**Module - 1 (Computer Basics)**

**5. Networking**

# Introduction To Computer Networks

Modern world scenario is ever changing. Data Communication and network have changed the way business and other daily affair works. Now, they highly rely on computer networks and internetwork.

A set of devices often mentioned as nodes connected by media link is called a Network.

A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called **Communication channels**.

Computer network is a telecommunication channel using which we can share data with other coomputers or devices, connected to the same network. It is also called Data Network. The best example of computer network is Internet.

Computer network does not mean a system with one Control Unit connected to multiple other systems as its slave. That is Distributed system, not Computer Network.

A network must be able to meet certain criterias, these are mentioned below:

1. Performance
2. Reliability
3. Scalability

### Computer Networks: Performance

It can be measured in the following ways:

* **Transit time :**It is the time taken to travel a message from one device to another.
* **Response time :**It is defined as the time elapsed between enquiry and response.

Other ways to measure performance are :

1. Efficiency of software
2. Number of users
3. Capability of connected hardware

### Computer Networks: Reliability

It decides the frequency at which network failure take place. More the failures are, less is the network's reliability.

### Computer Networks: Security

It refers to the protection of data from any unauthorised user or access. While travelling through network, data passes many layers of network, and data can be traced if attempted. Hence security is also a very important characteristic for Networks.

## Properties of a Good Network

1. **Interpersonal Communication:** We can communicate with each other efficiently and easily. Example: emails, chat rooms, video conferencing etc, all of these are possible because of computer networks.
2. **Resources can be shared:**We can share physical resources by making them available on a network such as printers, scanners etc.
3. **Sharing files, data:**Authorised users are allowed to share the files on the network.

### Components of Data Communication

1. **Message:**It is the information to be delivered.
2. **Sender:**Sender is the person who is sending the message.
3. **Receiver:**Receiver is the person to whom the message is being sent to.
4. **Medium:**It is the medium through which the message is sent. For example: A Modem.
5. **Protocol:**These are some set of rules which govern data communication.

# Computer Network Components

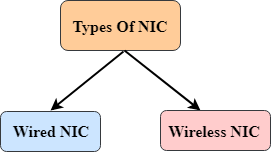
Computer network components are the major parts which are needed to install the software. Some important network components are **NIC**, **switch**, **cable**, **hub**, **router**, and **modem**. Depending on the type of network that we need to install, some network components can also be removed. For example, the wireless network does not require a cable.

Following are the major components required to install a network:

## NIC

* NIC stands for network interface card.
* NIC is a hardware component used to connect a computer with another computer onto a network
* It can support a transfer rate of 10,100 to 1000 Mb/s.
* The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).

### There are two types of NIC:



1. Wired NIC
2. Wireless NIC

**Wired NIC:** The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data.

**Wireless NIC:** The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC.

## Hub

A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.

The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

## Switch

A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

## Router

* A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
* A router works in a **Layer 3 (Network layer)** of the OSI Reference model.
* A router forwards the packet based on the information available in the routing table.
* It determines the best path from the available paths for the transmission of the packet.

### Advantages Of Router:

* **Security:** The information which is transmitted to the network will traverse the entire cable, but the only specified device which has been addressed can read the data.
* **Reliability:** If the server has stopped functioning, the network goes down, but no other networks are affected that are served by the router.
* **Performance:** Router enhances the overall performance of the network. Suppose there are 24 workstations in a network generates a same amount of traffic. This increases the traffic load on the network. Router splits the single network into two networks of 12 workstations each, reduces the traffic load by half.
* **Network range**

## Modem

* A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
* A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.
* It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

Based on the differences in speed and transmission rate, a modem can be classified in the following categories:

* Standard PC modem or Dial-up modem
* Cellular Modem
* Cable modem

## Cables and Connectors

Cable is a transmission media used for transmitting a signal.

There are three types of cables used in transmission:

* Twisted pair cable
* Coaxial cable
* Fibre-optic cable

# Computer Network Types

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



* LAN(Local Area Network)
* PAN(Personal Area Network)
* MAN(Metropolitan Area Network)
* WAN(Wide Area Network)

## LAN(Local Area Network)

* Local Area Network is a group of computers connected to each other in a small area such as building, office.
* LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
* It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
* The data is transferred at an extremely faster rate in Local Area Network.
* Local Area Network provides higher security.



## PAN(Personal Area Network)

* Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
* Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
* **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
* Personal Area Network covers an area of **30 feet**.
* Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.



**There are two types of Personal Area Network:**



* Wired Personal Area Network
* Wireless Personal Area Network

**Wireless Personal Area Network:** Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

**Wired Personal Area Network:** Wired Personal Area Network is created by using the USB.

### Examples Of Personal Area Network:

* **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.
* **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.
* **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

## MAN(Metropolitan Area Network)

* A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
* Government agencies use MAN to connect to the citizens and private industries.
* In MAN, various LANs are connected to each other through a telephone exchange line.
* The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
* It has a higher range than Local Area Network(LAN).



### Uses Of Metropolitan Area Network:

* MAN is used in communication between the banks in a city.
* It can be used in an Airline Reservation.
* It can be used in a college within a city.
* It can also be used for communication in the military.

## WAN(Wide Area Network)

* A Wide Area Network is a network that extends over a large geographical area such as states or countries.
* A Wide Area Network is quite bigger network than the LAN.
* A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
* The internet is one of the biggest WAN in the world.
* A Wide Area Network is widely used in the field of Business, government, and education.



### Examples Of Wide Area Network:

* **Mobile Broadband:** A 4G network is widely used across a region or country.
* **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
* **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

### Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

* **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
* **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
* **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
* **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
* **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
* **Global business:** We can do the business over the internet globally.
* **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

### Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

* **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
* **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
* **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
* **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

## Internetwork

* An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as **internetworking**.
* An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.
* An internetworking uses the **internet protocol**.
* The reference model used for internetworking is **Open System Interconnection(OSI)**.

## Types Of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it must have one connection to the external network.

2. **Intranet:** An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

## Intranet advantages:

* **Communication:** It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.
* **Time-saving:** Information on the intranet is shared in real time, so it is time-saving.
* **Collaboration:** Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.
* **Platform independency:** It is a neutral architecture as the computer can be connected to another device with different architecture.
* **Cost effective:** People can see the data and documents by using the browser and distributes the duplicate copies over the intranet. This leads to a reduction in the cost.

# Uses of Computer Networks

Had it not been of high importance, nobody would have bothered connecting computers over a network. Let's start exploring the uses of Computer Networks with some traditional usecases at companies and for individuals and then move on to the recent developments in the area of mobile users and home networking.

## Computer Networks: Business Applications

Following are some business applications of computer networks:

#### 1. Resource Sharing:

The goal is to make all programs, equipments(like printers etc), and especially data, available to anyone on the network without regard to the physical location of the resource and the user.

#### 2. Server-Client model:

One can imagine a company's information system as consisting of one or more databases and some employees who need to access it remotely. In this model, the data is stored on powerful computers called **Servers**. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simple machines, called **Clients**, on their desks, using which they access remote data.

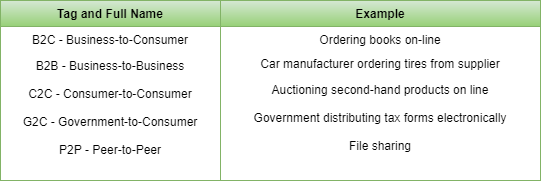
#### 3. Communication Medium:

A computer network can provide a powerful communication medium among employees. Virtually every company that has two or more computers now has e-mail (electronic mail), which employees generally use for a great deal of daily communication

#### 4. eCommerce:

A goal that is starting to become more important in businesses is doing business with consumers over the Internet. Airlines, bookstores and music vendors have discovered that many customers like the convenience of shopping from home. This sector is expected to grow quickly in the future.

The most popular forms are listed in the below figure:



## Computer Networks: Home Applications

Some of the most important uses of the Internet for home users are as follows:

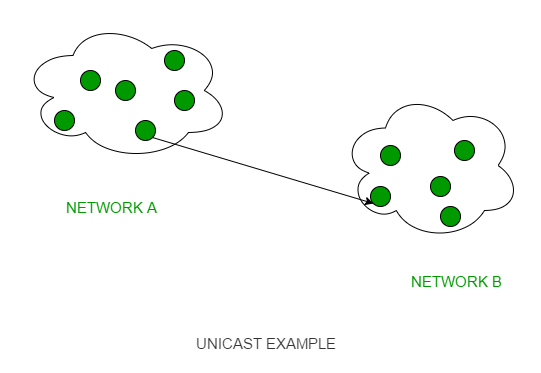
* **Access to remote information**
* **Person-to-person communication**
* **Interactive entertainment**
* **Electronic commerce**

# Difference between Unicast, Broadcast and Multicast in Computer Network

The **cast** term here signifies some data(stream of packets) is being transmitted to the recipient(s) from client(s) side over the communication channel that help them to communicate. Let’s see some of the “cast” concepts that are prevailing in the computer networks field.

### 1. Unicast –

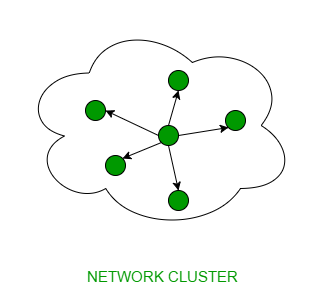
This type of information transfer is useful when there is a participation of single sender and single recipient. So, in short you can term it as a one-to-one transmission. For example, a device having IP address 10.1.2.0 in a network wants to send the traffic stream(data packets) to the device with IP address 20.12.4.2 in the other network,then unicast comes into picture. This is the most common form of data transfer over the networks.



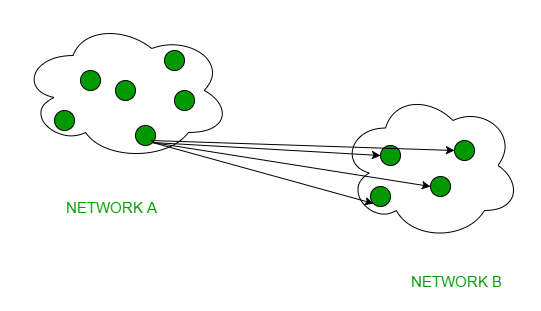
### 2. Broadcast –

Broadcasting transfer (one-to-all) techniques can be classified into two types :

* **Limited Broadcasting –**  
  Suppose you have to send stream of packets to all the devices over the network that you reside, this broadcasting comes handy. For this to achieve,it will append 255.255.255.255 (all the 32 bits of IP address set to 1) called as **Limited Broadcast Address** in the destination address of the datagram (packet) header which is reserved for information tranfer to all the recipients from a single client (sender) over the network.



* **Direct Broadcasting –**  
  This is useful when a device in one network wants to transfer packet stream to all the devices over the other network.This is achieved by translating all the Host ID part bits of the destination address to 1,referred as **Direct Broadcast Address** in the datagram header for information transfer.



This mode is mainly utilized by television networks for video and audio distribution.  
One important protocol of this class in Computer Networks is [Address Resolution Protocol (ARP)](https://www.geeksforgeeks.org/computer-network-arp-works/) that is used for resolving IP address into physical address which is necessary for underlying communication.

### 3. Multicast –

In multicasting, one/more senders and one/more recipients participate in data transfer traffic. In this method traffic recline between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast lets server’s direct single copies of data streams that are then simulated and routed to hosts that request it. IP multicast requires support of some other protocols like **IGMP (Internet Group Management Protocol), Multicast routing** for its working. Also in Classful IP addressing **Class D** is reserved for multicast groups.

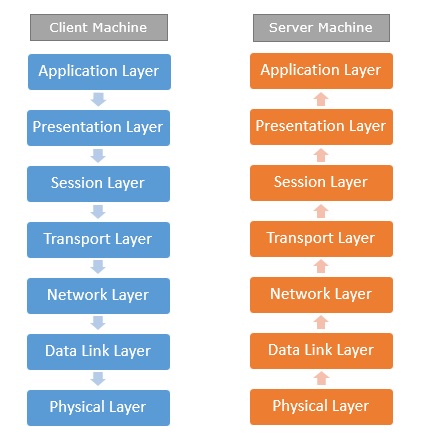
**Network Protocols** are a set of rules governing exchange of information in an easy, reliable and secure way. Before we discuss the most common protocols used to transmit and receive data over a network, we need to understand how a network is logically organized or designed. The most popular model used to establish open communication between two systems is the **Open Systems Interface (OSI) model** proposed by ISO.

## OSI Model

OSI model is not a **network architecture** because it does not specify the exact services and protocols for each layer. It simply tells what each layer should do by defining its input and output data. It is up to network architects to implement the layers according to their needs and resources available.

These are the seven layers of the OSI model −

* **Physical layer** −It is the first layer that physically connects the two systems that need to communicate. It transmits data in bits and manages simplex or duplex transmission by modem. It also manages Network Interface Card’s hardware interface to the network, like cabling, cable terminators, topography, voltage levels, etc.
* **Data link layer** − It is the firmware layer of Network Interface Card. It assembles datagrams into frames and adds start and stop flags to each frame. It also resolves problems caused by damaged, lost or duplicate frames.
* **Network layer** − It is concerned with routing, switching and controlling flow of information between the workstations. It also breaks down transport layer datagrams into smaller datagrams.
* **Transport layer** − Till the session layer, file is in its own form. Transport layer breaks it down into data frames, provides error checking at network segment level and prevents a fast host from overrunning a slower one. Transport layer isolates the upper layers from network hardware.
* **Session layer** − This layer is responsible for establishing a session between two workstations that want to exchange data.
* **Presentation layer** − This layer is concerned with correct representation of data, i.e. syntax and semantics of information. It controls file level security and is also responsible for converting data to network standards.
* **Application layer** − It is the topmost layer of the network that is responsible for sending application requests by the user to the lower levels. Typical applications include file transfer, E-mail, remote logon, data entry, etc.



It is not necessary for every network to have all the layers. For example, network layer is not there in broadcast networks.

When a system wants to share data with another workstation or send a request over the network, it is received by the application layer. Data then proceeds to lower layers after processing till it reaches the physical layer.

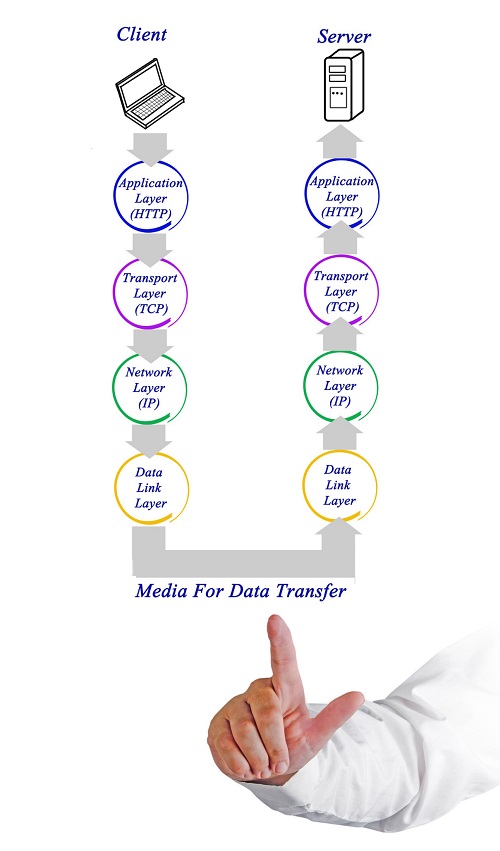
At the physical layer, the data is actually transferred and received by the physical layer of the destination workstation. There, the data proceeds to upper layers after processing till it reaches application layer.

At the application layer, data or request is shared with the workstation. So each layer has opposite functions for source and destination workstations. For example, data link layer of the source workstation adds start and stop flags to the frames but the same layer of the destination workstation will remove the start and stop flags from the frames.

Let us now see some of the protocols used by different layers to accomplish user requests.

## TCP/IP

TCP/IP stands for **Transmission Control Protocol/Internet Protocol**. TCP/IP is a set of layered protocols used for communication over the Internet. The communication model of this suite is client-server model. A computer that sends a request is the client and a computer to which the request is sent is the server.



TCP/IP has four layers −

* **Application layer** − Application layer protocols like HTTP and FTP are used.
* **Transport layer** − Data is transmitted in form of datagrams using the Transmission Control Protocol (TCP). TCP is responsible for breaking up data at the client side and then reassembling it on the server side.
* **Network layer** − Network layer connection is established using Internet Protocol (IP) at the network layer. Every machine connected to the Internet is assigned an address called IP address by the protocol to easily identify source and destination machines.
* **Data link layer** − Actual data transmission in bits occurs at the data link layer using the destination address provided by network layer.

TCP/IP is widely used in many communication networks other than the Internet.

## FTP

As we have seen, the need for network came up primarily to facilitate sharing of files between researchers. And to this day, file transfer remains one of the most used facilities.The protocol that handles these requests is **File Transfer Protocol** or **FTP**.

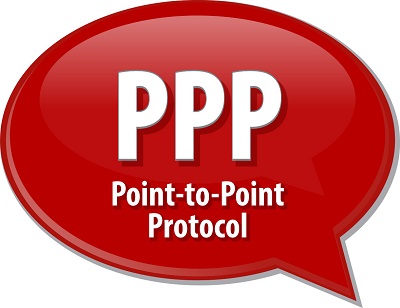


Using FTP to transfer files is helpful in these ways −

* Easily transfers files between two different networks
* Can resume file transfer sessions even if connection is dropped, if protocol is configure appropriately
* Enables collaboration between geographically separated teams

## PPP

Point to Point Protocol or PPP is a data link layer protocol that enables transmission of TCP/IP traffic over serial connection, like telephone line.



To do this, PPP defines these three things −

* A framing method to clearly define end of one frame and start of another, incorporating errors detection as well.
* Link control protocol (LCP) for bringing communication lines up, authenticating and bringing them down when no longer needed.
* Network control protocol (NCP) for each network layer protocol supported by other networks.

Using PPP, home users can avail Internet connection over telephone lines.

Difference between MAC Address and IP Address

Both [MAC Address](https://www.geeksforgeeks.org/computer-network-introduction-mac-address/) and [IP Address](https://www.geeksforgeeks.org/ip-addressing-introduction-and-classful-addressing/) are used to uniquely defines a device on the internet. NIC Card’s Manufacturer provides the MAC Address, on the other hand Internet Service Provider provides IP Address.

The main difference between MAC and IP address is that, MAC Address is used to ensure the physical address of computer. It uniquely identifies the devices on a network. While IP address are used to uniquely identifies the connection of network with that device take part in a network.

Let’s see the difference between MAC Address and IP Address:

|  |  |  |
| --- | --- | --- |
| **S.NO** | **MAC ADDRESS** | **IP ADDRESS** |
| 1. | MAC Address stands for Media Access Control Address. | IP Address stands for Internet Protocol Address. |
| 2. | MAC Address is a six byte hexadecimal address. | IP Address is either four byte (IPv4) or six byte (IPv6) address. |
| 3. | A device attached with MAC Address can retrieve by ARP protocol. | A device attached with IP Address can retrieve by RARP protocol. |
| 4. | NIC Card’s Manufacturer provides the MAC Address. | Internet Service Provider provides IP Address. |
| 5. | MAC Address is used to ensure the physical address of computer. | IP Address is the logical address of the computer. |

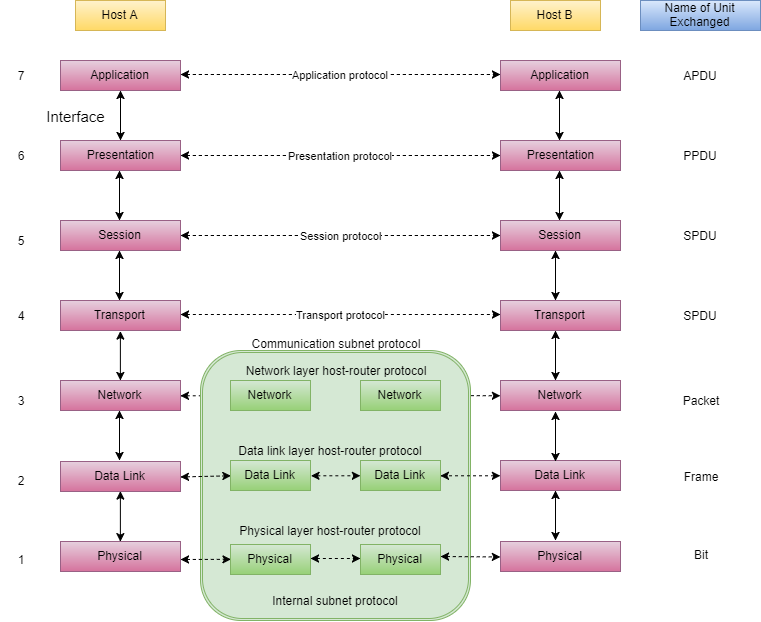
The OSI Model - Features, Principles and Layers

There are n numbers of users who use computer network and are located over the world. So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other ISO has developed a standard. ISO stands for **International organization of Standardization**. This is called a model for **Open System Interconnection** (OSI) and is commonly known as OSI model.

The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system. They are:

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Datalink Layer
7. Physical Layer

Below we have the complete representation of the OSI model, showcasing all the layers and how they communicate with each other.



## Functions of Different Layers

Following are the functions performed by each layer of the OSI model. This is just an introduction, we will cover each layer in details in the coming tutorials.

### OSI Model Layer 1: The Physical Layer

1. [Physical Layer](https://www.studytonight.com/computer-networks/osi-model-physical-layer) is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.

### OSI Model Layer 2: Data Link Layer

1. [Data link layer](https://www.studytonight.com/computer-networks/osi-model-datalink-layer) synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
3. Transmitting and receiving data frames sequentially is managed by this layer.
4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

### OSI Model Layer 3: The Network Layer

1. [Network Layer](https://www.studytonight.com/computer-networks/osi-model-network-layer) routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

### OSI Model Layer 4: Transport Layer

1. [Transport Layer](https://www.studytonight.com/computer-networks/osi-model-transport-layer) decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
3. It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

### OSI Model Layer 5: The Session Layer

1. [Session Layer](https://www.studytonight.com/computer-networks/osi-model-session-layer) manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

### OSI Model Layer 6: The Presentation Layer

1. [Presentation Layer](https://www.studytonight.com/computer-networks/osi-model-presentation-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.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. It perfroms Data compression, Data encryption, Data conversion etc.

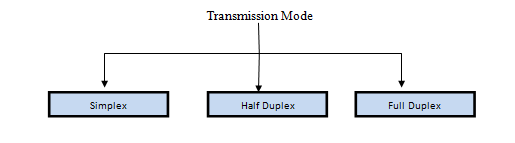
### OSI Model Layer 7: Application Layer

1. [Application Layer](https://www.studytonight.com/computer-networks/osi-model-application-layer) is the topmost layer.
2. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
3. This layer mainly holds application programs to act upon the received and to be sent data.

# Transmission Modes in Computer Networks

Transmission mode refers to the mechanism of transferring of data between two devices connected over a network. It is also called **Communication Mode**. These modes direct the direction of flow of information. There are three types of transmission modes. They are:

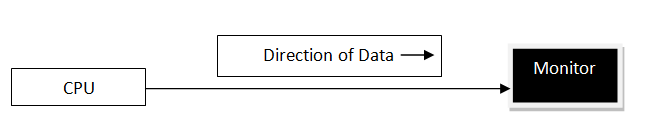
1. Simplex Mode
2. Half duplex Mode
3. Full duplex Mode



## SIMPLEX Mode

In this type of transmission mode, data can be sent only in one direction i.e. communication is unidirectional. We cannot send a message back to the sender. Unidirectional communication is done in Simplex Systems where we just need to send a command/signal, and do not expect any response back.

Examples of simplex Mode are loudspeakers, television broadcasting, television and remote, keyboard and monitor etc.

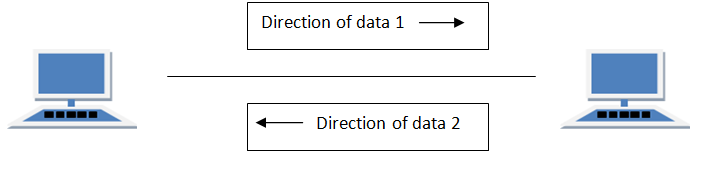


## HALF DUPLEX Mode

Half-duplex data transmission means that data can be transmitted in both directions on a signal carrier, but not at the same time.

**For example**, on a local area network using a technology that has half-duplex transmission, one workstation can send data on the line and then immediately receive data on the line from the same direction in which data was just transmitted. Hence half-duplex transmission implies a bidirectional line (one that can carry data in both directions) but data can be sent in only one direction at a time.

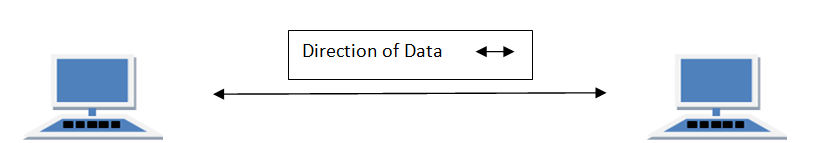
Example of half duplex is a walkie- talkie in which message is sent one at a time but messages are sent in both the directions.



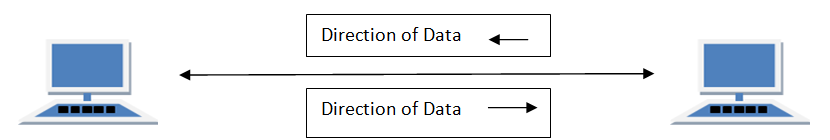
## FULL DUPLEX Mode

In full duplex system we can send data in both the directions as it is bidirectional at the same time in other words, data can be sent in both directions simultaneously.

Example of Full Duplex is a Telephone Network in which there is communication between two persons by a telephone line, using which both can talk and listen at the same time.



In full duplex system there can be two lines one for sending the data and the other for receiving data.

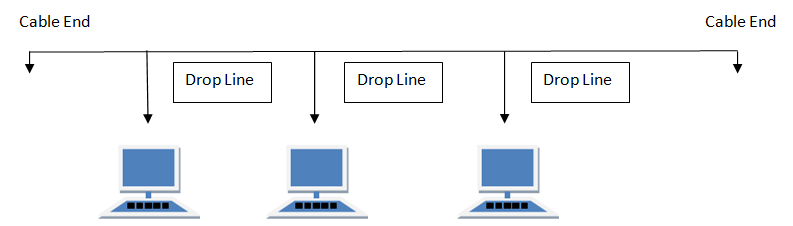


# Types of Network Topology

Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

## BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



#### Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

#### Advantages of Bus Topology

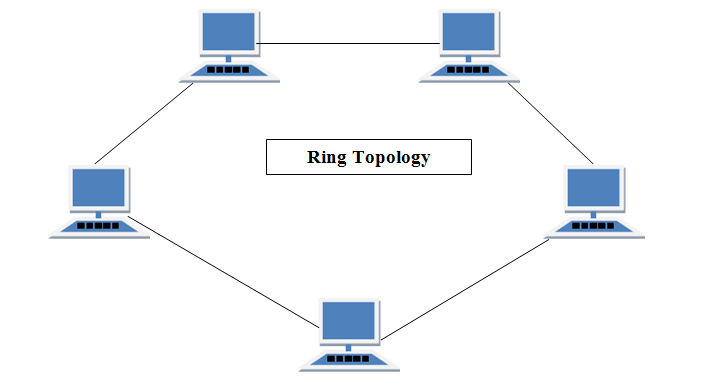
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

#### Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

## RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



#### Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

#### Advantages of Ring Topology

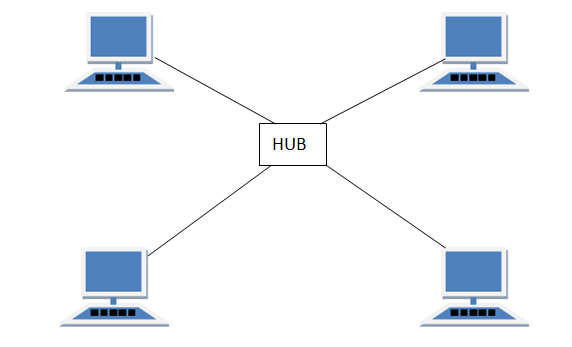
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

#### Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

## STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



#### Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

#### Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

#### Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

## MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

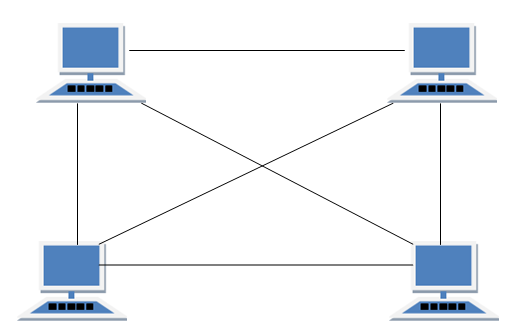
1. Routing
2. Flooding

### MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

### MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



#### Types of Mesh Topology

1. **Partial Mesh Topology :**In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :**Each and every nodes or devices are connected to each other.

#### Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

#### Advantages of Mesh Topology

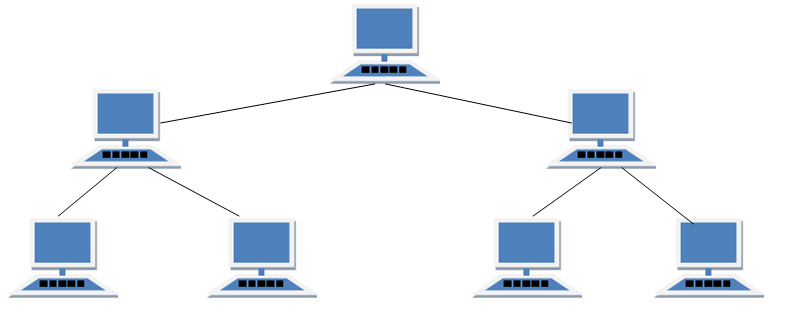
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

#### Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

## TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



#### Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

#### Advantages of Tree Topology

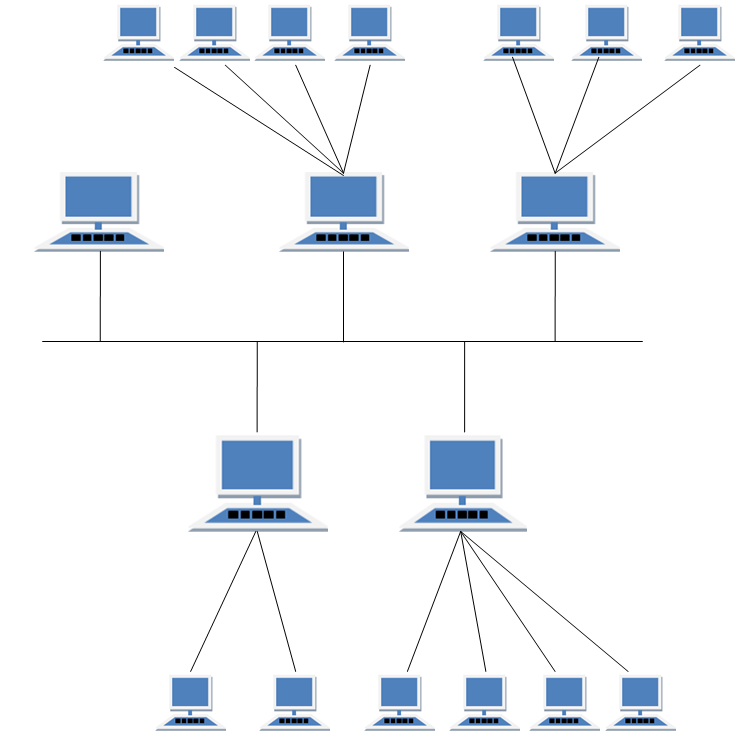
1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

#### Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

## HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



#### Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

#### Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

#### Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

## Introduction To Firewall

The concept of the firewall was introduced in order to secure the communication process between various networks.

A firewall is a software or a hardware device which examines the data from several networks and then either permits it or blocks it to communicate with your network and this process is governed by a set of predefined security guidelines.

In this tutorial, we will explore the various aspects of the Firewall and its applications.

**Definition:**

A firewall is a device or a combination of systems that supervises the flow of traffic between distinctive parts of the network. A firewall is used to guard the network against nasty people and prohibit their actions at predefined boundary levels.

A firewall is not only used to protect the system from exterior threats but the threat can be internal as well. Therefore we need protection at each level of the hierarchy of networking systems.

A good firewall should be sufficient enough to deal with both internal and external threats and be able to deal with malicious software such as worms from acquiring access to the network. It also provisions your system to stop forwarding unlawful data to another system.

**For Example**, firewall always exists between a private network and the Internet which is a public network thus filters packets coming in and out.

**Firewall as a barrier between the Internet and LAN**

Selecting a precise firewall is critical in building up a secure networking system.

Firewall provisions the security apparatus for allowing and restricting traffic, authentication, address translation and content security.

It ensures 365 \*24\*7 protection of network from hackers. It is a onetime investment for any organization and only needs timely updates to function properly. By deploying firewall there is no need of any panic in case of network attacks.

### Software Vs Hardware Firewall

**Basic Firewall Network Example**

Hardware firewall protects the entire network of an organization using it from external threats only. In case, if an employee of the organization is connected to the network via his personal laptop then he can’t avail the protection.

On the other hand, software firewall provision host-based security as the software is installed on each of the device connected to the network, thereby protecting the system from external as well as internal threats. It is most widely used by mobile users to digitally protect their handset from malicious attacks.

### Network Threats

**A list of Network threats are briefed below:**

* Worms, denial of service (DoS) and Trojan horses are few examples of network threats which are used to demolish the computer networking systems.
* Trojan horse virus is a kind of malware which performs an assigned task in the system. But actually, it was trying to illegally access the network resources. These viruses if injected in your system give the hacker’s the rights to hack your network.
* These are very dangerous viruses as they can even cause your PC to crash and can remotely modify or delete your crucial data from the system.
* Computer worms are a type of malware program. They consume the bandwidth and speed of the network to transmit copies of them to the other PCs of the network. They harm the computers by corrupting or modifying the database of the computer entirely.
* The worms are very dangerous as they can destroy the encrypted files and attach themselves with e-mail and thus can be transmitted in the network through the internet.

### Firewall Protection

In small networks, we can make each of our network device secured by ensuring that all the software patches are installed, unneeded services are disabled, and security software are properly installed within it.

In this situation, as also shown in the figure, the firewall software is mounted on each machine & server and configured in such a manner that only listed traffic can come in and out of the device. But this works efficiently in small-scale networks only.

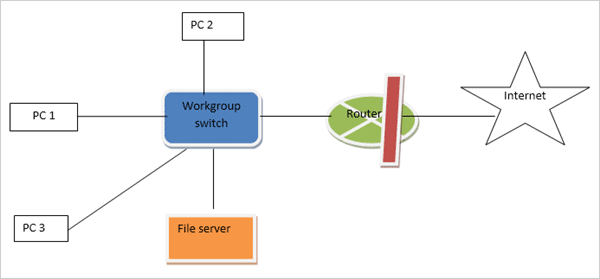
**Firewall Protection in Small Scale Network**

In a large-scale network, it is almost next to impossible to manually configure the firewall protection on each node.

The centralized security system is a solution to provide a secure network to big networks. With the help of an example, it is shown in the below figure that the firewall solution is imposed with the router itself, and it becomes simple to handle security policies. The policies of traffic come in and out into the device and can be handled solely by one device.

This makes the overall security system cost-effective.

**Firewall Protection in Big Networks**

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2018/07/Firewall-Protection-in-big-networks.png)

### Firewall and OSI Reference Model

A firewall system can work on five layers of OSI-ISO reference model. But most of them run at only four layers i.e. data-link layer, network layer, transport layer and application layers.

The number of layers envelops by a firewall is dependent upon the type of firewall used. Greater will be a count of layers it covers more efficient will be the firewall solution to deal with all kind of security concerns.

### Dealing with Internal Threats

Most of the attack on the network occurs from inside the system so to deal with it Firewall system should be capable of securing from internal threats also.

**Few kinds of internal threats are described below:**

**#1)** Malicious cyber attacks are the most common type of internal attack. The system administrator or any employee from the IT department who is having access to the network system can plant some virus to steal crucial network information or to damage the networking system.

The solution to deal with it is to monitor the activities of every employee and guard the internal network by using multiple layers of the password to each of the servers. The system can also be protected by giving access of system to least of the employees as possible.

**#2)** Any of the host computers of the internal network of the organization can download malicious internet content with lack of knowledge of downloading the virus also with it. Thus the host systems should have limited access to the internet. All unnecessary browsing should be blocked.

**#3)** Information leakage from any of the host PC through pen drives, hard disk or CD-ROM is also a network threat to the system. This can lead to crucial database leakage of the organization to the outer world or competitors. This can be controlled by disabling the USB ports of host device so that they can’t take out any data from the system.

### DMZ

A demilitarized zone (DMZ) is used by a majority of firewall systems to guard assets and resources. DMZ’s are deployed to give external users access to resources like e-mail server, DNS server and web page without uncovering the internal network. It behaves as a buffer in between distinctive segments in the network.

Each region in the firewall system is allocated a security level.

**For Example**, low, medium and high. Normally traffic flows from a higher level to a lower level. But for traffic to move from a lower to a higher level, a different set of filtering rules are deployed.

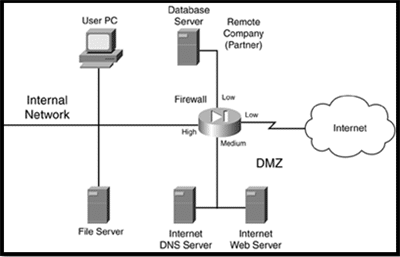
For permitting the traffic to move from a lower security level to a higher security level, one should be precise about kind of traffic permitted. By being precise we are unlocking firewall system only for that traffic which is essential, all another kind of traffic will be blocked by configuration.

A firewall is deployed to separate distinctive parts of the network.

**The various interfaces are as follows:**

* Link to the Internet, assigned with the lowest level of security.
* A link to DMZ assigned a medium security because of the presence of servers.
* A link to the organization, situated at the remote end, assigned a medium security.
* Highest security is assigned to the internal network.

**Firewall Protection with DMS**

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2018/07/Firewall-protection-with-DMZ.png)

**Rules assigned to the organization are:**

* High to low-level access is allowed
* Low to high-level access is not allowed
* Equivalent level access also not allowed

**By using the above set of rules, the traffic allowed to automatically flow through the firewall is:**

* Internal devices to DMZ, remote organization, and the internet.
* DMZ to the remote organization and the internet.

Any other kind of traffic flow is blocked. The benefit of such design is that since the internet and the remote organization are assigned the equivalent kind of security levels, traffic from the Internet not able to destine organization which itself enhances protection and organization will not be able to use the internet at free of cost( it saves money).

Another benefit is that it provides layered security thus if a hacker wants to hack the internal resources then it first has to hack the DMZ. Hacker’s task becomes tougher which in turn makes the system much more secure.

### Components of a Firewall System

**The building blocks of a good firewall system are as follows:**

* Perimeter router
* Firewall
* VPN
* IDS

#### #1) Perimeter Router

The main reason for using it is to provide a link to the public networking system like the internet, or to a distinctive organization. It performs the routing of data packets by following an appropriate routing protocol.

It also provisions the filtering of packets and addresses translations.

#### #2) Firewall

As discussed earlier also its main task is to provisions distinctive levels of security and supervises traffic among each level. Most of the firewall exists near the router to provide security from external threats but sometimes present in the internal network also to protect from internal attacks.

#### #3) VPN

Its function is to provisions a secured connection among two machines or networks or a machine and a network. This consist of encryption, authentication and, packet-reliability assurance. It provisions the secure remote access of the network, thereby connecting two WAN networks together on the same platform while not being physically connected.

#### #4) IDS

Its function is to identify, preclude, investigate and resolve the unauthorized attacks. A hacker can attack the network in various ways. It can execute a DoS attack or an attack from the back side of the network through some unauthorized access. An IDS solution should be smart enough to deal with these types of attacks.

**IDS solution**is of two kinds, network-based and host-based. A network-based IDS solution should be skilled in such a way whenever an attack is spotted, can access the firewall system and after logging into it can configure an efficient filter which can restrict the unwanted traffic.

A host-based IDS solution is a kind of software that runs on a host device such as a laptop or server, which spots the threat against that device only. IDS solution should inspect network threats closely and report them timely and should take necessary actions against the attacks.

### Component Placement

We have discussed few of the major building blocks of the firewall system. Now let’s discuss the placement of these components.

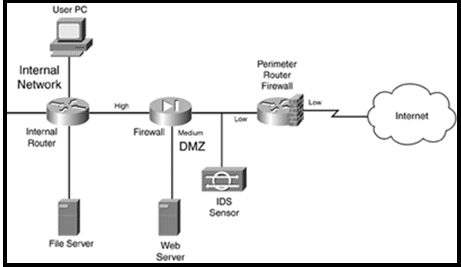
Below with the help of an Example, I am illustrating a design of the network. But it can’t be said completely that it is the overall secure network design because every design can have some constraints.

The perimeter router having fundamental filtering features are used when traffic penetrate the network. A IDS component is placed to identify attacks that the perimeter router was incapable to filter out.

The traffic thereby goes through the firewall. The firewall has initiate three levels of security, low for the Internet means external side, medium for DMZ and high for the internal network. The rule followed is to permit the traffic from the internet to web server only.

Rest of traffic flow from lower to the higher side is restricted, though, higher to lower traffic flow is allowed, so that the administrator residing on the internal network for logging onto the DMZ server.

**Overall Firewall System Design Example**

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2018/07/Overall-Firewall-System-Design-Example.png)

An internal router is also implemented in this design as to route the packets internally and perform filtering actions.

The advantage of this design is that it having three layers of security, the packet filtering perimeter router, IDS and the firewall.

The disadvantage of this set-up is that no IDS occurs in the internal network thus can’t easily prevent internal attacks.

**Important Designing Facts:**

* Packet-filtering firewall should be used at the boundary of the network to give enhanced security.
* Every server having exposure to a public network such as the Internet will be placed in DMZ. Servers having crucial data will be equipped with host-based firewall software within them. In addition to these on servers, all unwanted services should be disabled.
* If your network is having critical database server such as HLR server, IN, and SGSN which is used in mobile operations, then multiple DMZ will definitely be deployed.
* If external sources such as far end organization want to access your server placed in an internal network of security system then use VPN.
* For crucial internal sources, such as R&D or financial sources, IDS should be used to monitor and deal with internal attacks. By imposing levels of security separately, extra security can be provided to the internal network.
* For e-mail services, all outgoing emails should be pass through the DMZ e-mail server firstly and then some extra security software so that internal threats can be avoided.
* For incoming e-mail, in addition to DMZ server, antivirus, spam and host-based software should be installed and run on the server every time a mail enters the server.

### Firewall Administration and Management

Now we have chosen the building blocks of our firewall system. Now the time has come to configure the security rules onto a network system.

Command line interface (CLI) and graphic user interface (GUI) are used to configure firewall software. **For Example**, Cisco products support both kinds of configuration methods.

Nowadays in most of the networks, Security device manager (SDM) which is also a product of Cisco is used to configure routers, Firewall, and VPN attributes.

To implement a firewall system an efficient administration is very essential to run the process smoothly. The people managing the security system must be master in their work as there is no scope for human error.

Any type of configuration errors should be avoided. Every time when configuration updates will be done, the administrator must examine and double check the whole process so that leaving no scope for loopholes and hackers to attack it. The administrator should use a software tool to examine the alterations done.

Any major configuration changes in firewall systems can’t be directly applied to the ongoing big networks as if failed can lead to big loss to network and directly allowing unwanted traffic to enter the system. Thus firstly it should be performed in the lab and examine the outcomes if results are found ok then we can implement the changes in the live network.

### Firewall Categories

**Based on the filtering of traffic there are many categories of the firewall, some are explained below:**

#### #1) Packet Filtering Firewall

It is a kind of router which is having the ability to filter the few of the substance of the data packets. When using packet-filtering, the rules are classified on the firewall. These rules find out from the packets which traffic is permitted and which are not.

#### #2) Stateful Firewall

It is also called as dynamic packet filtering, it inspects the status of active connections and uses that data to find out which of the packets should be permitted through the firewall and which are not.

The firewall inspects the packet down to the application layer. By tracing the session data like IP address and port number of the data packet it can provide a much strong security to the network.

It also inspects both incoming and outgoing traffic thus hackers found it difficult to interfere in the network using this firewall.

#### #3) Proxy Firewall

These are also known as application gateway firewalls. The stateful firewall is unable to protect the system from HTTP based attacks. Therefore proxy firewall is introduced in the market.

It includes the features of stateful inspection plus having the capability of closely analyzing application layer protocols.

Thus it can monitor traffic from HTTP and FTP and find out the possibility of attacks. Thus firewall behaves as a proxy means client initiates a connection with the firewall and the firewall in return initiates a solo link with the server on the client’s side.

### Types of Firewall Software

The few of the most popular firewall software that the organizations use to protect their systems are mentioned below:

#### #1) Comodo Firewall

Virtual Internet browsing, to block unwanted pop-up ads, and customizing DNS servers are the common features of this Firewall. Virtual Kiosk is used to block some procedure and programs by absconding and penetrating the network.

In this firewall, apart from following the long process for defining ports and other programs to allow and block, any program can be allowed and blocked by just browsing for the program and clicking on the desired output.

Comodo killswitch is also an enhanced feature of this firewall which illustrates all ongoing processes and makes it very easy to block any unwanted program.

#### #2) AVS Firewall

It is very simple to implement. It guards your system against nasty registry amendments, pop-up windows, and unwanted advertisements. We can also modify the URL’s for ads anytime and can block them also.

It’s also having the feature of Parent control, which is a part of permitting access to a precise group of websites only.

It is used in Windows 8, 7, Vista and XP.

#### #3) Netdefender

Here we can easily outline the source and destination IP address, port number and protocol that are permitted and not permitted in the system. We can allow and block FTP for being deployed and restricted in any network.

It also has a port scanner, which can visualize which can be used for traffic flow.

#### #4) PeerBlock

Despite blocking individual class of programs defined in the computer it blocks the overall IP addresses class fall in particular category.

It deploys this feature by blocking both incoming and outgoing traffic by defining a set of IP addresses that are barred. Therefore the network or computer using that set of IP’s can’t access the network and also the internal network can’t send the outgoing traffic to those blocked programs.

#### #5) Windows Firewall

The most frequent firewall used by Windows 7 users is this firewall. It provisions the access and restriction of traffic and communication between networks or a network or a device by analyzing IP address and port number. It by default permits all outbound traffic but allows only those inbound traffic which is defined.

#### #6) Juniper Firewall

The juniper in itself a networking organization and design various types of routers and firewall filters also. In a live network like Mobile service providers uses Juniper made firewall to protect their network services from different types of threats.

They guard the network routers and extra incoming traffic and unreceptive attacks from external sources that can interrupt network services and handle which traffic to be forwarded from which of router interfaces.

It implements one input and one output firewall filter to each of the incoming and outgoing physical interfaces. This filters out the unwanted data packets following the rules defined at both incoming and outgoing interfaces.

According to default firewall configuration settings, which packets to be accepted and which to be discarded is decided.

### Conclusion

From the above description about various aspects of the firewall, we will come to a conclusion that to overcome the external and internal network attacks the concept of the firewall has been introduced.

The firewall can be hardware or software which by following a certain set of rules will guard our networking system from the virus and other types of malicious attacks.

We have also explored here the different categories of the firewall, components of the firewall, designing and implementation of a firewall, and then some of the famous firewall software we used to deploy in the networking industry.

Network Switching

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

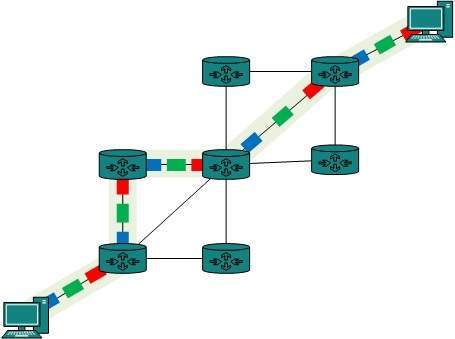
* **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
* **Connection Oriented:**  Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

## Circuit Switching

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching.There 'is a need of pre-specified route from which data will travels and no other data is permitted.In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.

Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:

* Establish a circuit
* Transfer the data
* Disconnect the circuit

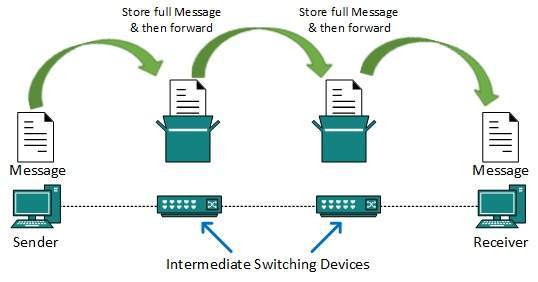


Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

## Message Switching

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.

A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.



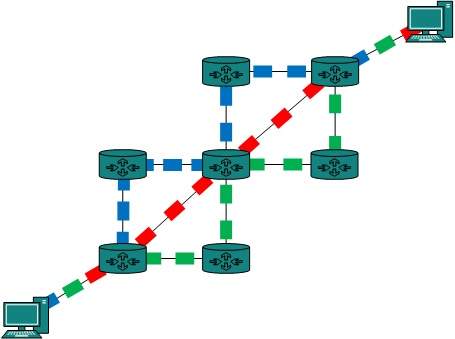
This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching. Message switching has the following drawbacks:

* Every switch in transit path needs enough storage to accommodate entire message.
* Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
* Message switching was not a solution for streaming media and real-time applications.

## Packet Switching

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.

It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches.



Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

**MODEM**

Modem is short for "Modulator-Demodulator." It is a [hardware](https://techterms.com/definition/hardware) component that allows a [computer](https://techterms.com/definition/computer) or another device, such as a [router](https://techterms.com/definition/router) or [switch](https://techterms.com/definition/switch), to connect to the Internet. It converts or "modulates" an [analog](https://techterms.com/definition/analog) signal from a telephone or cable wire to [digital](https://techterms.com/definition/digital) data (1s and 0s) that a computer can recognize. Similarly, it converts digital data from a computer or other device into an analog signal that can be sent over standard telephone lines.

The first modems were "[dial-up](https://techterms.com/definition/dialup)," meaning they had to dial a phone number to connect to an [ISP](https://techterms.com/definition/isp). These modems operated over standard analog phone lines and used the same frequencies as telephone calls, which limited their maximum [data transfer rate](https://techterms.com/definition/datatransferrate) to 56 [Kbps](https://techterms.com/definition/kbps). Dial-up modems also required full use of the local telephone line, meaning voice calls would interrupt the Internet connection.

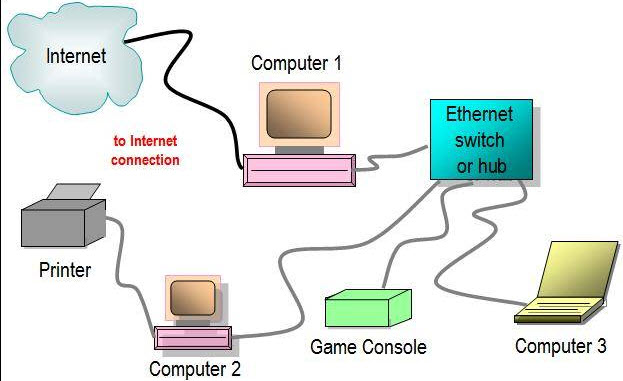
**Comparison in MODEM and Router**

| **Basis for comparison** | **Modem** | **Router** |
| --- | --- | --- |
| **Definition** | A Modem is a device which performs both modulation and demodulation of signals. | The router is a networking device which associates various networks with each other for LAN and WAN networks. |
| **Layer** | It works on the data-link layer of the ISO-OSI reference model and doesn’t have any inbuilt intelligence. | It works on the physical, data-link and network layer of the ISO-OSI reference model and maintains the routing table to forward and route the data packet to the desired destination path. |
| **Working Principle** | It acts as a modulator and demodulator. It modulates the digital signal of the computer or router to the analog signal of the telephone line so that easily understood by the telephone line when getting through it and performs the demodulation function at the other end by converting the analog signal which comes from the telephone line into a digital signal for the network device like PC. | It doesn’t perform any type of modulation and demodulation function, but it routes a data packet between source and destination end by following the shortest path and securely directs the data packet by following the routing table. The router permits various network devices to connect into the network. |
| **Purpose** | The modem plays a very vital role in the communication system as it is an essential part of the networking system for connecting any device to the ISP. The modem brings out the requested data from the ISP to the end device like a PC or router. If we need to connect only one computer to the Internet then the modem can do it, it doesn’t require the router. | It routes the data packets among the networking devices and the different networking systems. The router is one of the basic building blocks of the WAN communication system. |
| **Security** | It delivers the information as it is in the form it derives it from the ISP without checking any security threats as it is not smart enough to get it examined. Thus any threat can easily get access to the network through a modem. | The router uses a firewall to examine the incoming data packets and filters the unwanted data packets by using the firewall and other antivirus software. Thus it is difficult for the unwanted material to enter the network by means of the router. |
| **Placement** | It is placed between the telephone line and the PC or router.It provisions connectivity with both wireless or wired like optical fiber, telephone line medium. The connectivity is done by the Ethernet port available with the modem. It connects the ISP to the single PC for the home or office network connections. | It is placed between a modem and the network system. The network can be a set of computers or a set of computers and switches etc. The modem and router are physically connected with each other. Therefore the devices which are associated with a router can access the Internet via a modem. It doesn’t provide the direct connectivity with the ISP as it doesn’t work at the physical layer. It works at the network layer. The router has the Ethernet and gigabit ports to connect with the different network devices and other networking systems. The routers also have the Wi-Fi port for wireless connectivity. |

**Ethernet**

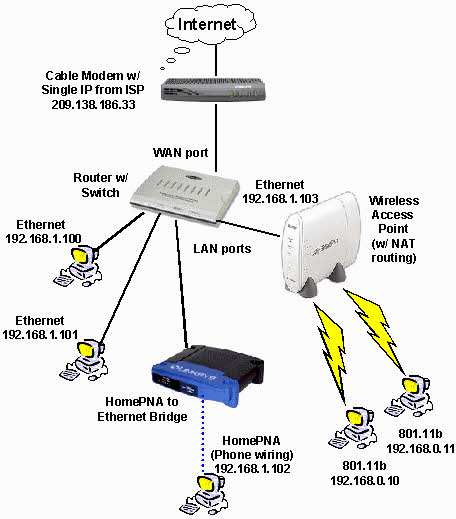
## Wired Ethernet Network

The Ethernet technology mainly works with the fiber optic cables that connect devices within a distance of 10 km. The Ethernet supports 10 Mbps.

[](https://www.elprocus.com/wp-content/uploads/2014/02/111.jpg)Ethernet communication

A computer network interface card (NIC) is installed in each computer, and is assigned to a unique address. An Ethernet cable runs from each NIC to the central switch or hub. The switch and hub act as a relay though they have significant differences in the manner in which they handle network traffic – receiving and directing packets of data across the LAN. Thus, Ethernet networking creates a communications system that allows sharing of data and resources including printers, fax machines and scanners.

## Wireless Ethernet

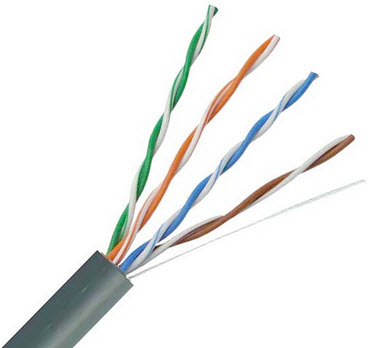
[](https://www.elprocus.com/wp-content/uploads/2014/02/29.jpg)Wireless Network

Ethernet networks can also be wireless. Rather than using Ethernet cable to connect the computers, wireless NICs use radio waves for two-way communication with a wireless switch or hub. It consists of Ethernet ports, wireless NICs, switches and hubs. [Wireless network technology](https://www.elprocus.com/how-does-wifi-work/" \t "_blank) can be more flexible to use, but also require extra care in configuring security.

### Types of Ethernet Networks

There are several types of Ethernet networks, such as Fast Ethernet, Gigabit Ethernet, and Switch Ethernet. A network is a group of two or more computer systems connected together.

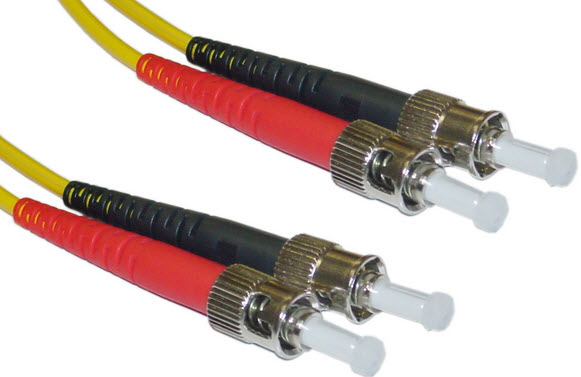
**1. Fast Ethernet**

[](https://www.elprocus.com/wp-content/uploads/2014/02/39.jpg)Twisted pair cable

The fast Ethernet is a type of Ethernet network that can transfer data at a rate of 100 Mbps using a twisted-pair cable or a fiber-optic cable. The older 10 Mbps Ethernet is still used, but such networks do not provide necessary bandwidth for some network-based video applications.

Fast Ethernet is based on the proven CSMA/CD Media Access Control (MAC) protocol, and uses existing 10BaseT cabling. Data can move from 10 Mbps to 100 Mbps without any protocol translation or changes to the application and networking software.

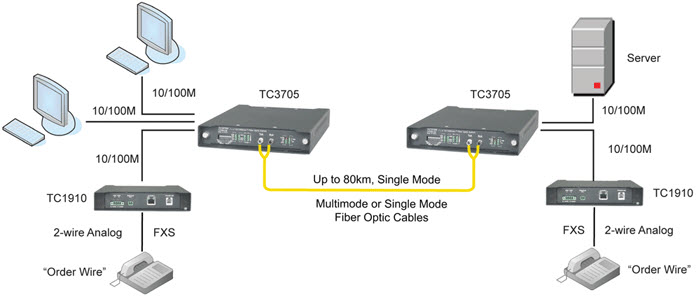
**2. Gigabit Ethernet**

[](https://www.elprocus.com/wp-content/uploads/2014/02/411.jpg)Optic fiber cable

The Gigabit Ethernet is a type of Ethernet network capable of transferring data at a rate of 1000 Mbps based on a twisted-pair or fiber optic cable, and it is very popular. The type of twisted-pair cables that support Gigabit Ethernet is Cat 5e cable, where all the four pairs of twisted wires of the cable are used to achieve high data transfer rates. The 10 Gigabit Ethernet is a latest generation Ethernet capable of transferring data at a rate of 10 Gbps using twisted-pair or fiber optic cable.

**3. Switch Ethernet**

Multiple network devices in a LAN require network equipments such as a network switch or hub. When using a network switch, a regular network cable is used instead of a crossover cable. The crossover cable consists of a transmission pair at one end and a receiving pair at the other end.

[](https://www.elprocus.com/wp-content/uploads/2014/02/58.jpg)Switch Ethernet

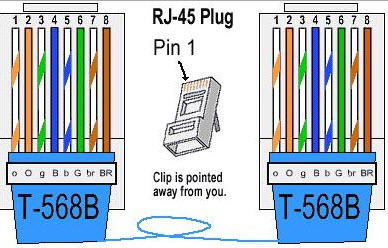
The network switch normally supports different data transfer rates. The most common data transfer rates include 10 Mbps – 100 Mbps for fast Ethernet, and 1000 Mbps – 10 Gbps for the latest Ethernet.

Switch Ethernet uses star topology, which is organized around a switch. The switch in a network uses a filtering and switching mechanism similar to the one used by the gateways, in which these techniques have been in use for a long time.

### Different Types of Ethernet Cables

Different variants of Ethernet technologies are designated according to the type and diameter of the cables used as given below:

* 10Base2: The cable used is a thin coaxial cable: thin Ethernet.
* 10Base5: The cable used is a thick coaxial cable: thick Ethernet.
* 10Base-T: The cable used is a twisted-pair (T means twisted pair) and the speed achieved is around 10 Mbps.
* 100Base-FX: Makes it possible to achieve a speed of 100 Mbps by using multimode fiber optic (F stands for Fiber).
* 100Base-TX: Similar to 10Base-T, but with a speed 10 times greater (100 Mbps).
* 1000Base-T: Uses a double-twisted pair of category 5 cables and allows a speed up to one Gigabit per second.
* 1000Base-SX: Based on multimode fiber optic uses a short wavelength signal (S stands for short) of 850 nanometers (770 to 860 nm).
* 1000Base-LX: Based on multimode fiber optic uses a long wavelength signal (L stands for long) of 1350 nm (1270 to 1355 nm). Ethernet is a widely used network technology because the cost of such a network is not very high.

[](https://www.elprocus.com/wp-content/uploads/2014/02/91.jpg)Types of Ethernet Cables

### Top Features of Ethernet controller

1. Includes 1st round “hop” to a Tier 1 provider
2. Provides wholesale pricing for all types of businesses
3. Connects directly to the carrier’s backbone
4. Offers Service Level Agreements with every connection
5. Provides low-cost bandwidth
6. Provides higher rates of data transfer
7. Offers ‘Plug and Play’ provisioning

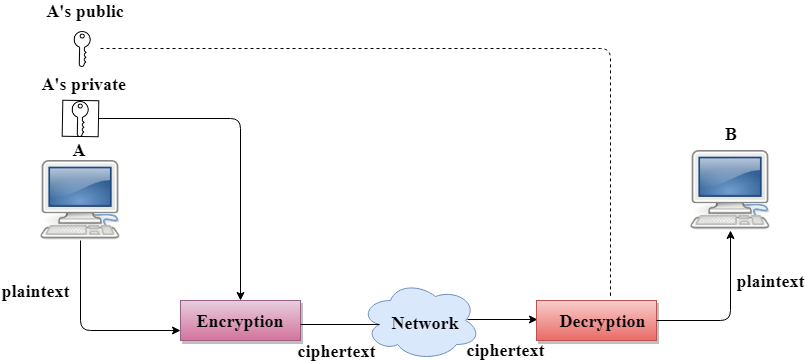
# Digital Signature

The Digital Signature is a technique which is used to validate the authenticity and integrity of the message. We know that there are four aspects of security: privacy, authentication, integrity, and non-repudiation. We have already discussed the first aspect of security and other three aspects can be achieved by using a digital signature.

The basic idea behind the Digital Signature is to sign a document. When we send a document electronically, we can also sign it. We can sign a document in two ways: to sign a whole document and to sign a digest.

## Signing the Whole Document

* In Digital Signature, a public key encryption technique is used to sign a document. However, the roles of a public key and private key are different here. The sender uses a private key to encrypt the message while the receiver uses the public key of the sender to decrypt the message.
* In Digital Signature, the private key is used for encryption while the public key is used for decryption.
* Digital Signature cannot be achieved by using secret key encryption.

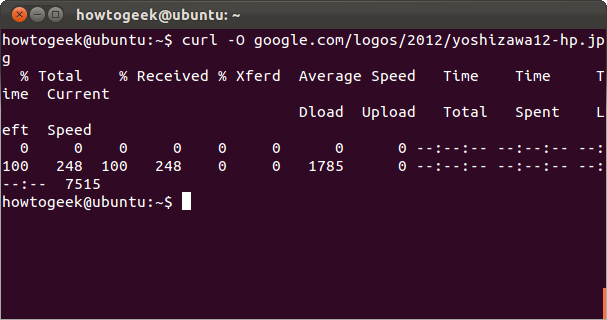


**Networking Commands in Linux**

**curl & wget**

Use the **curl** or **wget** commands to download a file from the Internet without leaving the terminal. If you’re using curl, type **curl -O** followed by the path to the file. wget users can use **wget** without any options.. The file will appear in the current directory.

curl -O website.com/file  
wget website.com/file

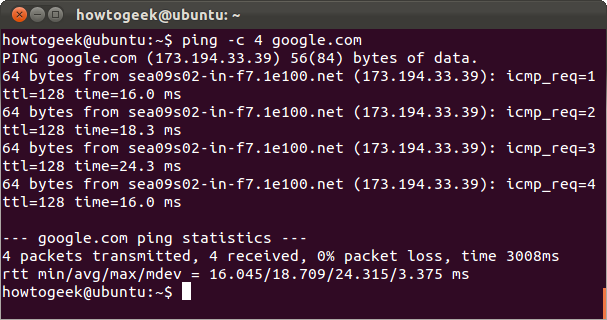


**ping**

**ping** sends ECHO\_REQUEST packets to the address you specify. It’s a great way to see whether your computer can communicate with the Internet or a specific IP address. Bear in mind that many systems are configured not to respond to pings, however.

Unlike the ping command on Windows, the Linux ping command will keep sending packets until you terminate it. You can specify a finite amount of packets with the **-c** switch.

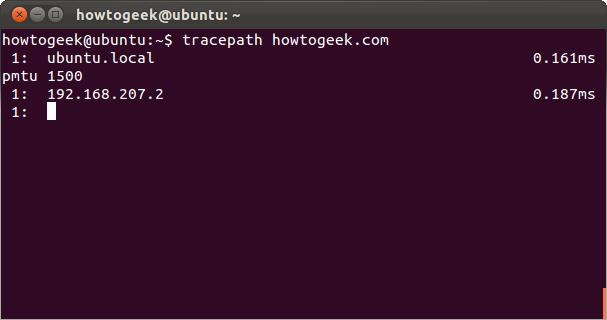
ping -c 4 google.com



**tracepath & traceroute**

The **tracepath** command is similar to **traceroute**, but it doesn’t require root privileges. It’s also installed by default on Ubuntu, while traceroute isn’t. tracepath traces the network path to a destination you specify and reports each “hop” along the path. If you’re having network problems or slowness, tracepath can show you where the network is failing or where the slowness is occurring.

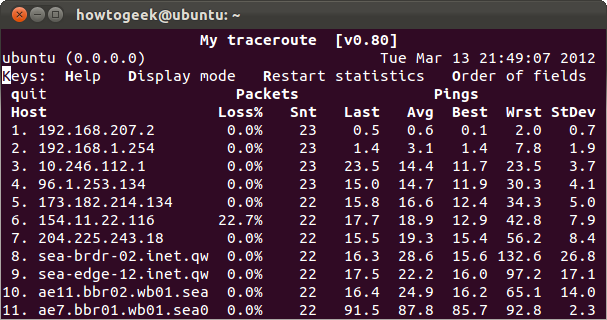
tracepath example.com



**mtr**

The **mtr** command combines ping and tracepath into a single command. mtr will continue to send packets, showing you the ping time to each “hop.” This will also show you any problems — in this case, we can see that hop 6 is losing over 20% of the packets.

mtr howtogeek.com

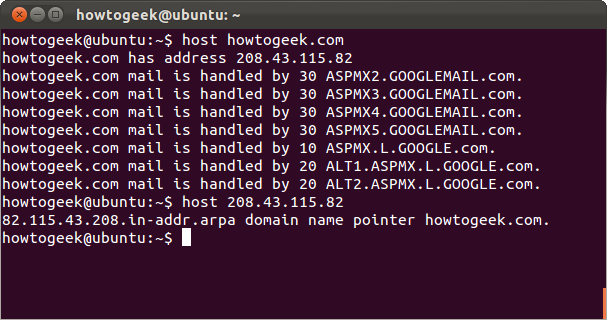


Press q or Ctrl-C to quit when you’re done.

**host**

The **host** command performs DNS lookups. Give it a domain name and you’ll see the associated IP address. Give it an IP address and you’ll see the associated domain name.

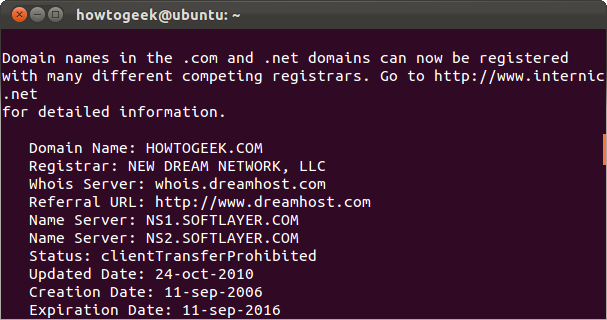
host howtogeek.com  
host 208.43.115.82



**whois**

The **whois** command will show you a website’s whois records, so you can view more information about who registered and owns a specific website.

whois example.com



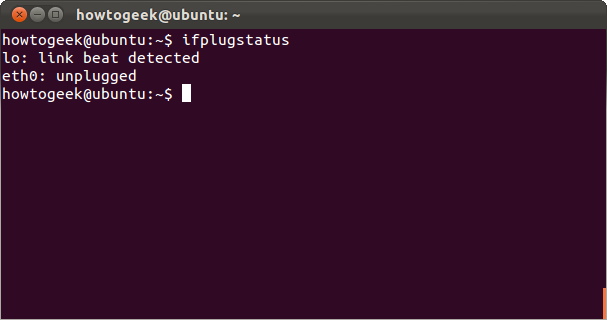
**ifplugstatus**

The **ifplugstatus** command will tell you whether a cable is plugged into a network interface or not. It isn’t installed by default on Ubuntu. Use the following command to install it:

sudo apt-get install ifplugd

Run the command to see the status of all interfaces or specify a specific interface to view its status.

ifplugstatus  
ifplugstatus eth0

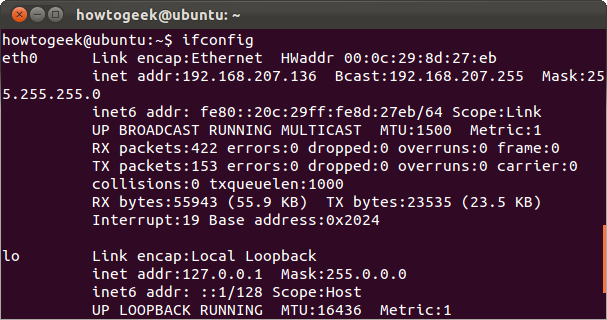


“Link beat detected” means the cable is plugged in. You’ll see “unplugged” if it isn’t.

**ifconfig**

The **ifconfig** command has a variety of options to configure, tune, and debug your system’s network interfaces. It’s also a quick way to view IP addresses and other network interface information. Type **ifconfig** to view the status of all currently active network interfaces, including their names. You can also specify an interface’s name to view only information about that interface.

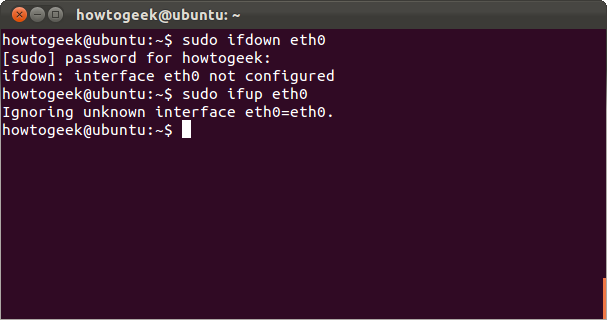
ifconfig  
ifconfig eth0



**ifdown & ifup**

The **ifdown** and **ifup** commands are the same thing as running **ifconfig up** or **ifconfig down**. Given an interface’s name, they take the interface down or bring it up. This requires root permissions, so you have to use sudo on Ubuntu.

sudo ifdown eth0  
sudo ifup eth0



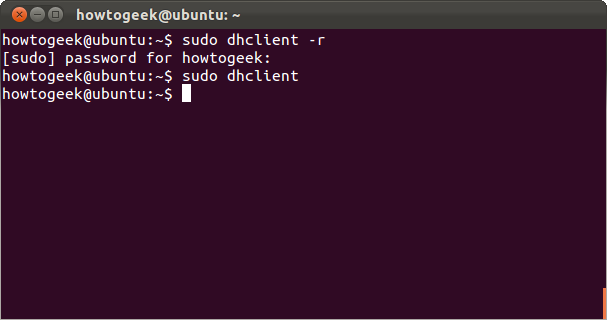
Try this on a Linux desktop system and you’ll probably get an error message. Linux desktops usually use NetworkManager, which manages network interfaces for you. These commands will still work on servers without NetworkManager, though.

If you really need to configure NetworkManager from the command line, use the **nmcli** command.

**dhclient**

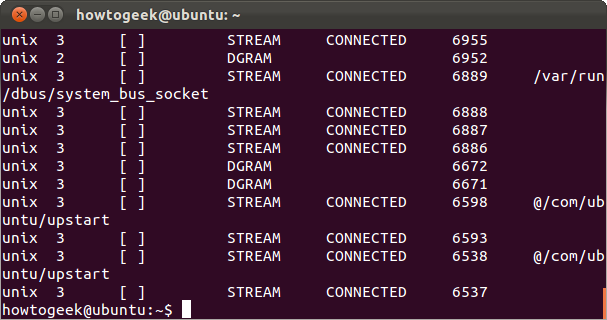
The **dhclient** command can release your computer’s IP address and get a new one from your DHCP server. This requires root permissions, so use sudo on Ubuntu. Run dhclient with no options to get a new IP address or use the **-r** switch to release your current IP address.

sudo dhclient -r  
sudo dhclient

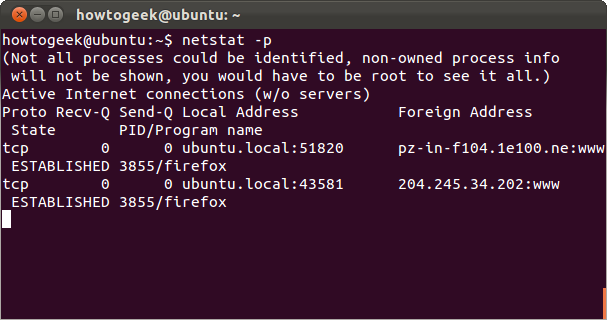


**netstat**

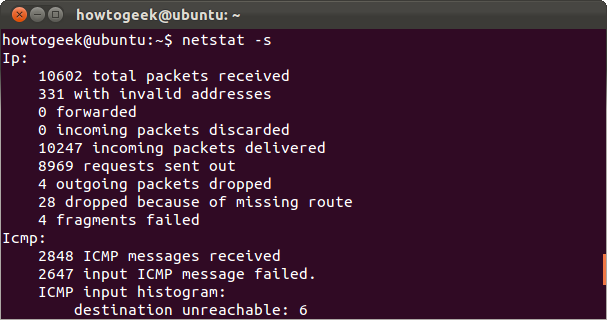
The **netstat** command can show a lot of different interface statistics, including open sockets and routing tables. Run the netstat command with no options and you’ll see a list of open sockets.



There’s a lot more you can do with this command. For example, use the **netstat -p** command to view the programs associated with open sockets.



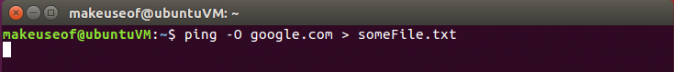
View detailed statistics for all ports with **netstat -s**.



### Output to a File

The reason you may want to leave a ping running for a long period could be to monitor the network connection between two devices. Or even between your computer and the internet. This can be achieved by running:

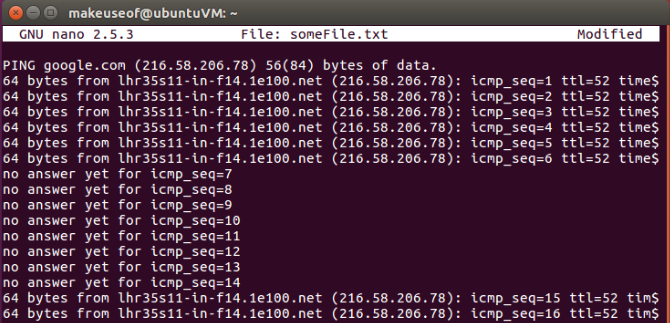
ping -O google.com > someFile.txt



After you run this command it will seem like nothing is happening and your cursor will just blink continuously. However, there are two things happening in this command. There is an infinite ping running and it is piping the output of that ping command to a file called someFile.txt in the same directory. This file can be opened and subjected to your forensic investigation. By default the ping command will not show when there was no reply. Enter the **-O** option as you see above.

To demonstrate this, I have an infinite ping running, piping it’s output to a text file, and while it’s running I unplugged and reconnected my network cable a few times. This will simulate a drop in connection, and the connection returning. To view the contents of the text file you can run the following command:

nano someFile.txt



The above information displayed in the text file clearly shows where the network connection has dropped. If you’re experiencing strange network issues, this simple experiment can help you eliminate certain possibilities. For example, if you were to leave a ping running against a device on your local network and there were no dropped replies, but the same experiment against an address on the internet does show some dropped packets. There is a strong likelihood that your computer hardware is okay, but the device connecting to the internet may need further inspection.

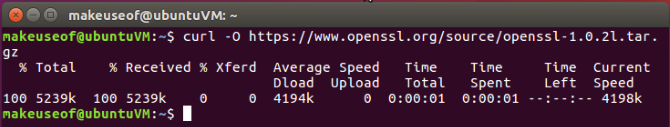
## Download a File From the Internet

Open a web browser, navigate to the page, click the download link. That’s the way to download a file, right?

No!

Using **curl** or **wget**, you can easily download a file from without leaving the warm, snug atmosphere of [**your terminal session**](https://www.makeuseof.com/tag/4-ways-teach-terminal-commands-linux-si/).

curl -O https://www.openssl.org/source/openssl-1.0.2l.tar.gz



wget https://www.openssl.org/source/openssl-1.0.2l.tar.gz

**TCP/IP (Transmission Control Protocol/Internet Protocol)**

TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication [protocols](https://searchnetworking.techtarget.com/definition/protocol) used to interconnect [network](https://searchnetworking.techtarget.com/definition/network) devices on the internet. TCP/IP can also be used as a communications protocol in a private network (an [intranet](https://searchwindevelopment.techtarget.com/definition/intranet) or an [extranet](https://searchenterprisewan.techtarget.com/definition/extranet)).

The entire internet protocol suite -- a set of rules and procedures -- is commonly referred to as TCP/IP, though others are included in the suite*.*

TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management, and it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network.

The two main protocols in the internet protocol suite serve specific functions. [TCP](https://searchnetworking.techtarget.com/definition/TCP) defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller [packets](https://searchnetworking.techtarget.com/definition/packet) before they are then transmitted over the internet and reassembled in the right order at the destination address.

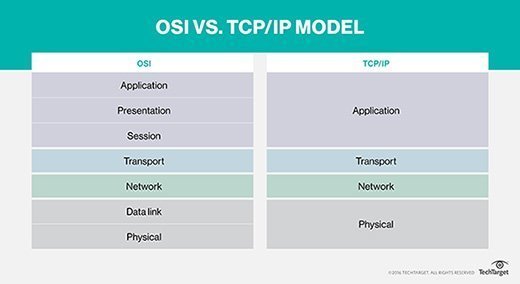
[IP](https://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol) defines how to [address](https://searchnetworking.techtarget.com/definition/address) and [route](https://searchnetworking.techtarget.com/definition/routing-table) each packet to make sure it reaches the right destination. Each [gateway](https://internetofthingsagenda.techtarget.com/definition/gateway) computer on the network checks this IP address to determine where to forward the message.

**How TCP/IP works**

TCP/IP uses the [client/server](https://searchnetworking.techtarget.com/definition/client-server) model of communication in which a user or machine (a client) is provided a service (like sending a webpage) by another computer (a server) in the network.

Collectively, the TCP/IP suite of protocols is classified as [stateless](https://whatis.techtarget.com/definition/stateless), which means each client request is considered new because it is unrelated to previous requests. Being stateless frees up network paths so they can be used continuously.

The transport layer itself, however, is stateful. It transmits a single message, and its connection remains in place until all the packets in a message have been received and reassembled at the destination.



The TCP/IP model differs slightly from the seven-layer Open Systems Interconnection ([OSI](https://searchnetworking.techtarget.com/definition/OSI)) networking model designed after it, which defines how applications can communicate over a network.

**TCP/IP model layers**

TCP/IP functionality is divided into four [layers](https://searchsoftwarequality.techtarget.com/definition/layer), each of which include specific protocols.

* *The application layer* provides applications with standardized data exchange. Its protocols include the Hypertext Transfer Protocol ([HTTP](https://searchwindevelopment.techtarget.com/definition/HTTP)), File Transfer Protocol ([FTP](https://searchenterprisewan.techtarget.com/definition/File-Transfer-Protocol)), Post Office Protocol 3 ([POP3](https://whatis.techtarget.com/definition/POP3-Post-Office-Protocol-3)), Simple Mail Transfer Protocol ([SMTP](https://whatis.techtarget.com/definition/SMTP-Simple-Mail-Transfer-Protocol)) and Simple Network Management Protocol ([SNMP](https://searchnetworking.techtarget.com/definition/SNMP)).
* *The transport layer* is responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include TCP and User Datagram Protocol ([UDP](https://searchnetworking.techtarget.com/definition/UDP-User-Datagram-Protocol)), which is sometimes used instead of TCP for special purposes.
* *The network layer*, also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol ([ICMP](https://searchnetworking.techtarget.com/definition/ICMP)), which is used for error reporting.
* *The physical layer* consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network. The protocols in this layer include [Ethernet](https://searchnetworking.techtarget.com/definition/Ethernet) for local area networks ([LANs](https://searchnetworking.techtarget.com/definition/local-area-network-LAN)) and the Address Resolution Protocol ([ARP](https://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP)).

**Importance of TCP/IP**

TCP/IP is nonproprietary and, as a result, is not controlled by any single company. Therefore, the internet protocol suite can be modified easily. It is compatible with all operating systems, so it can communicate with any other system. The internet protocol suite is also compatible with all types of computer hardware and networks.

TCP/IP is highly scalable and, as a routable protocol, can determine the most efficient path through the network.

**The history of TCP/IP**

The Defense Advanced Research Projects Agency ([DARPA](https://searchnetworking.techtarget.com/definition/DARPA)), the research branch of the U.S. Department of Defense, created the TCP/IP model in the 1970s for use in ARPANET, a wide area network that preceded the internet. TCP/IP was originally designed for the [Unix](https://searchdatacenter.techtarget.com/definition/Unix) operating system, and it has been built into all of the operating systems that came after it.

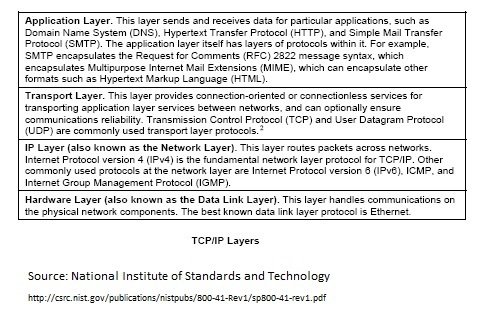
# TCP (Transmission Control Protocol)

TCP (Transmission Control [Protocol](https://searchnetworking.techtarget.com/definition/protocol)) is a standard that defines how to establish and maintain a network conversation via which [application programs](https://searchsoftwarequality.techtarget.com/definition/application) can exchange data. TCP works with the Internet Protocol ([IP](https://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol)), which defines how computers send [packet](https://searchnetworking.techtarget.com/definition/packet)s of [data](https://searchdatamanagement.techtarget.com/definition/data) to each other. Together, TCP and IP are the basic rules defining the Internet. TCP is defined by the Internet Engineering Task Force ([IETF](https://searchmicroservices.techtarget.com/definition/IETF-Internet-Engineering-Task-Force)) in the Request for Comment ([RFC](https://whatis.techtarget.com/definition/Request-for-Comments-RFC)) standards document number 793.

TCP is a [connection-oriented](https://searchnetworking.techtarget.com/definition/connection-oriented) protocol, which means a connection is established and maintained until the [application programs](https://searchsoftwarequality.techtarget.com/definition/application) at each end have finished exchanging [messages](https://whatis.techtarget.com/definition/messaging). It determines how to break application data into packets that [networks](https://searchnetworking.techtarget.com/definition/network) can deliver, sends packets to and accepts packets from the network layer, manages [flow control](https://whatis.techtarget.com/definition/flow-control), and—because it is meant to provide error-free data transmission—handles retransmission of dropped or garbled packets as well as acknowledgement of all packets that arrive.  In the [Open Systems Interconnection](https://searchnetworking.techtarget.com/definition/OSI) (OSI) communication model, TCP covers parts of Layer 4, the [Transport Layer](https://searchnetworking.techtarget.com/definition/Transport-layer), and parts of Layer 5, the [Session Layer](https://searchnetworking.techtarget.com/definition/Session-layer).

For example, when a Web [server](https://whatis.techtarget.com/definition/server) sends an [HTML](https://www.theserverside.com/definition/HTML-Hypertext-Markup-Language) file to a [client](https://searchenterprisedesktop.techtarget.com/definition/client), it uses the [HTTP](https://searchwindevelopment.techtarget.com/definition/HTTP) protocol to do so. The HTTP program layer asks the TCP layer to set up the connection and send the file.  The TCP stack divides the file into packets, numbers them and then forwards them individually to the IP layer for delivery. Although each packet in the transmission will have the same source and destination [IP address](https://searchwindevelopment.techtarget.com/definition/IP-address)es, packets may be sent along multiple routes. The TCP program layer in the client computer waits until all of the packets have arrived, then acknowledges those it receives and asks for the retransmission on any it does not (based on missing packet numbers), then assembles them into a file and delivers the file to the receiving application.

### TCP/IP stack



Retransmissions and the need to reorder packets after they arrive can introduce [latency](https://whatis.techtarget.com/definition/latency) in a TCP stream. Highly time-sensitive applications like voice over IP ([VoIP](https://searchunifiedcommunications.techtarget.com/definition/VoIP)) and [streaming video](https://searchunifiedcommunications.techtarget.com/definition/streaming-video) generally rely on a transport like User Datagram Protocol ([UDP](https://searchnetworking.techtarget.com/definition/UDP-User-Datagram-Protocol)) that reduces latency and [jitter](https://searchunifiedcommunications.techtarget.com/definition/jitter) (variation in latency) by not worrying about reordering packets or getting missing data retransmitted.

**Domain Name System**

When **DNS** was not into existence, one had to download a **Host file** containing host names and their corresponding IP address. But with increase in number of hosts of internet, the size of host file also increased. This resulted in increased traffic on downloading this file. To solve this problem the DNS system was introduced.

**Domain Name System** helps to resolve the host name to an address. It uses a hierarchical naming scheme and distributed database of IP addresses and associated names

IP Address

IP address is a unique logical address assigned to a machine over the network. An IP address exhibits the following properties:

* IP address is the unique address assigned to each host present on Internet.
* IP address is 32 bits (4 bytes) long.
* IP address consists of two components:**network component** and **host component**.
* Each of the 4 bytes is represented by a number from 0 to 255, separated with dots. For example 137.170.4.124

IP address is 32-bit number while on the other hand domain names are easy to remember names. For example, when we enter an email address we always enter a symbolic string such as webmaster@website.com.

Uniform Resource Locator (URL)

**Uniform Resource Locator (URL)** refers to a web address which uniquely identifies a document over the internet.

This document can be a web page, image, audio, video or anything else present on the web.

For example, **www.website.com/internet\_technology/index.html** is an URL to the index.html which is stored on website web server under internet\_technology directory.

URL Types

There are two forms of URL as listed below:

* Absolute URL
* Relative URL

Absolute URL

Absolute URL is a complete address of a resource on the web. This completed address comprises of protocol used, server name, path name and file name.

For example http:// www.website.com / internet\_technology /index.htm. where:

* **http** is the protocol.
* **website.com** is the server name.
* **index.htm** is the file name.

The protocol part tells the web browser how to handle the file. Similarly we have some other protocols also that can be used to create URL are:

* FTP
* https
* Gopher
* mailto
* news

Relative URL

Relative URL is a partial address of a webpage. Unlike absolute URL, the protocol and server part are omitted from relative URL.

Relative URLs are used for internal links i.e. to create links to file that are part of same website as the WebPages on which you are placing the link.

For example, to link an image on tutorialspoint.com/internet\_technology/internet\_referemce\_models, we can use the relative URL which can take the form like **/internet\_technologies/internet-osi\_model.jpg.**

Difference between Absolute and Relative URL

|  |  |
| --- | --- |
| **Absolute URL** | **Relative URL** |
| Used to link web pages on different websites | Used to link web pages within the same website. |
| Difficult to manage. | Easy to Manage |
| Changes when the server name or directory name changes | Remains same even of we change the server name or directory name. |
| Take time to access | Comparatively faster to access. |

Domain Name System Architecture

The Domain name system comprises of **Domain Names, Domain Name Space, Name Server** that have been described below:

Domain Names

Domain Name is a symbolic string associated with an IP address. There are several domain names available; some of them are generic such as **com, edu, gov, net** etc, while some country level domain names such as **au, in, za, us** etc.

The following table shows the **Generic** Top-Level Domain names:

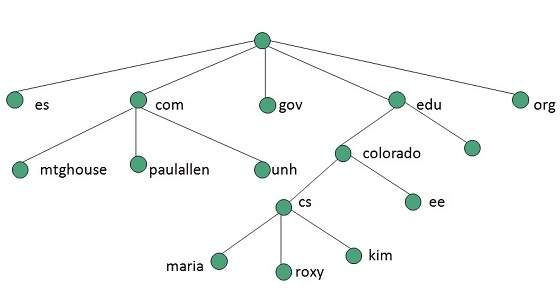
|  |
| --- |
|  |
| **Domain Name** | **Meaning** |
| Com | Commercial business |
| Edu | Education |
| Gov | U.S. government agency |
| Int | International entity |
| Mil | U.S. military |
| Net | Networking organization |
| Org | Non profit organization |

The following table shows the **Country top-level** domain names:

|  |
| --- |
|  |
| **Domain Name** | **Meaning** |
| au | Australia |
| in | India |
| cl | Chile |
| fr | France |
| us | United States |
| za | South Africa |
| uk | United Kingdom |
| jp | Japan |
| es | Spain |
| de | Germany |
| ca | Canada |
| ee | Estonia |
| hk | Hong Kong |

Domain Name Space

The domain name space refers a hierarchy in the internet naming structure. This hierarchy has multiple levels (from 0 to 127), with a root at the top. The following diagram shows the domain name space hierarchy:



In the above diagram each subtree represents a domain. Each domain can be partitioned into sub domains and these can be further partitioned and so on.

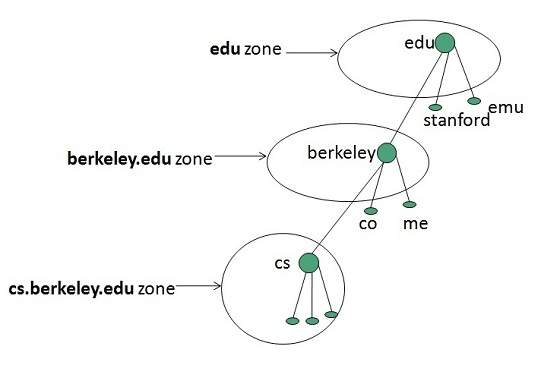
Name Server

Name server contains the DNS database. This database comprises of various names and their corresponding IP addresses. Since it is not possible for a single server to maintain entire DNS database, therefore, the information is distributed among many DNS servers.

* Hierarchy of server is same as hierarchy of names.
* The entire name space is divided into the zones

Zones

Zone is collection of nodes (sub domains) under the main domain. The server maintains a database called zone file for every zone.



If the domain is not further divided into sub domains then domain and zone refers to the same thing.

The information about the nodes in the sub domain is stored in the servers at the lower levels however; the original server keeps reference to these lower levels of servers.

Types of Name Servers

Following are the three categories of Name Servers that manages the entire Domain Name System:

* Root Server
* Primary Server
* Secondary Server

Root Server

Root Server is the top level server which consists of the entire DNS tree. It does not contain the information about domains but delegates the authority to the other server

Primary Servers

Primary Server stores a file about its zone. It has authority to create, maintain, and update the zone file.

Secondary Server

Secondary Server transfers complete information about a zone from another server which may be primary or secondary server. The secondary server does not have authority to create or update a zone file.

DNS Working

DNS translates the domain name into IP address automatically. Following steps will take you through the steps included in domain resolution process:

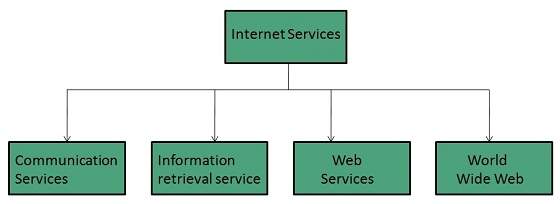
* When we type **www.website.com** into the browser, it asks the local DNS Server for its IP address.

Here the local DNS is at ISP end.

* When the local DNS does not find the IP address of requested domain name, it forwards the request to the root DNS server and again enquires about IP address of it.
* The root DNS server replies with delegation that **I do not know the IP address of www.website.com but know the IP address of DNS Server.**
* The local DNS server then asks the com DNS Server the same question.
* The **com** DNS Server replies the same that it does not know the IP address of www.tutorialspont.com but knows the address of tutorialspoint.com.
* Then the local DNS asks the tutorialspoint.com DNS server the same question.
* Then tutorialspoint.com DNS server replies with IP address of www.tutorialspoint.com.
* Now, the local DNS sends the IP address of www.tutorialspoint.com to the computer that sends the request.

**Internet Services**

**Internet Services** allows us to access huge amount of information such as text, graphics, sound and software over the internet. Following diagram shows the four different categories of Internet Services.



Communication Services

There are various Communication Services available that offer exchange of information with individuals or groups. The following table gives a brief introduction to these services:

|  |  |
| --- | --- |
| **S.N.** | **Service Description** |
| 1 | **Electronic Mail** Used to send electronic message over the internet. |
| 2 | **Telnet** Used to log on to a remote computer that is attached to internet. |
| 3 | **Newsgroup** Offers a forum for people to discuss topics of common interests. |
| 4 | **Internet Relay Chat (IRC)** Allows the people from all over the world to communicate in real time. |
| 5 | **Mailing Lists** Used to organize group of internet users to share common information through e-mail. |
| 6 | **Internet Telephony (VoIP)** Allows the internet users to talk across internet to any PC equipped to receive the call. |
| 7 | **Instant Messaging** Offers real time chat between individuals and group of people. Eg. Yahoo messenger, MSN messenger. |

Information Retrieval Services

There exist several Information retrieval services offering easy access to information present on the internet. The following table gives a brief introduction to these services:

|  |  |
| --- | --- |
| **S.N.** | **Service Description** |
| 1 | **File Transfer Protocol (FTP)** Enable the users to transfer files. |
| 2 | **Archie** It’s updated database of public FTP sites and their content. It helps to search a file by its name. |
| 3 | **Gopher** Used to search, retrieve, and display documents on remote sites. |
| 4 | **Very Easy Rodent Oriented Netwide Index to Computer Achieved (VERONICA)** VERONICA is gopher based resource. It allows access to the information resource stored on gopher’s servers. |

Web Services

Web services allow exchange of information between applications on the web. Using web services, applications can easily interact with each other.

The web services are offered using concept of **Utility Computing.**

World Wide Web (WWW)

WWW is also known as W3. It offers a way to access documents spread over the several servers over the internet. These documents may contain texts, graphics, audio, video, hyperlinks. The hyperlinks allow the users to navigate between the documents.

Video Conferencing

Video conferencing or Video teleconferencing is a method of communicating by two-way video and audio transmission with help of telecommunication technologies.

Modes of Video Conferencing

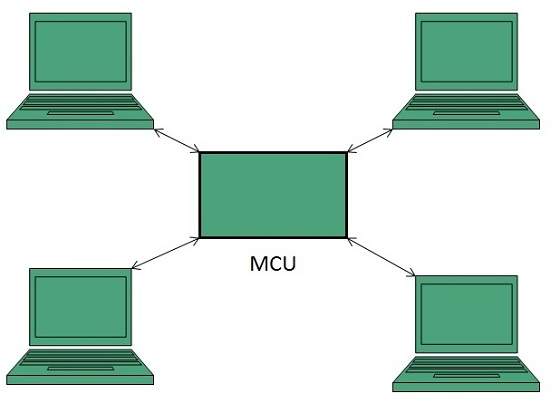
Point-to-Point

This mode of conferencing connects two locations only.



Multi-point

This mode of conferencing connects more than two locations through **Multi-point Control Unit (MCU).**



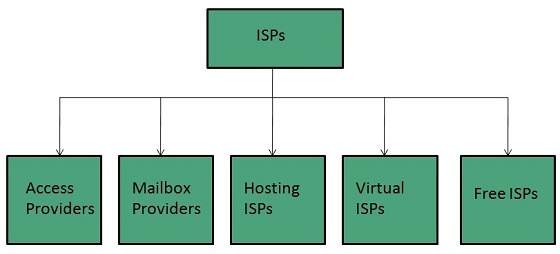
Internet Service Providers (ISP)

**Internet Service Provider (ISP)** is a company offering access to internet. They offer various services:

* Internet Access
* Domain name registration
* Dial-up access
* Leased line access

ISP Types

ISPs can broadly be classified into six categories as shown in the following diagram:



Access providers

They provide access to internet through telephone lines, cable wi-fi or fiber optics.

Mailbox Provider

Such providers offer mailbox hosting services.

Hosting ISPs

Hosting ISPs offers e-mail, and other web hosting services such as virtual machines, clouds etc.

Virtual ISPs

Such ISPs offer internet access via other ISP services.

Free ISPs

Free ISPs do not charge for internet services.

Connection Types

There exist several ways to connect to the internet. Following are these connection types available:

1. Dial-up Connection
2. ISDN
3. DSL
4. Cable TV Internet connections
5. Satellite Internet connections
6. Wireless Internet Connections

Dial-up Connection

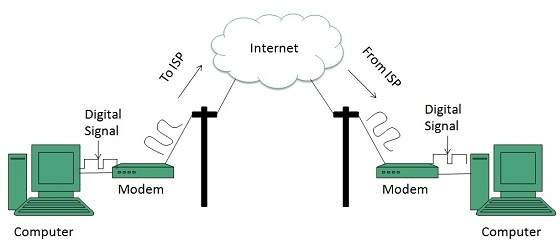
**Dial-up** connection uses telephone line to connect PC to the internet. It requires a modem to setup dial-up connection. This modem works as an interface between PC and the telephone line.

There is also a communication program that instructs the modem to make a call to specific number provided by an ISP.

Dial-up connection uses either of the following protocols:

1. Serial Line Internet Protocol (SLIP)
2. Point to Point Protocol (PPP)

The following diagram shows the accessing internet using modem:



ISDN

**ISDN** is acronym of **Integrated Services Digital Network.** It establishes the connection using the phone lines which carry digital signals instead of analog signals.

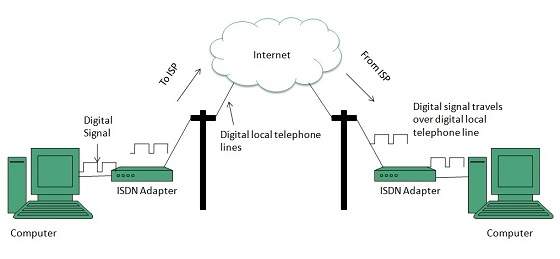
There are two techniques to deliver ISDN services:

1. Basic Rate Interface (BRI)
2. Primary Rate Interface (PRI)

**Key points:**

* The BRI ISDN consists of three distinct channels on a single ISDN line: t1o 64kbps B (Bearer) channel and one 16kbps D (Delta or Data) channels.
* The PRI ISDN consists of 23 B channels and one D channels with both have operating capacity of 64kbps individually making a total transmission rate of 1.54Mbps.

The following diagram shows accessing internet using ISDN connection:



DSL

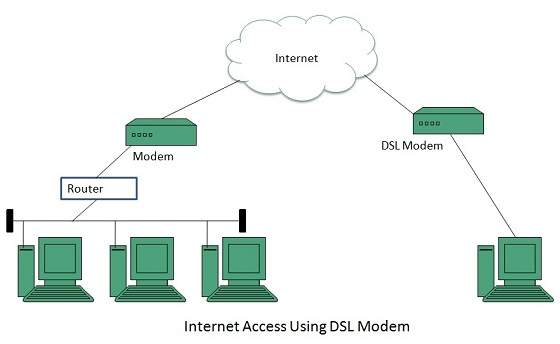
**DSL** is acronym of **Digital Subscriber Line.** It is a form of broadband connection as it provides connection over ordinary telephone lines.

Following are the several versions of DSL technique available today:

1. Asymmetric DSL (ADSL)
2. Symmetric DSL (SDSL)
3. High bit-rate DSL (HDSL)
4. Rate adaptive DSL (RDSL)
5. Very high bit-rate DSL (VDSL)
6. ISDN DSL (IDSL)

All of the above mentioned technologies differ in their upload and download speed, bit transfer rate and level of service.

The following diagram shows that how we can connect to internet using DSL technology:



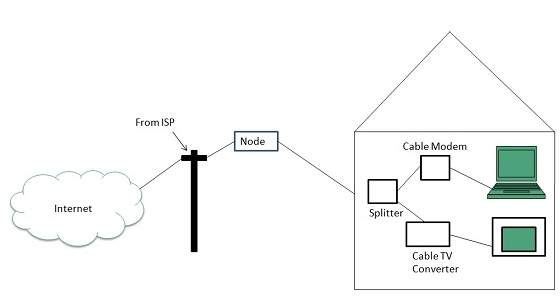
Cable TV Internet Connection

Cable TV Internet connection is provided through Cable TV lines. It uses coaxial cable which is capable of transferring data at much higher speed than common telephone line.

**Key Points:**

* A cable modem is used to access this service, provided by the cable operator.
* The Cable modem comprises of two connections: one for internet service and other for Cable TV signals.
* Since Cable TV internet connections share a set amount of bandwidth with a group of customers, therefore, data transfer rate also depends on number of customers using the internet at the same time.

The following diagram shows that how internet is accessed using Cable TV connection:



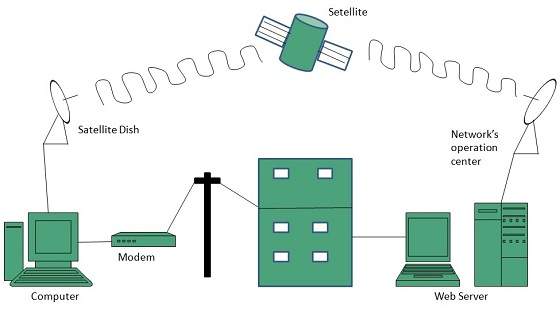
Satellite Internet Connection

Satellite Internet connection offers high speed connection to the internet. There are two types of satellite internet connection: one way connection or two way connection.

In one way connection, we can only download data but if we want to upload, we need a dialup access through ISP over telephone line.

In two way connection, we can download and upload the data by the satellite. It does not require any dialup connection.

The following diagram shows how internet is accessed using satellite internet connection:



Wireless Internet Connection

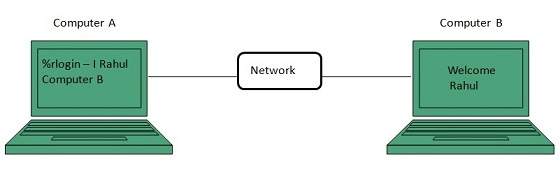
Wireless Internet Connection makes use of radio frequency bands to connect to the internet and offers a very high speed. The wireless internet connection can be obtained by either WiFi or Bluetooth.

**Key Points:**

* Wi Fi wireless technology is based on IEEE 802.11 standards which allow the electronic device to connect to the internet.
* Bluetooth wireless technology makes use of short-wavelength radio waves and helps to create personal area network (PAN).

Telnet

Telnet is a protocol used to log in to remote computer on the internet. There are a number of Telnet clients having user friendly user interface. The following diagram shows a person is logged in to computer A, and from there, he remote logged into computer B.



Email

Email is a service which allows us to send the message in electronic mode over the internet. It offers an efficient, inexpensive and real time mean of distributing information among people.

E-Mail Address

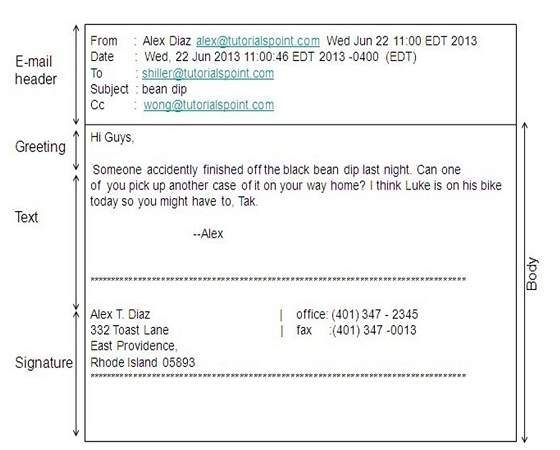
Each user of email is assigned a unique name for his email account. This name is known as E-mail address. Different users can send and receive messages according to the e-mail address.

E-mail is generally of the form username@domainname. For example, webmaster@tutorialspoint.com is an e-mail address where webmaster is username and tutorialspoint.com is domain name.

* The username and the domain name are separated by @ (at) symbol.
* E-mail addresses are not case sensitive.
* Spaces are not allowed in e-mail address.

E-mail Message Components

E-mail message comprises of different components: E-mail Header, Greeting, Text, and Signature. These components are described in the following diagram:



E-mail Header

The first five lines of an E-mail message is called E-mail header. The header part comprises of following fields:

* From
* Date
* To
* Subject
* CC
* BCC

From

The From field indicates the sender’s address i.e. who sent the e-mail.

Date

The Date field indicates the date when the e-mail was sent.

To

The To field indicates the recipient’s address i.e. to whom the e-mail is sent.

Subject

The Subject field indicates the purpose of e-mail. It should be precise and to the point.

CC

CC stands for Carbon copy. It includes those recipient addresses whom we want to keep informed but not exactly the intended recipient.

BCC

BCC stands for Black Carbon Copy. It is used when we do not want one or more of the recipients to know that someone else was copied on the message.

Greeting

Greeting is the opening of the actual message. Eg. Hi Sir or Hi Guys etc.

Text

It represents the actual content of the message.

Signature

This is the final part of an e-mail message. It includes Name of Sender, Address, and Contact Number.

Advantages

E-mail has prooved to be powerful and reliable medium of commmunication. Here are the benefits of E-mail:

* Reliable
* Convenience
* Speed
* Inexpensive
* Printable
* Global
* Generality

Reliable

Many of the mail systems notify the sender if e-mail message was undeliverable.

Convenience

There is no requirement of stationary and stamps. One does not have to go to post office. But all these things are not required for sending or receiving an mail.

Speed

E-mail is very fast. However, the speed also depends upon the underlying network.

Inexpensive

The cost of sending e-mail is very low.

Printable

It is easy to obtain a hardcopy of an e-mail. Also an electronic copy of an e-mail can also be saved for records.

Global

E-mail can be sent and received by a person sitting across the globe.

Generality

It is also possible to send graphics, programs and sounds with an e-mail.

Disadvantages

Apart from several benefits of E-mail, there also exists some disadvantages as discussed below:

* Forgery
* Overload
* Misdirection
* Junk
* No response

Forgery

E-mail doesn’t prevent from forgery, that is, someone impersonating the sender, since sender is usually not authenticated in any way.

Overload

Convenience of E-mail may result in a flood of mail.

Misdirection

It is possible that you may send e-mail to an unintended recipient.

Junk

Junk emails are undesirable and inappropriate emails. Junk emails are sometimes referred to as spam.

No Response

It may be frustrating when the recipient does not read the e-mail and respond on a regular basis.

E-mail System

E-mail system comprises of the following three components:

* Mailer
* Mail Server
* Mailbox

Mailer

It is also called mail program, mail application or mail client. It allows us to manage, read and compose e-mail.

Mail Server

The function of mail server is to receive, store and deliver the email. It is must for mail servers to be Running all the time because if it crashes or is down, email can be lost.

Mailboxes

Mailbox is generally a folder that contains emails and information about them.

Working of E-mail

Email working follows the client server approach. In this client is the mailer i.e. the mail application or mail program and server is a device that manages emails.

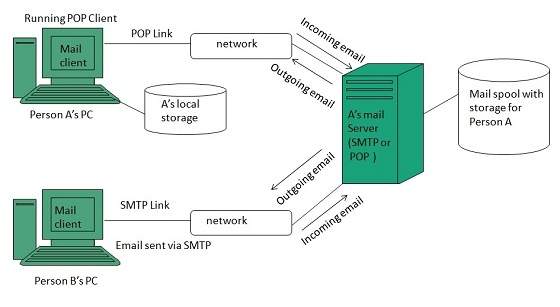
Following example will take you through the basic steps involved in sending and receiving emails and will give you a better understanding of working of email system:

* Suppose person A wants to send an email message to person B.
* Person A composes the messages using a mailer program i.e. mail client and then select Send option.
* The message is routed to Simple Mail Transfer Protocol to person B’s mail server.
* The mail server stores the email message on disk in an area designated for person B.

The disk space area on mail server is called mail spool.

* Now, suppose person B is running a POP client and knows how to communicate with B’s mail server.
* It will periodically poll the POP server to check if any new email has arrived for B.As in this case, person B has sent an email for person B, so email is forwarded over the network to B’s PC. This is message is now stored on person B’s PC.

The following diagram gives pictorial representation of the steps discussed above:



E-mail Hacking

Email hacking can be done in any of the following ways:

* Spam
* Virus
* Phishing

Spam

E-mail spamming is an act of sending Unsolicited Bulk E-mails (UBI) which one has not asked for. Email spams are the junk mails sent by commercial companies as an advertisement of their products and services.

Virus

Some emails may incorporate with files containing malicious script which when run on your computer may lead to destroy your important data.

Phishing

Email phishing is an activity of sending emails to a user claiming to be a legitimate enterprise. Its main purpose is to steal sensitive information such as usernames, passwords, and credit card details.

Such emails contains link to websites that are infected with malware and direct the user to enter details at a fake website whose look and feels are same to legitimate one.

E-mail Spamming and Junk Mails

Email spamming is an act of sending Unsolicited Bulk E-mails (UBI) which one has not asked for. Email spams are the junk mails sent by commercial companies as an advertisement of their products and services.

Spams may cause the following problems:

* It floods your e-mail account with unwanted e-mails, which may result in loss of important e-mails if inbox is full.
* Time and energy is wasted in reviewing and deleting junk emails or spams.
* It consumes the bandwidth that slows the speed with which mails are delivered.
* Some unsolicited email may contain virus that can cause harm to your computer.

Blocking Spams

Following ways will help you to reduce spams:

* While posting letters to newsgroups or mailing list, use a separate e-mail address than the one you used for your personal e-mails.
* Don’t give your email address on the websites as it can easily be spammed.
* Avoid replying to emails which you have received from unknown persons.
* Never buy anything in response to a spam that advertises a product.

E-mail Cleanup and Archiving

In order to have light weighted Inbox, it’s good to archive your inbox from time to time. Here I will discuss the steps to clean up and archive your Outlook inbox.

* Select File tab on the mail pane.
* Select Cleanup Tools button on account information screen.
* Select Archive from cleanup tools drop down menu.
* Select Archive this folder and all subfolders option and then click on the folder that you want to archive. Select the date from the Archive items older than: list. Click Browse to create new .pst file name and location. Click OK.

MIME Types

MIME is acronym of Multipurpose Internet Mail Extensions. MIME compliant mailer allows us to send files other than simple text i.e. It allows us to send audio, video, images, document, and pdf files as an attachment to an email.

Suppose if you want to send a word processor document that has a group of tabular columns with complex formatting. If we transfer the file as text, all the formatting may be lost. MIME compliant mailer takes care of messy details and the message arrives as desired.

The following table describes commonly used MIME Types:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1.** | **Type** | **Subtype** | **Description** | **File extension(s)** |
| 2. | Application | postscript  tex  troff | Printable postscript document  TEX document  Printable troff document | .eps, .ps  .tex  .t, .tr, .roff |
| 3. | Audio | aiff  au  midi  real audio | Apple sound  Sun Microsystems sound  Musical Instrument Digital Interface  Progressive Network sound | .aif, .aiff,.aifc  .au, .snd  .midi, .mid  .ra, .ram |
| 4. | image | gif  jpeg  png  triff | Graphics Interchange Format  Joint Photographic Experts Group  Portable Network Graphics  Tagged Image Modeling Language | .gif  .jpeg, .jpg, .jpe  .png  .tiff, .tif |
| 5. | Model | vrml | Virual reality Modelling Language | .wrl |
| 6. | Text  plain  sgml | html | Hyper Text Markup Language  Unformatted text  Standard Generalized Markup language | .html, .htm  .txt  .sgml |
| 7. | Video | avi  mpeg  quicktime  sgi-movie | Microsoft Audio Video Interleaved  Moving Pictures Expert Group  Apple QuickTime movie  silicon graphic movie | .avi  .mpeg, .mpg  .qt, .mov  .movie |

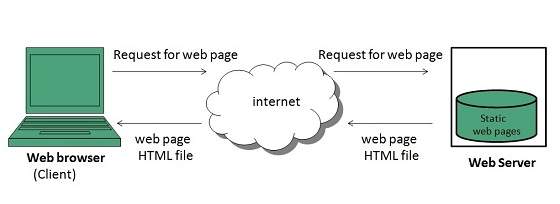
**Website**

Website is a location on web and is hosted on a web server. It is a set of related web pages. It is accessed using Internet address known as Uniform Resource Locator

Static Websites

**Static websites** are also known as flat or stationary websites. They are loaded on the client’s browser as exactly they are stored on the web server. Such websites contain only static information. User can only read the information but can’t do any modification or interact with the information.

Static websites are created using only HTML. Static websites are only used when the information is no more required to be modified.



Dynamic Websites

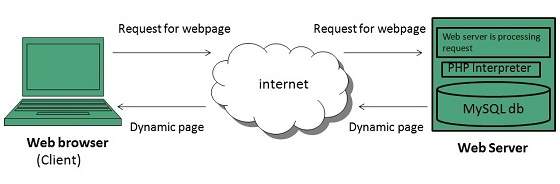
**Dynamic websites** shows different information at different point of time. It is possible to change a portion of a web page without loading the entire web page. It has been made possible using **Ajax** technology.

Server-side dynamic web page

It is created by using server-side scripting. There are server-side scripting parameters that determine how to assemble a new web page which also include setting up of more client-side processing.

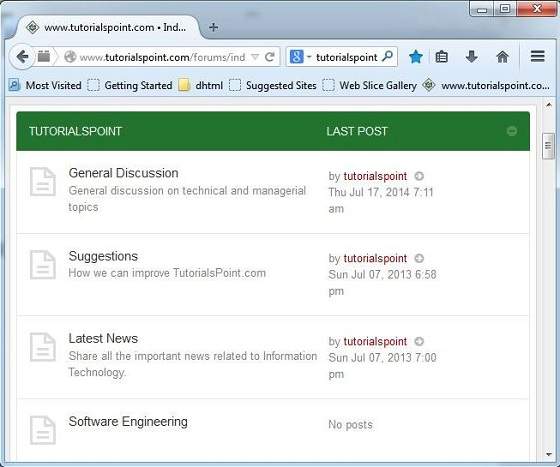
Client-side dynamic web page

It is processed using client side scripting such as javascript. And then passed in to **Document Object Model (DOM).**



Internet Forums

An internet forum is message board where people can hold conversation by posting messages.



**Key Points**

* A forum can contain several sub forums.
* Each of sub forums may contain a number of topics.
* Within a forum’s topic, each new discussion started is called a thread.
* This thread can be replied by as many people as so wish.

Blog

The term **Blog** is taken from we**b** **log.** It is a kind of web site that is updated regularly, with content about almost anything. In other words, blog is a **Content Management System (CMS)**, an easy way of publishing articles on the internet.



Blogging Terminologies

Blog

A type of website used to publish content on the internet.

Blogger

A person who writes for a blog.

Blogging

Writing for blogs is referred as blogging.

Blogosphere

A term is used to refer all the blogs on the web.

What to Blog about

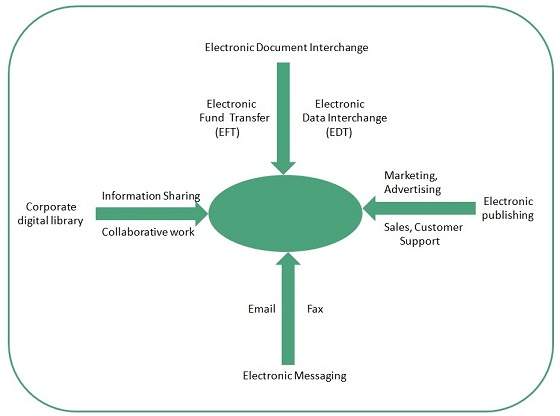
Following discussion will help you to figure out what to write about and as well as what to name your blog.

* Write what you know about. For example, if you have good computer knowledge. You can write what you know about the subject.
* You can share your experience. You can also write what you gained from that experience, what you learned.
* Detail your personal research.
* Share your memory of someone.

E-commerce

**E-Commerce** or **Electronics Commerce** is a methodology of modern business which addresses the need of business organizations, vendors and customers to reduce cost and improve the quality of goods and services while increasing the speed of delivery. E-commerce refers to paperless exchange of business information using following ways.

* Electronic Data Exchange (EDI)
* Electronic Mail (e-mail)
* Electronic Bulletin Boards
* Electronic Fund Transfer (EFT)
* Other Network-based technologies



Features

E-Commerce provides following features:

Non-Cash Payment

E-Commerce enables use of credit cards, debit cards, smart cards, electronic fund transfer via bank's website and other modes of electronics payment.

24x7 Service availability

E-commerce automates business of enterprises and services provided by them to customers are available anytime, anywhere. Here 24x7 refers to 24 hours of each seven days of a week.

Advertising / Marketing

E-commerce increases the reach of advertising of products and services of businesses. It helps in better marketing management of products / services.

Improved Sales

Using E-Commerce, orders for the products can be generated anytime, anywhere without any human intervention. By this way, dependencies to buy a product reduce at large and sales increases.

Support

E-Commerce provides various ways to provide pre sales and post sales assistance to provide better services to customers.

Portfolio

Online portfolio is collection of images, multimedia, emails, blog entries, and hyperlinks that are managed online. It can be seen as a kind of learning record that provides actual evidence of achievement.

Types

There are three types of online portfolio:

1. Developmental (e.g. working)
2. Reflective (e.g. learning)
3. Representational (e.g. showcase)

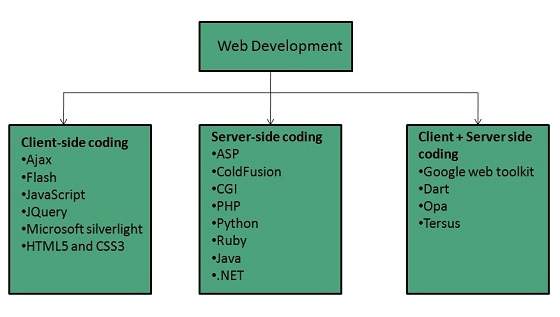
**Developmental** portfolio contains all the things that an individual has done over a period of time.

**Reflective** portfolio contains personal reflection on the content.

**Representational** online portfolio refers to learner’s achievement in a particular work.

Web development

**Web development** refers to building website and deploying on the web. Web development requires use of scripting languages both at the server end as well as at client end.

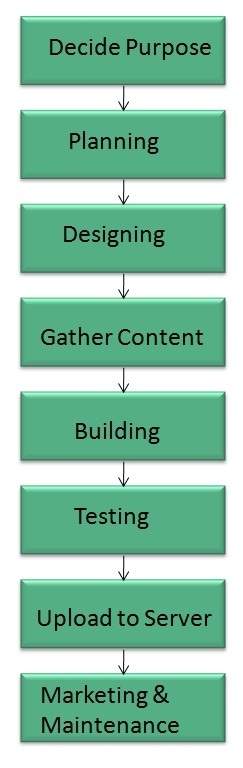


Before developing a web site once should keep several aspects in mind like:

* What to put on the web site?
* Who will host it?
* How to make it interactive?
* How to code it?
* How to create search engine friendly web site?
* How to secure the source code frequently?
* Will the web site design display well in different browsers?
* Will the navigation menus be easy to use?
* Will the web site loads quickly?
* How easily will the site pages print?
* How easily will visitors find important details specific to the web site?
* How effectively the style sheets be used on your web sites?

Web Development Process

Web development process includes all the steps that are good to take to build an attractive, effective and responsive website. These steps are shown in the following diagram:



Web development tools

Web development tools helps the developer to test and debug the web sites. Now a days the web development tooll come with the web browsers as add-ons. All web browsers have built in tools for this purpose.

Thsese tools allow the web developer to use HTML, CSS and JavaScript etc.. These are accessed by hovering over an item on a web page and selecting the “Inspect Element” from the context menu.

Featues

Following are the common featuers that every web development tool exhibits:

HTML and the DOM

HTML and DOM viewer allows you to see the DOM as it was rendered. It also allows to make changes to HTML and DOM and see the changes reflected in the page after the change is made.

Web Page Assests, Resources, and Network Information

Web development tools also helps to inspect the resources that are loaded and available on the web page.

Profiing and Auditing

**Profiling** refers to get information about the performance of a web page or web application and **Auditing** provides developers suggestions, after analyzing a page, for optimizations to decerease page load time and increase responsiveness.

Skills Required

For being a successful web developer, one should possess the following skills:

* Understanding of client and server side scripting.
* Creating, editing and modifying templates for a CMS or web development framework.
* Testing cross browser inconsistencies.
* Conducting observational user testing.
* Testing for compliance to specified standards such as accessibility standards in the client region.
* Programming interaction with javaScript, PHP, and Jquery etc.

Website publishing is the process of uploading content on the internet. It includes:

* uploading files
* updating web pages
* posting blogs

Website is published by uploading files on the remote server which is provided by the hosting company.

Prerequisites for Website Publishing

In order to publish your site, you need the following things:

* Web development software
* Internet Connection
* Web Server

Web development software

It is used for building web pages for your web site. Dreamweaver and WordPress are example of web development softwares.

Internet Connection

Internet connection is required to connect to a remotely located web server.

Web Server

Web server is the actual location where your website resides on. A web server may host single or multiple sites depending on what hosting service you have paid for.

**Website URL Registration**

A domain name is the part of your Internet address that comes after **"www".** For example, in **www.tutorialspoint.com** the domain name is **tutorialspoint.com.**

A domain name becomes your Business Address so care should be taken to select a domain name. Your domain name should be easy to remember and easy to type.

Domain Extensions

The final letter at end of internet address is known as top level domain names. They are called top level because they are read from right to left, and the part after the dot is the highest in a hierarchy.

The following table shows the **Generic** Top-Level Domain names:

|  |  |
| --- | --- |
| **Domain** | **Meaning** |
| .com | Commercial Business |
| .edu | Education |
| .gov | U.S. government agency |
| .int | International Entity |
| .mil | U.S. military |
| .net | Networking organization |
| .org | Non profit organization |

Registering Domain Name

Registering a Domain Name is very simple. You can take following step to get your desired domain name registered:

* Think of a name that justifies your business need. To find out the available names you can enter a name at commercial domain name registrar such as GoDaddy.
* If the domain name entered by you is available, then select that particular domain name.
* Now it will ask you for other additional services such as Email inbox, hosting etc. that host also provides. You may choose what’s best for you.
* Now they will ask you for your personal information which is stored in WHOIS database.
* It will then ask for payment information. Pay for the purchase you have made. Make sure you enter the correct payment information.
* Once you are done with all above steps, you are ready to use their tools to upload your stuff to your site.

**Web Hosting**

**Web hosting** is a service of providing online space for storage of web pages. These web pages are made available via **World Wide Web.** The companies which offer website hosting are known as **Web hosts.**

The servers on which web site is hosted remain switched on 24 x7. These servers are run by web hosting companies. Each server has its own IP address. Since IP addresses are difficult to remember therefore, webmaster points their domain name to the IP address of the server their website is stored on.

It is not possible to host your website on your local computer, to do so you would have to leave your computer on 24 hours a day. This is not practical and cheaper as well. This is where web hosting companies comes in.

**Type of Servers**

**There are many types of servers that all perform different functions. Many networks contain one or more of the common server types:**

#### File servers

**File servers store and distribute files. Multiple clients or users may share files stored on a server. In addition, centrally storing files offers easier backup or fault tolerance solutions than attempting to provide security and integrity for files on every device in an organization. File server hardware can be designed to maximize read and write speeds to improve performance.**

#### Print servers

**Print servers allow for the management and distribution of printing functionality. Rather than attaching a printer to every workstation, a single print server can respond to printing requests from numerous clients. Today, some larger and higher-end printers come with their own built-in print server, which removes the need for an additional computer-based print server. This internal print server also functions by responding to print requests from a client.**

#### Application servers

**Application servers run applications in lieu of client computers running applications locally. Application servers often run resource-intensive applications that are shared by a large number of users. Doing so removes the need for each client to have sufficient resources to run the applications. It also removes the need to install and maintain software on many machines as opposed to only one.**

**DNS servers**

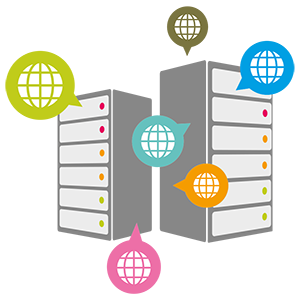
**Domain Name System (DNS) servers are application servers that provide name resolution to client computers by converting names easily understood by humans into machine-readable IP addresses. The DNS system is a widely distributed database of names and other DNS servers, each of which can be used to request an otherwise unknown computer name. When a client needs the address of a system, it sends a DNS request with the name of the desired resource to a DNS server. The DNS server responds with the necessary IP address from its table of names.**

**Mail servers**

**Mail servers are a very common type of application server. Mail servers receive emails sent to a user and store them until requested by a client on behalf of said user. Having an email server allows for a single machine to be properly configured and attached to the network at all times. It is then ready to send and receive messages rather than requiring every client machine to have its own email subsystem continuously running.**

#### Web servers

**One of the most abundant types of servers in today’s market is a web server. A web server is a special kind of application server that hosts programs and data requested by users across the Internet or an intranet. Web servers respond to requests from browsers running on client computers for web pages, or other web-based services. Common web servers include Apache web servers, Microsoft Internet Information Services (IIS) servers and Nginx servers.**

****

#### Database servers

**The amount of data used by companies, users, and other services is staggering. Much of that data is stored in databases. Databases need to be accessible to multiple clients at any given time and can require extraordinary amounts of disk space. Both of these needs lend themselves well to locating such databases on servers. Database servers run database applications and respond to numerous requests from clients. Common database server applications include Oracle, Microsoft SQL Server, DB2, and Informix.**

#### Virtual servers

**Virtual servers are taking the server world by storm. Unlike traditional servers that are installed as an operating system on machine hardware, virtual servers exist only as defined within specialized software called hypervisor. Each hypervisor can run hundreds, or even thousands, of virtual servers all at once. The hypervisor presents virtual hardware to the server as if it were real physical hardware. The virtual server uses the virtual hardware as usual, and the hypervisor passes the actual computation and storage needs onto the real hardware beneath, which is shared among all the other virtual servers.**

#### Proxy servers

**A proxy server acts as an intermediary between a client and a server. Often used to isolate either the clients or servers for security purposes, a proxy server takes the request from the client. Instead of responding to the client, it passes the request on to another server or process. The proxy server receives the response from the second server and then replies to the original client as if it were replying on its own. In this way, neither the client nor the responding server needs to directly connect to each other.**

# What is telnet?

**Telnet is a client-server protocol based on character-oriented data exchange over TCP connections. Telnet enables remote control of computers via text-based inputs and outputs. For this reason, a client-server connection is established as a default via the TCP protocol and port 23, where the remote-controlled device acts as a server and waits for commands. The Telnet client, the controlling instance in this process (also referred to as** [**remote access**](https://www.ionos.com/digitalguide/server/know-how/remote-desktop-success-of-the-application/) **or login), can be installed on a particular device, as well as on an ordinary computer. However, the presentation of the transmitted information differs, depending on the device. This protocol can also be used to manage applications that do not have a graphical interface.**

**As early as 1969 (during the nine months of work on** [**ARPANET**](https://www.ionos.com/digitalguide/websites/web-development/arpanet-definition-history-of-the-internet-predecessor/)**), the development of Telnet (Teletype Network) was practically completed. But it was only in 1973 that the protocol allowing access to remote computers first received its final specification in RFC 495 (Request for Comments). It was implemented by most platforms as the official standard of the Internet Engineering Task Force (IETF). The kernel protocol and the basic working methods and extensions are characterized in the more recent standards RFC 854 and RFC 855.**

# Command line FTP client in Windows

**Windows has native ftp client which can be used to connect to any ftp servers with in LAN or outside LAN. Below you can learn how to use this command. You can also see examples for each command. This command works on all Windows releases : XP, Vista and Windows 7.**

**Connect to a ftp server**

**ftp  connect  hostname\_or\_ip**

**You will be prompted for user name and password to verify if you have access to the ftp server. Some servers provide anonymous access.**

**C:\>ftp ftp.mysite.net**

**Connected to ftp.mysite.net.**

**220 Mysite FTP Service**

**User (ftp.mysite.net:(none)): anonymous**

**331 Anonymous access allowed, send identity (e-mail name) as password.**

**Password:**

**230-Welcome to ftp.mysite.net.**

**230 User logged in.**

**How to download files after connecting to ftp server**

**Once you are connected to the server you can use the following commands in ftp command prompt**

***ls*  – List the contents of the current directory.**

**ftp> ls**

**200 PORT command successful.**

**125 Data connection already open; Transfer starting.**

**bussys**

**deskapps**

**Products**

**PSS**

**226 Transfer complete.**

**ftp: 101 bytes received in 0.00Seconds 101000.00Kbytes/sec.**

**cd  directory\_name :  Change to the specified directory**

**ftp> cd pss**

**250 CWD command successful.**

**ftp>**

**Download files from ftp server**

***get  filename* : Download the file from ftp server to the local computer**

**ftp> get Filever.exe**

**200 PORT command successful.**

**125 Data connection already open; Transfer starting.**

**226 Transfer complete.**

**ftp: 55056 bytes received in 2.55Seconds 21.57Kbytes/sec.**

**ftp>**

***lcd directory\_name* : Change the directory of your local host.**

**ftp> lcd c:\users**

**Local directory now C:\Users.**

**ftp>**

***put filename* :  Upload the file from your local host to the current directory in ftp server**

**ftp> put filever.exe**

**200 PORT command successful.**

**550 Access is denied.**

**ftp>**

**In this example, I don’t have write access to the ftp server, so I have got ‘Access is denied’ message from the server.**

**Download multiple files**

**We can use ‘mget \*’ command to get multiple files from the server. But this command will prompt you for confirmation for each of the files.**

**ftp> mget \***

**200 Type set to A.**

**mget file1.exe? y**

**200 PORT command successful.**

**125 Data connection already open; Transfer starting.**

**226 Transfer complete.**

**ftp: 768784 bytes received in 46.89Seconds 16.40Kbytes/sec.**

**mget file2.exe? y**

**200 PORT command successful.**

**125 Data connection already open; Transfer starting.**

**226 Transfer complete.**

**ftp: 515584 bytes received in 31.02Seconds 16.62Kbytes/sec.**

**mget file3.exe? n**

**ftp>**

**This can be avoided by runing the  command ‘*prompt*‘ which sets the interactive mode to off.**

**ftp> mget \***

**200 Type set to A.**

**200 PORT command successful.**

**125 Data connection already open; Transfer starting.**

**226 Transfer complete.**

**ftp: 768784 bytes received in 46.08Seconds 16.69Kbytes/sec.**

**200 PORT command successful.**

**125 Data connection already open; Transfer starting.**

**226 Transfer complete.**

**ftp: 515584 bytes received in 32.41Seconds 15.91Kbytes/sec.**

**200 PORT command successful.**

**125 Data connection already open; Transfer starting.**

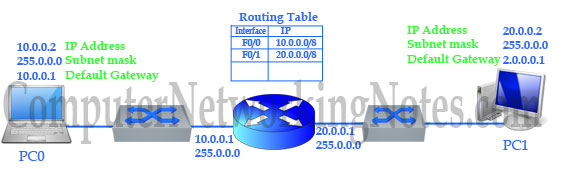
**226 Transfer complete.**

**ftp: 574464 bytes received in 34.50Seconds 16.65Kbytes/sec.**

**ftp>**

**Every data packet has two addresses; source address and destination address. Destination address is used to deliver the data packet at destination. Source address is used to identify the sender device at destination device. If source address and destination address both belong to same network, no routing is required. If both addresses belong to different network, an intermediate device which can create route between both networks is required. Intermediate device is known as routing device. Routers and multilayer switches are the examples of routing device. In short connecting two different networks through a routing device (or a series of routing devices) is known as routing. Let’s understand this process in more detail with an example.**

**In following figure we have two PCs. Both are located in different network. Assume that PC0 sends a packet to PC1. It will go through the following steps.**

****

**Upper layers (application, presentation, session) and transport layer prepare the data segments and handed down to network layer.**

**Network layer determines the routed protocol. Routed protocol is used to transmit user data packet across the network. IP and IPX are the example of routed protocol.**

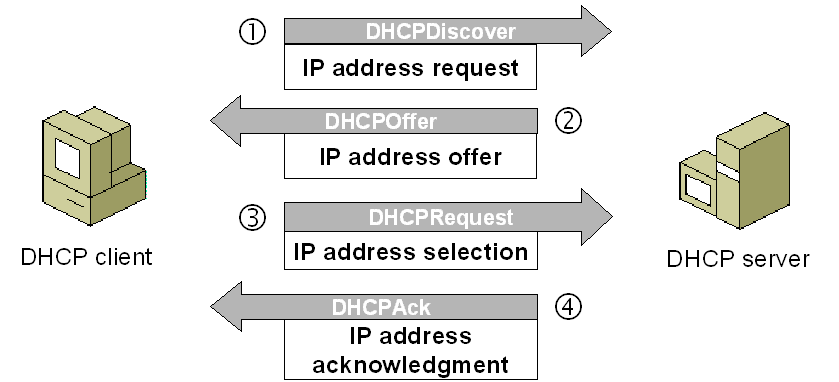
**Network layer attaches IP header to the segment. With IP header segment becomes packet. IP header includes several fields. One of them is the destination address filed. It plays leading role in routing. Based on it network layer decides whether packet will remain in local network or goes to the remote network. All remote requests are sent to the default gateway. Default gateway is the router that switches packets between different networks.**

**Since our destination address is located in remote network, the packet need to be sent to the default gateway.**

**Network layer handed down this packet to Data link layer. Data link layer appends header. It adds source and destination MAC address in header and FCS in tail. After this modification packet becomes frame.**

## How DHCP work

DHCP provides an automated way to distribute and update IP addresses and other configuration information on a network. A DHCP server provides this information to a DHCP client through the exchange of a series of messages, known as the DHCP conversation or the DHCP transaction.



### DHCP discovery

The client computers broadcasts messages on the physical subnet to discover available DHCP servers. This client-computers creates a User Datagram Protocol (UDP) packet with the default broadcast destination of 255.255.255.255 or the specific subnet broadcast address if any configured.

### DHCP offer

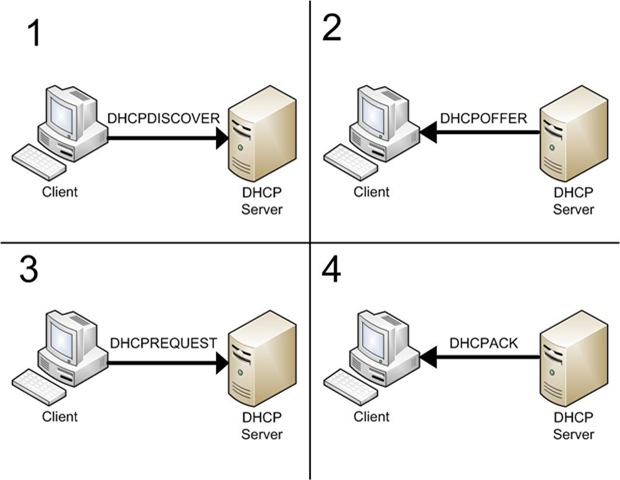
When a DHCP server receives an IP lease request from a client, it reserves an IP address for the client and extends an IP lease offer by sending a DHCPOFFER message to the client. This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer.

### DHCP request

In most companies, two DHCP servers provide fault tolerance of IP addressing if one server fails or must be taken offline for maintenance. So client could receive DHCP offers from multiple servers, but it will accept only one DHCP offer. In response to the offer Client requests the server. The client replies DHCP Request, unicast to the server, requesting the offered address. Based on the Transaction ID field in the request, servers are informed whose offer the client has accepted. When other DHCP servers receive this message, they withdraw any offers that they might have made to the client and return the offered address to the pool of available addresses. In some cases DHCP request message is broadcast, instead of being unicast to a particular DHCP server, because the DHCP client has still not received an IP address. Also, this way one message can let all other DHCP servers know that another server will be supplying the IP address without missing any of the servers with a series of unicast messages.

### DHCP acknowledgement

When the DHCP server receives the DHCPREQUEST message from the client, the configuration process enters its final phase.

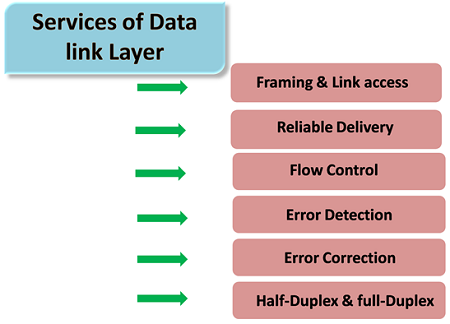


The acknowledgement phase involves sending a DHCPACK packet to the client. This packet includes the lease duration and any other configuration information that the client might have requested. At this point, the IP configuration process is completed.

# Data Link Layer

* **In the OSI model, the data link layer is a 4th layer from the top and 2nd layer from the bottom.**
* **The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.**
* **The main responsibility of the Data Link Layer is to transfer the datagram across an individual link.**
* **The Data link layer protocol defines the format of the packet exchanged across the nodes as well as the actions such as Error detection, retransmission, flow control, and random access.**
* **The Data Link Layer protocols are Ethernet, token ring, FDDI and PPP.**
* **An important characteristic of a Data Link Layer is that datagram can be handled by different link layer protocols on different links in a path. For example, the datagram is handled by Ethernet on the first link, PPP on the second link.**

### Following services are provided by the Data Link Layer:



* **Framing & Link access: Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link.**
* **Reliable delivery: Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.**
* **Flow control: A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.**
* **Error detection: Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.**
* **Error correction: Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.**
* **Half-Duplex & Full-Duplex: In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.**

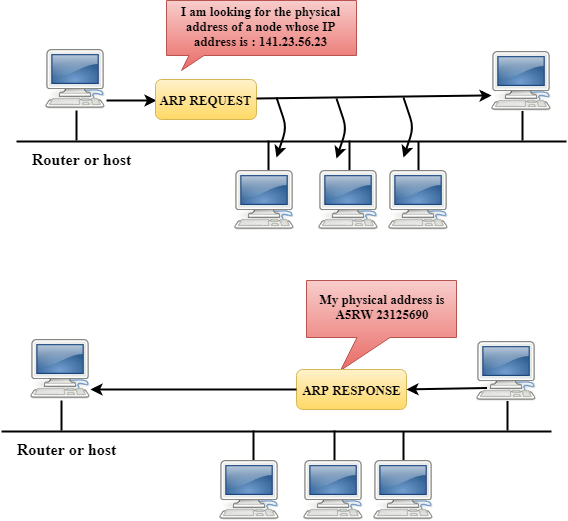
## ARP

* ARP stands for Address Resolution Protocol.
* It is used to associate an IP address with the MAC address.
* Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network. MAC address can be changed easily. For example, if the NIC on a particular machine fails, the MAC address changes but IP address does not change. ARP is used to find the MAC address of the node when an internet address is known.

#### Note: MAC address: The MAC address is used to identify the actual device. IP address: It is an address used to locate a device on the network.

### How ARP works

If the host wants to know the physical address of another host on its network, then it sends an ARP query packet that includes the IP address and broadcast it over the network. Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes the IP address and sends back the physical address. The host holding the datagram adds the physical address to the cache memory and to the datagram header, then sends back to the sender.



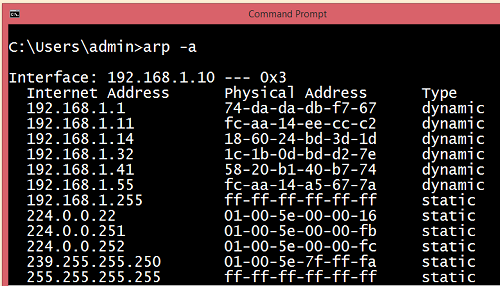
### Steps taken by ARP protocol

If a device wants to communicate with another device, the following steps are taken by the device:

* The device will first look at its internet list, called the ARP cache to check whether an IP address contains a matching MAC address or not. It will check the ARP cache in command prompt by using a command **arp-a**.



* If ARP cache is empty, then device broadcast the message to the entire network asking each device for a matching MAC address.
* The device that has the matching IP address will then respond back to the sender with its MAC address
* Once the MAC address is received by the device, then the communication can take place between two devices.
* If the device receives the MAC address, then the MAC address gets stored in the ARP cache. We can check the ARP cache in command prompt by using a command arp -a.



#### Note: ARP cache is used to make a network more efficient.

In the above screenshot, we observe the association of IP address to the MAC address.

### There are two types of ARP entries:

* **Dynamic entry:** It is an entry which is created automatically when the sender broadcast its message to the entire network. Dynamic entries are not permanent, and they are removed periodically.
* **Static entry:** It is an entry where someone manually enters the IP to MAC address association by using the ARP command utility.

## RARP

* RARP stands for **Reverse Address Resolution Protocol**.
* If the host wants to know its IP address, then it broadcast the RARP query packet that contains its physical address to the entire network. A RARP server on the network recognizes the RARP packet and responds back with the host IP address.
* The protocol which is used to obtain the IP address from a server is known as **Reverse Address Resolution Protocol**.
* The message format of the RARP protocol is similar to the ARP protocol.
* Like ARP frame, RARP frame is sent from one machine to another encapsulated in the data portion of a frame.

