a building or campus, while wide area networks (WANs) connect devices across larger geographical areas. Other types of networks include metropolitan area networks (MANs), which cover a city or town, and storage area networks (SANs), which connect storage devices to servers.

Networking plays a crucial role in modern communication and information technology, enabling businesses, organizations, and individuals to collaborate, share resources, and access information and services from remote locations.

**How Does a Computer Network Work?**

Computer networks function by connecting multiple devices together and allowing them to communicate and exchange data with each other. The basic functioning of a computer network involves three key elements: hardware, software, and protocols.

1. **Hardware**: The hardware components of a network include the physical devices that are used to connect and transmit data between devices. This includes network interface cards (NICs), routers, switches, hubs, cables, and other networking equipment.
2. **Software**: The software components of a network include the various applications and programs that are used to manage and control the network. This includes network operating systems, device drivers, and management tools.
3. **Protocols**: The protocols are a set of rules and procedures that are used to govern the communication between devices on a network. This includes protocols like TCP/IP, HTTP, FTP, and DNS, which define how data is transmitted, addressed, and routed across the network.
4. When devices are connected to a network, they are assigned unique addresses that enable them to send and receive data to and from other devices on the network.
5. Data is transmitted across the network in the form of packets, which contain the information being transmitted as well as the address of the destination device.
6. In order for data to be transmitted across the network, it must first be broken down into smaller packets that can be transmitted more efficiently.
7. Each packet is then transmitted across the network using a series of routers, switches, and other networking devices that help to direct the packet to its destination.
8. Once the packets reach their destination device, they are reassembled into the original data format and delivered to the appropriate application or program.

Overall, computer networks function by allowing devices to communicate and exchange data with each other through a combination of hardware, software, and protocols. By connecting devices together, computer networks enable users to share resources, collaborate on projects, and access information from anywhere in the world.

**Network Hardware:**

There are various hardware devices used in computer networking to facilitate connectivity, communication, and data transmission. Some of the commonly used hardware devices for networking include:

1. Network Interface Card (NIC): A Network Interface Card, also known as a network adapter or network card, is a hardware device that enables a computer or device to connect to a network. It provides the physical interface between the computer and the network medium, such as Ethernet or Wi-Fi.
2. Router: A router is a networking device that connects multiple networks together and routes data packets between them. Routers determine the optimal path for data transmission across the network and help in directing traffic efficiently.
3. Switch: A switch is a networking device that connects multiple devices within a network. It operates at the data link layer (Layer 2) of the OSI model and forwards data packets only to the intended device within the network.
4. Hub: A hub is a simple networking device that connects multiple devices within a network. Unlike a switch, a hub broadcasts incoming data packets to all connected devices, which means all devices on the hub receive the same data.
5. Modem: A modem (modulator-demodulator) is a device that converts digital signals from a computer into analog signals that can be transmitted over telephone lines or cable lines. It is used to establish a connection to an Internet Service Provider (ISP).
6. Firewall: A firewall is a network security device that monitors and filters network traffic to protect a network from unauthorized access and potential threats. It helps in enforcing security policies and controlling network traffic.
7. Wireless Access Point (WAP): A wireless access point, also known as an access point, enables wireless devices to connect to a wired network. It acts as a bridge between wired and wireless networks, providing wireless connectivity within a specific area.
8. Network Attached Storage (NAS): NAS is a specialized device used for storing and sharing files over a network. It provides centralized storage that can be accessed by multiple devices on the network.
9. Network Cables: Various types of network cables, such as Ethernet cables (e.g., Cat5e, Cat6) and fiber optic cables, are used to physically connect devices within a network.

These are just a few examples of hardware devices used in computer networking. The selection of specific hardware devices depends on the network requirements, scale, and technology being employed.

**Network Software:**

There are several software components and applications used in computer networking to manage and control network operations. Here are some common software used in networking:

1. Network Operating Systems (NOS): Network operating systems are specialized software designed to manage and administer network resources. They provide features such as file sharing, printer sharing, user authentication, and security settings. Examples of network operating systems include Windows Server, Linux distributions like Ubuntu Server, and Novell NetWare.
2. Network Management Software: Network management software enables network administrators to monitor, configure, and control network devices and infrastructure. These tools provide functionalities such as network performance monitoring, device configuration management, and fault detection. Popular network management software includes SolarWinds Network Performance Monitor, Cisco Prime Infrastructure, and Nagios.
3. Protocol Analyzers: Protocol analyzers or network sniffers are software tools that capture and analyze network traffic. They help in troubleshooting network issues, monitoring network performance, and identifying potential security threats. Wireshark and tcpdump are widely used protocol analyzers.
4. Network Configuration Tools: These tools assist in configuring and managing network devices, such as routers and switches. They simplify the process of setting up network parameters, IP addressing, and security settings. Examples include Cisco Configuration Professional, Juniper Networks Junos Space, and HP Intelligent Management Center.
5. Virtual Private Network (VPN) Software: VPN software enables secure remote access to a private network over the public internet. It provides encryption and authentication mechanisms for secure data transmission. Popular VPN software includes OpenVPN, Cisco AnyConnect, and Fortinet FortiClient.
6. Network Monitoring and Analysis Tools: These tools monitor network performance, analyze network traffic, and provide insights into network behavior. They help in identifying bottlenecks, troubleshooting issues, and optimizing network performance. Examples include PRTG Network Monitor, Zabbix, and Nagios.
7. Firewall and Security Software: Firewall software is used to protect networks from unauthorized access and malicious activities. It filters network traffic based on predefined security policies and rules. Software firewalls like Windows Firewall and zone-based firewalls like pfSense are commonly used.

These are just a few examples of software used in computer networking. The specific software used depends on the network requirements, infrastructure, and management needs.

**Protocols:**

In the context of computer networking, a protocol refers to a set of rules and procedures that govern the communication between devices on a network. Protocols define the format and content of data packets that are exchanged between devices, as well as the order in which packets are transmitted and received. A few such protocols are TCP, IP, UDP, ARP, DHCP, FTP, and so on.

Protocols are essential for enabling different devices to communicate with each other in a predictable and consistent manner. They ensure that data is transmitted reliably and efficiently, and that devices can understand and interpret the information being exchanged.

There are many different protocols used in computer networking, each with its own specific set of rules and procedures. Some common protocols include TCP/IP, HTTP, FTP, DNS, SMTP, and many others.

TCP/IP, for example, is a protocol suite that defines how data is transmitted over the internet. It includes the Transmission Control Protocol (TCP), which is responsible for establishing and maintaining connections between devices, and the Internet Protocol (IP), which is responsible for routing data packets between devices.

HTTP, which stands for Hypertext Transfer Protocol, is a protocol used for transmitting data over the World Wide Web. It defines how web browsers and web servers communicate with each other, and how web pages are formatted and displayed.

Overall, protocols are essential for ensuring the smooth and efficient operation of computer networks, and for enabling devices to communicate and exchange data in a reliable and predictable manner.

**Protocols Function:**

Protocols function by providing a set of rules, procedures, and formats that devices on a network follow to enable communication and data exchange. They establish a common language and framework that devices use to understand and interpret the information being transmitted.

Here's an overview of how protocols function:

1. **Message Format**: Protocols define the structure and format of messages or data packets exchanged between devices. This includes specifying how data is organized, the order of information within the packet, and any necessary headers or trailers.
2. **Addressing**: Protocols define how devices are identified and addressed on the network. They establish addressing schemes, such as IP addresses or MAC addresses, to ensure that data is sent to the intended destination.
3. **Handshaking**: Many protocols include mechanisms for devices to establish a connection or session with each other before data transfer. This typically involves a series of communication steps to negotiate settings, synchronize communication, and verify readiness.
4. **Error Detection and Correction**: Protocols often incorporate error detection and correction mechanisms to ensure data integrity. They use techniques such as checksums or cyclic redundancy checks (CRC) to identify errors in the data and request retransmission if needed.
5. **Flow Control and Congestion Control**: Protocols include methods to manage the flow of data between devices and handle congestion. Flow control mechanisms regulate the rate of data transmission to prevent overwhelming the receiving device, while congestion control techniques manage network congestion by adjusting transmission rates.
6. **Routing and Address Resolution**: Network protocols, such as routing protocols, determine the best path for data to reach its destination across interconnected networks. Address resolution protocols, like ARP (Address Resolution Protocol), help devices map IP addresses to MAC addresses for proper communication within a local network.
7. **Security**: Protocols may incorporate security mechanisms to protect data and ensure secure communication. This can involve encryption, authentication, and authorization protocols to safeguard sensitive information and prevent unauthorized access.

By defining these rules and procedures, protocols enable devices from different manufacturers and with different operating systems to communicate effectively. They ensure that devices understand how to send, receive, and process data in a standardized manner, enabling seamless communication and interoperability within the network.

## Basic Terminologies of Computer Networks

* **Network:**A network is a collection of computers and devices that are connected to enable communication and data exchange.
* **Nodes:**Nodes are devices that are connected to a network. These can include computers, Servers, Printers, [Routers,](https://www.geeksforgeeks.org/introduction-of-a-router/) [Switches](https://www.geeksforgeeks.org/types-of-switches-in-computer-network/), 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](https://www.geeksforgeeks.org/tcp-ip-model/), [HTTP](https://www.geeksforgeeks.org/http-full-form/), and [FTP](https://www.geeksforgeeks.org/file-transfer-protocol-ftp-in-application-layer/).
* **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.
* **Service Provider Networks:**These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.
* **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)](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/) 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](https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/) 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.

**Types of Enterprise Computer Networks**

* **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.
* **Cloud Networks**: Cloud Networks can be visualized with a Wide Area Network (WAN) as they can be hosted on public or private cloud service providers and cloud networks are available if there is a demand. Cloud Networks consist of Virtual Routers, Firewalls, etc.

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. Now we are going to discuss some more concepts on Computer Networking.

* **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.

**Cloud Networks**

Cloud networks refer to the infrastructure and networking components that enable the delivery of cloud computing services over the internet. Cloud networks play a crucial role in facilitating connectivity, data transfer, and communication between various components of a cloud environment, including servers, storage systems, virtual machines, and applications.

Here are some key aspects of cloud networks:

1. Virtualized Infrastructure: Cloud networks are built on virtualized infrastructure, where physical resources, such as servers and storage, are abstracted and partitioned into virtual instances. This virtualization enables flexible resource allocation and scalability, allowing cloud providers to dynamically allocate resources based on demand.
2. Network Virtualization: Network virtualization is a key component of cloud networks. It involves creating virtual networks that operate on top of the physical network infrastructure. Virtual networks provide isolation, security, and flexibility, allowing multiple customers or tenants to share the same underlying physical network infrastructure while maintaining separation and control over their respective virtual networks.
3. Software-Defined Networking (SDN): SDN is a network architecture that separates the control plane from the data plane. In the context of cloud networks, SDN enables centralized management and control of network resources. It allows network administrators to dynamically configure and provision network services, adjust network policies, and optimize traffic routing based on application needs.
4. Network Connectivity: Cloud networks provide connectivity between different components and services within the cloud environment. This includes establishing secure connections between virtual machines, containers, and storage systems, as well as enabling communication between cloud-based applications and end-users accessing those applications over the internet.
5. Load Balancing and Traffic Management: Cloud networks often employ load balancing and traffic management techniques to distribute incoming network traffic across multiple servers or instances. Load balancers help optimize resource utilization, enhance performance, and improve availability by efficiently distributing workloads across the cloud infrastructure.
6. Hybrid and Multi-Cloud Networking: Cloud networks also support hybrid and multi-cloud environments, where organizations combine their on-premises infrastructure with public cloud services or utilize multiple cloud providers. Networking components and technologies, such as virtual private networks (VPNs), software-defined wide area networks (SD-WAN), and inter-cloud connectivity options, facilitate seamless integration and communication across different cloud environments.

Cloud networks are designed to provide reliable, scalable, and secure connectivity to support the delivery of cloud-based services. They enable organizations to leverage the benefits of cloud computing, including flexibility, scalability, and on-demand resource allocation, while ensuring efficient communication and data transfer within the cloud environment.

[Cloud Networking](https://www.javatpoint.com/cloud-networking-managing-and-optimizing-cloud-based-networks)

**Types of Computer Network Architecture**

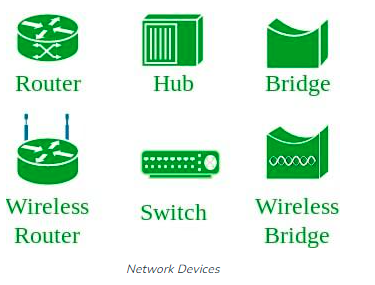
Computer Network falls under these broad Categories:

Client-Server Architecture: [Client-Server Architecture](https://www.geeksforgeeks.org/client-server-model/) is a type of Computer Network Architecture in which Nodes can be Servers or Clients. Here, the server node can manage the Client Node Behaviour.

Peer-to-Peer Architecture: In [P2P (Peer-to-Peer) Architecture](https://www.geeksforgeeks.org/what-is-p2ppeer-to-peer-process/),, there is not any concept of a Central Server. Each device is free for working as either client or server.

**Network Devices**

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](https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/) and include things such as routers, switches, hubs, and bridges.



**Network Topology**

The [Network Topology](https://www.geeksforgeeks.org/types-of-network-topology/) is the layout arrangement of the different devices in a network. Common examples include Bus, Star, Mesh, Ring, and Daisy chain.

A picture containing diagram, line, font, origami

Description automatically generated

### **OSI Model**

OSI stands for [Open Systems Interconnection](https://www.geeksforgeeks.org/layers-of-osi-model/). It is a reference model that specifies standards for communications protocols and 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 as follows:

### [Physical Layer](https://www.geeksforgeeks.org/physical-layer-in-osi-model/)

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

A picture containing font, text, line, number

Description automatically generated

The Functions of the Physical Layer

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

Note: 1. Hub, Repeater, Modem, and Cables are Physical Layer devices.

Network Layer, Data Link Layer, and Physical Layer are also known as Lower Layers or Hardware Layers.

### [Data link Layer](https://www.geeksforgeeks.org/data-link-layer/)

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

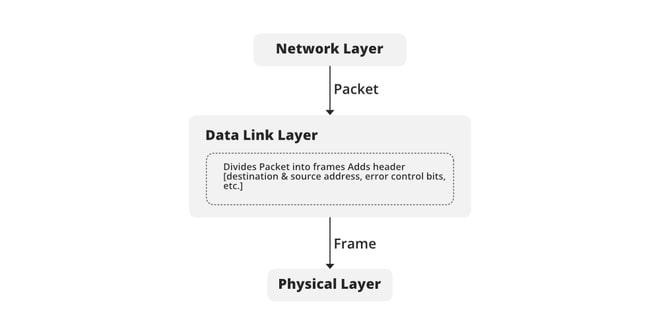
1. [Logical Link Control (LLC)](https://www.geeksforgeeks.org/logical-link-control-llc-protocol-data-unit/)
2. [Media Access Control (MAC)](https://www.geeksforgeeks.org/introduction-of-mac-address-in-computer-network/)

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

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

### The Functions of the Data Link Layer

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



*Function of DLL*

**Note:**1. Packet in the Data Link layer is referred to as **Frame.**

           2. Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.

           3. Switch & Bridge are Data Link Layer devices.

### [Network Layer](https://www.geeksforgeeks.org/network-layer-services-packetizing-routing-and-forwarding/)

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver’s IP addresses are placed in the header by the network layer.

### The Functions of the Network Layer

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

Note: 1. Segment in the Network layer is referred to as **Packet**.

          2. Network layer is implemented by networking devices such as routers.

### [Transport Layer](https://www.geeksforgeeks.org/transport-layer-responsibilities/)

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

**At the sender’s side:**The transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

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

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

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

### The Functions of the Transport Layer

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

#### Services Provided by Transport Layer

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

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

* Connection Establishment
* Data Transfer
* Termination/disconnection

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

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

**Note:** 1. Data in the Transport Layer is called **Segments**.

         2. Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.   
           3. The transport layer is called as **Heart of the OSI** model.

### [Session Layer](https://www.geeksforgeeks.org/session-layer-in-osi-model/)

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

### The Functions of the Session Layer

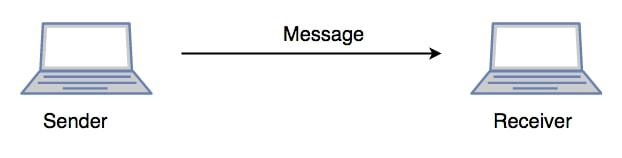
* **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use and terminate a connection.
* **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to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

**Note:** 1. All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as the “Application Layer”.

           2. Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers or** **Software Layers.**

#### Scenario

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



*Communication in Session Layer*

### [Presentation Layer](https://www.geeksforgeeks.org/presentation-layer-in-osi-model/)

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

### The Functions of the Presentation Layer are

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

### [Application Layer](https://www.geeksforgeeks.org/application-layer-in-osi-model/)

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

Example: Application – Browsers, Skype Messenger, etc.

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

### The Functions of the Application Layer are

* Network Virtual Terminal
* FTAM- File transfer access and management
* Mail Services
* Directory Services

The layers of the OSI model work together in a hierarchical manner, with each layer relying on the services provided by the layer below it. Data from the upper layers is encapsulated and processed as it moves down the layers, and at the receiving end, the process is reversed as data is passed up the layers.

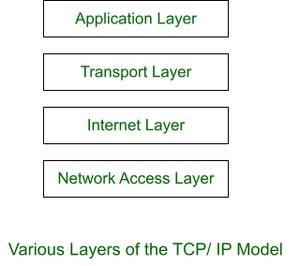
This layering approach allows for modularity, flexibility, and interoperability in network design and implementation, as different layers can be developed, updated, and replaced independently, as long as they adhere to the standardized protocols and interfaces defined by the model.

**OSI Model in a Nutshell**

| **Layer No** | **Layer Name** | **Responsibility** | **Information Form(Data Unit)** | **Device** |
| --- | --- | --- | --- | --- |
| 7 | Application Layer | Helps in identifying the client and synchronizing communication. | Message | – |
| 6 | Presentation Layer | Data from the application layer is extracted and manipulated in the required format for transmission. | Message | – |
| 5 | Session Layer | Establishes Connection, Maintenance, Ensures Authentication, and Ensures security. | Message | Gateway |
| 4 | Transport Layer | Take Service from Network Layer and provide it to the Application Layer. | Segment | Firewall |
| 3 | Network Layer | Transmission of data from one host to another, located in different networks. | Packet | Router |
| 2 | Data Link Layer | Node to Node Delivery of Message. | Frame | Switch, Bridge |
| 1 | Physical Layer | Establishing Physical Connections between Devices. | Bits | Hub, Repeater, Modem, Cables |

**TCP/IP Model**

TCP/IP stands for Transmission Control Protocol/Internet Protocol. It has 4 layers named as Physical layer, Network layer, Transport layer, and Application layer.  It also can be used as a communications protocol in a private computer network. It was designed by Vint Cerf and Bob Kahn in the 1970s.



**Advantages**

* Many Routing protocols are supported.
* It is highly scalable and uses a client-server architecture.
* It is lightweight.

**Disadvantages**

* Little difficult to set up.
* Delivery of packets is not guaranteed by the transport layer.
* Vulnerable to a synchronization attack.

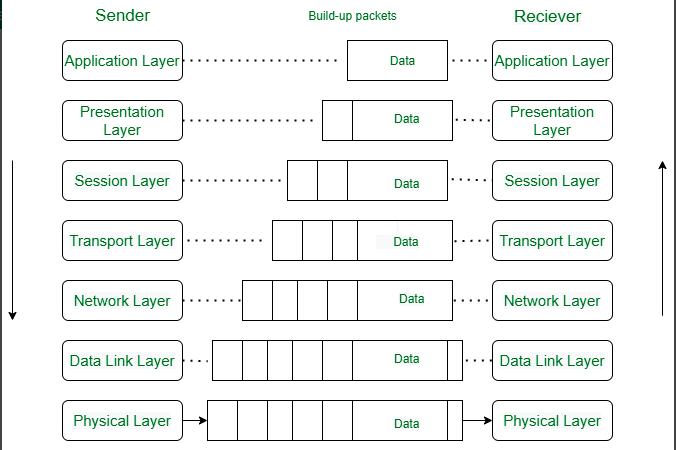
**Difference between OSI Model and TCP/IP Model**

| **Parameters** | **OSI Model** | **TCP/IP Model** |
| --- | --- | --- |
| Full Form | OSI stands for Open Systems Interconnection. | TCP/IP stands for Transmission Control Protocol/Internet Protocol. |
| Layers | It has 7 layers. | It has 4 layers. |
| Usage | It is low in usage. | It is mostly used. |
| Approach | It is vertically approached. | It is horizontally approached. |
| Delivery | Delivery of the package is guaranteed in OSI Model. | Delivery of the package is not guaranteed in TCP/IP Model. |
| Replacement | Replacement of tools and changes can easily be done in this model. | Replacing the tools is not easy as it is in OSI Model. |

[TCP/IP in Computer Networking](https://www.geeksforgeeks.org/tcp-ip-in-computer-networking/)

[Layers of OSI Model](https://www.geeksforgeeks.org/layers-of-osi-model/)

OSI stands for Open Systems Interconnection. It has been developed by ISO – ‘International Organization for Standardization ‘, in the year 1984. It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



Types of Networking:

There are several types of computer networking, each serving different purposes and catering to different requirements. Here are some common types of networking:

1. Local Area Network (**LAN**): A LAN connects devices within a limited geographical area, such as a home, office, or school. It enables devices to share resources and communicate with each other, typically at high speeds.
2. Wide Area Network (**WAN**): WANs connect devices over a large geographical area, often spanning multiple cities or even countries. The internet is an example of a WAN. WANs use routers and other networking equipment to transmit data across long distances.
3. Metropolitan Area Network (**MAN**): A MAN covers a larger area than a LAN but smaller than a WAN. It connects multiple LANs within a metropolitan area, such as a city. MANs are often used by service providers to offer internet connectivity to businesses and homes.
4. Wireless Local Area Network (**WLAN**): A WLAN is a type of LAN that uses wireless communication instead of physical cables to connect devices. Wi-Fi networks are examples of WLANs. They provide flexibility and mobility by allowing devices to connect without the need for wired connections.
5. Personal Area Network (**PAN**): A PAN is a network that connects devices within an individual's personal workspace, typically within a range of a few meters. Bluetooth technology is commonly used for PANs, enabling devices like smartphones, tablets, and peripherals to communicate with each other.
6. Campus Area Network (**CAN**): A CAN is a network that spans a university campus, corporate campus, or any other large-scale area. It connects multiple LANs within the campus and often incorporates high-speed connections and specialized equipment.
7. Storage Area Network (**SAN**): A SAN is a dedicated network that provides high-speed access to storage devices, such as disk arrays or tape libraries. SANs are commonly used in data centers to centralize storage resources and enable efficient data management.
8. Virtual Private Network (**VPN**): A VPN creates a secure and encrypted connection over a public network, such as the internet. It allows users to access a private network remotely, ensuring confidentiality and privacy for data transmission.

These are some of the primary types of networking, each with its own characteristics, advantages, and use cases.

**Firewall:**

A firewall is a security device or software that monitors and controls the incoming and outgoing network traffic between a computer network and the Internet. Its primary purpose is to protect the network and its connected devices from unauthorized access, malicious activities, and potential threats. A firewall acts as a barrier between the internal network and external networks, filtering and inspecting network traffic based on predefined security rules. Here's an overview of how a firewall works:

1. **Traffic Monitoring**: A firewall continuously monitors network traffic passing through it. It examines the source and destination addresses, ports, protocols, and other relevant information of each network packet.
2. **Traffic Filtering**: The firewall applies a set of predefined rules or policies to the incoming and outgoing network traffic. These rules determine whether to allow or block specific types of traffic based on various criteria, such as IP addresses, port numbers, protocols, and application signatures.
3. **Packet Inspection**: Firewalls can perform deep packet inspection (DPI) to analyze the contents of network packets beyond the header information. This allows the firewall to detect and block specific types of malicious or unauthorized content, such as malware, viruses, and intrusion attempts.
4. **Access Control**: Firewalls enforce access control policies by permitting or denying traffic based on the defined rules. For example, a firewall may allow outbound web browsing traffic on port 80 but block incoming traffic on certain ports that are commonly targeted by hackers.
5. **Network Address Translation (NAT):** Firewalls often incorporate network address translation to hide the internal IP addresses of devices on the internal network. This provides an additional layer of security by obfuscating the network topology and making it more challenging for external threats to target specific devices.
6. **Stateful Inspection**: Many firewalls use stateful inspection to keep track of the state of network connections. This involves examining the context and history of network traffic to determine whether a packet is part of an established connection or a new connection attempt. Stateful inspection helps prevent unauthorized access and ensures that incoming packets are legitimate responses to outgoing requests.
7. **Logging and Reporting**: Firewalls maintain logs of network traffic events, including allowed and blocked connections, intrusion attempts, and other security-related activities. These logs can be used for auditing, troubleshooting, and forensic analysis. Firewalls may also generate reports that provide insights into network traffic patterns, security incidents, and compliance with security policies.
8. **Virtual Private Network (VPN)** Support: Some firewalls include VPN capabilities, allowing secure remote access to the internal network. VPNs use encryption to create a secure tunnel between remote users or branch offices and the internal network, protecting data transmission over untrusted networks like the Internet.

By implementing a firewall, organizations can establish a secure perimeter for their networks, safeguarding against unauthorized access, data breaches, and network attacks. Firewalls are a critical component of network security, providing an essential layer of defense to protect sensitive information and maintain the integrity and confidentiality of network communications.

**Wired and Wireless Networking**

Wired and wireless networking refer to the methods used to connect devices in a network. Let's explore each of these types:

**Wired Networking**: In wired networking, devices are connected using physical cables. The most common type of wired network uses Ethernet cables, such as Category 5e (Cat 5e) or Category 6 (Cat 6) cables. These cables connect devices like computers, routers, switches, and servers to form a network. Wired networks offer stable and reliable connections with high data transfer speeds, making them suitable for applications that require consistent and fast communication, such as large file transfers, online gaming, and video streaming.

**Wireless Networking**: Wireless networking eliminates the need for physical cables by using radio waves to transmit data between devices. The most common wireless networking standard is Wi-Fi (Wireless Fidelity), which allows devices to connect to a network without a direct wired connection. Wi-Fi networks are widely used in homes, offices, cafes, and other public spaces. Wireless networks provide mobility and flexibility, allowing devices to connect and communicate without the constraint of physical cables. However, wireless connections can be affected by factors like signal interference, distance limitations, and obstacles.

It's worth noting that many modern networks use a combination of wired and wireless connections to optimize performance and convenience. For example, a typical home network may have wired connections for devices that require a stable connection, such as desktop computers and gaming consoles, while using Wi-Fi for laptops, smartphones, and other portable devices.

Ultimately, the choice between wired and wireless networking depends on factors like the specific requirements of the network, the desired level of mobility, the environment, and the available infrastructure.

**IPV4 and IPV6**

IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6) are two versions of the Internet Protocol, which is the foundational protocol used to identify and communicate with devices on a network. Here's an overview of IPv4 and IPv6:

**IPv4**: IPv4 is the older and most widely used version of the Internet Protocol. It uses a 32-bit addressing system and supports approximately 4.3 billion unique IP addresses. An IP address is a unique identifier assigned to each device connected to a network, allowing devices to send and receive data over the internet. The IPv4 address format consists of four sets of numbers separated by periods, such as 192.168.0.1.

However, with the rapid growth of the internet and the proliferation of connected devices, the available pool of IPv4 addresses has been exhausted, leading to the need for a new version of the Internet Protocol.

**IPv6**: IPv6 was developed to address the limitations of IPv4 and provide a significantly larger address space. It uses a 128-bit addressing system, allowing for approximately 340 undecillion unique IP addresses. The IPv6 address format consists of eight groups of four hexadecimal digits separated by colons, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

In addition to the expanded address space, IPv6 offers other improvements, including enhanced security, simplified network configuration, and better support for emerging technologies and devices, such as Internet of Things (IoT) devices.

While IPv6 has been available for many years, its adoption has been relatively slow. This is due to the need for infrastructure upgrades, compatibility issues with older systems designed for IPv4, and the coexistence of both protocols during the transition period.

To ensure a smooth transition, many networks and devices now support both IPv4 and IPv6. This allows for communication between devices using either protocol. Transition mechanisms, such as dual-stack (supporting both IPv4 and IPv6), tunnelling, and translation, are employed to facilitate interoperability between the two protocols.

In summary, IPv4 and IPv6 are two versions of the Internet Protocol. IPv4 is the older and more widely used version, while IPv6 is the newer version that offers a larger address space and improved features to accommodate the expanding requirements of the internet and connected devices.

**Wi-Fi**

Wi-Fi, short for "Wireless Fidelity," is a wireless networking technology that allows devices to connect and communicate with each other and access the internet without the need for physical cables. It utilizes radio waves to transmit data between devices within a certain range.

Here's how Wi-Fi generally works:

1. **Wi-Fi Network**: A Wi-Fi network consists of two main components: a wireless router and wireless devices. The router acts as the central point of communication, transmitting and receiving data to and from connected devices. The devices, such as laptops, smartphones, tablets, and smart home devices, have Wi-Fi capabilities and can connect to the router wirelessly.
2. **Wireless Access Point**: The wireless router serves as a wireless access point (WAP) in a Wi-Fi network. It converts data from the wired connection to a wireless signal that devices can receive. The WAP broadcasts the signal using a specific radio frequency (2.4 GHz or 5 GHz) and employs various Wi-Fi standards (such as 802.11ac or 802.11n) to transmit the data.
3. **Wi-Fi Signal and Range**: The Wi-Fi signal travels through the air in all directions from the router. The range of a Wi-Fi network depends on factors like the router's power, antenna design, physical obstructions, and environmental conditions. Typically, Wi-Fi signals can cover a range of tens to hundreds of meters. Within the coverage area, devices can connect to the Wi-Fi network and communicate with each other and the internet.
4. **Wi-Fi Authentication and Encryption**: To access a Wi-Fi network, devices must go through an authentication process. This usually involves entering a pre-shared key (password) or other security credentials to establish a secure connection. Wi-Fi networks also employ encryption protocols (such as WPA2 or WPA3) to protect data transmitted over the network from unauthorized access.

Wi-Fi technology has become widely adopted and is commonly found in homes, offices, public spaces, and many other environments. It offers the convenience of wireless connectivity, allowing users to connect multiple devices simultaneously, roam within the coverage area, and access the internet without physical restrictions.

It's important to note that Wi-Fi is just one method of wireless communication, and there are other wireless technologies, such as Bluetooth, Zigbee, and cellular networks, that serve different purposes and have their own unique characteristics.

[Cyber Security Tutorial](https://www.geeksforgeeks.org/cyber-security-tutorial/)

Cybersecurity, also known as computer security or information security, refers to the practice of protecting computer systems, networks, and data from unauthorized access, damage, theft, disruption, or any other form of cyber threats. With the increasing reliance on technology and interconnectedness, cybersecurity has become crucial in safeguarding sensitive information and maintaining the integrity, confidentiality, and availability of digital assets. It involves a combination of technologies, processes, and practices to prevent, detect, respond to, and recover from cybersecurity incidents.

Key elements of cybersecurity include:

1. Risk Assessment: Identifying and assessing potential risks and vulnerabilities to computer systems and data and determining the potential impact of security breaches.
2. Security Policies and Procedures: Developing and implementing security policies, procedures, and guidelines that define acceptable behaviour, access controls, password policies, and incident response plans.
3. Access Control and Authentication: Implementing mechanisms to control and manage user access to systems and data, including the use of strong passwords, multi-factor authentication, and role-based access controls.
4. Encryption: Utilizing encryption techniques to protect sensitive data from unauthorized access or interception, both during storage and transmission.
5. Network Security: Implementing firewalls, intrusion detection and prevention systems, and network monitoring tools to secure networks and detect potential threats or attacks.
6. Malware Protection: Deploying antivirus software, anti-malware tools, and other security measures to detect and prevent malicious software such as viruses, worms, ransomware, and spyware.
7. Incident Detection and Response: Monitoring networks and systems for suspicious activities, promptly detecting cybersecurity incidents, and responding effectively to mitigate the impact and prevent further damage.
8. Security Awareness and Training: Educating employees and users about cybersecurity best practices, potential threats, and social engineering techniques to promote a security-conscious culture.
9. Vulnerability Management: Regularly scanning systems and applications for vulnerabilities and applying patches and updates to address those vulnerabilities.
10. Data Backup and Recovery: Implementing regular data backup procedures and disaster recovery plans to ensure the availability and integrity of data in the event of a security incident or system failure.

Cybersecurity is a continuous and evolving process, as new threats and vulnerabilities emerge regularly. It requires a comprehensive and multi-layered approach to protect against a wide range of cyber threats, including unauthorized access, data breaches, phishing attacks, malware infections, and social engineering attacks. Organizations and individuals alike must remain vigilant, keep their systems up to date, and follow best practices to mitigate risks and protect sensitive information in the digital landscape.

## Introduction:

* [OSI Security Architecture](https://www.geeksforgeeks.org/osi-security-architecture/)
* [Security Attacks [active and passive]](https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/)
* [Security Services](https://www.geeksforgeeks.org/types-of-security-mechanism/)
* [Models for Network Security](https://www.geeksforgeeks.org/a-model-for-network-security/)

## Cyber Technology:

* [Networking](https://www.geeksforgeeks.org/basics-of-wi-fi/#:~:text=Access%20Point(AP)%20is%20a,wireless%20devices%20simultaneously%20to%20internet.&text=BSS%20is%20the%20basic%20building,base%20station%20called%20Access%20Point.)
* [Wireless LAN Basics](https://www.geeksforgeeks.org/basics-of-wi-fi/#:~:text=Access%20Point(AP)%20is%20a,wireless%20devices%20simultaneously%20to%20internet.&text=BSS%20is%20the%20basic%20building,base%20station%20called%20Access%20Point.)
* [Web Basics](https://www.geeksforgeeks.org/the-internet-and-the-web/)
* [Website](https://www.geeksforgeeks.org/what-is-a-website/#:~:text=A%20website%20is%20a%20collection,HTML(HyperText%20Markup%20Language).&text=Such%20computers%20are%20known%20as,a%20common%20interface%20and%20design.)
* [Information Security Principles](https://www.geeksforgeeks.org/cryptography-and-network-security-principles/)
* [Cryptography](https://www.geeksforgeeks.org/cryptography-introduction/%20https:/www.geeksforgeeks.org/cryptography-and-its-types/)
* [Public Key Infrastructure](https://www.geeksforgeeks.org/public-key-infrastructure/)
* [Electronic Signature](https://www.geeksforgeeks.org/what-is-electronic-signature/)
* [Access Management](https://www.geeksforgeeks.org/identity-and-access-management/)
* [User Access Management](https://www.geeksforgeeks.org/identity-and-access-management-iam-in-cyber-security-roles/)
* [Cloud Computing](https://www.geeksforgeeks.org/cloud-computing/)