## UNIT I FUNDAMENTALS AND PHYSICAL LAYER

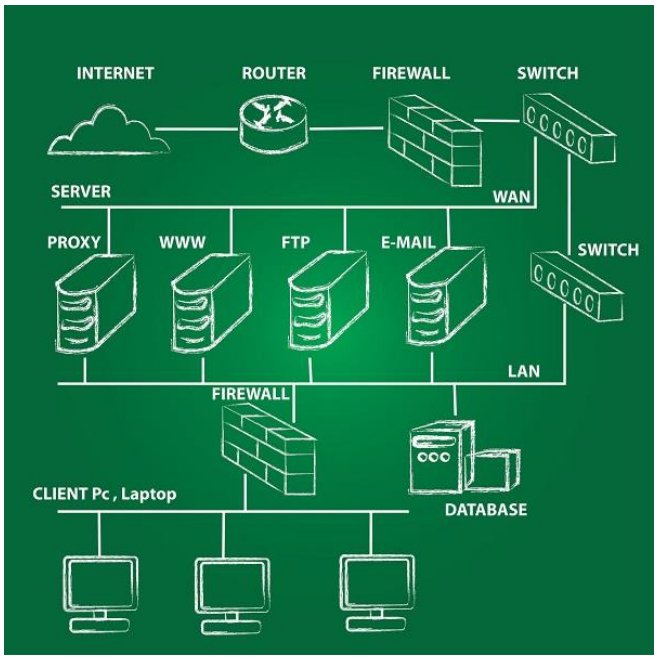
Computer Network Developments- Network Terms and Components-Network Topology-Standards-ISO/OSI layers-TCP/IP layers-, Transmission Media, LAN: Wired LAN, Wireless LANs, Connecting LAN and Virtual LAN, Techniques for Bandwidth utilization: Multiplexing - Frequency division, Time division and Wave division, Concepts on spread spectrum.

### Computer Network Developments

ARPANET - the First Network

**ARPANET − Advanced Research Projects Agency Network** − the granddad of Internet was a network established by the US Department of Defense (DOD). The work for establishing the network started in the early 1960s and DOD sponsored major research work, which resulted in development on initial protocols, languages and frameworks for network communication.

It had four nodes at University of California at Los Angeles (UCLA), Stanford Research Institute (SRI), University of California at Santa Barbara (UCSB) and University of Utah. On October 29, 1969, the first message was exchanged between UCLA and SRI. E-mail was created by Roy Tomlinson in 1972 at Bolt Beranek and Newman, Inc. (BBN) after UCLA was connected to BBN.




Internet

ARPANET expanded to connect DOD with those universities of the US that were carrying out defense-related research. It covered most of the major universities across the country. The concept of networking got a boost when University College of London (UK) and Royal Radar Network (Norway) connected to the ARPANET and a network of networks was formed.

The term Internet was coined by Vinton Cerf, Yogen Dalal and Carl Sunshine of Stanford University to describe this network of networks. Together they also developed protocols to facilitate information exchange over the Internet. Transmission Control Protocol (TCP) still forms the backbone of networking.

## Telenet

Telenet was the first commercial adaptation of ARPANET introduced in 1974. With this the concept of Internet Service Provider (ISP) was also introduced. The main function of an ISP is to provide uninterrupted Internet connection to its customers at affordable rates.

## World Wide Web

With commercialization of internet, more and more networks were developed in different part of the world. Each network used different protocols for communicating over the network. This prevented different networks from connecting together seamlessly. In the 1980s, Tim Berners-Lee led a group of Computer scientists at CERN, Switzerland, to create a seamless network of varied networks, called the World Wide Web (WWW).

World Wide Web is a complex web of websites and web pages connected together through hypertexts. Hypertext is a word or group of words linking to another web page of the same or different website. When the hypertext is clicked, another web page opens.

The evolution from ARPANET to WWW was possible due to many new achievements by researchers and computer scientists all over the world. Here are some of those developments –

| Year | Milestone |
| --- | --- |

| | |
|---|---|
| 1957 | Advanced Research Project Agency formed by US |
| 1969 | ARPANET became functional |
| 1970 | ARPANET connected to BBNs |
| 1972 | Roy Tomlinson develops network messaging or E-mail. Symbol @ comes to mean "at" |
| 1973 | APRANET connected to Royal Radar Network of Norway |
| 1974 | Term Internet coined<br>First commercial use of ARPANET, Telenet, is approved |
| 1982 | TCP/IP introduced as standard protocol on ARPANET |
| 1983 | Domain Name System introduced |
| 1986 | National Science Foundation brings connectivity to more people with its NSFNET program |
| 1990 | ARPANET decommissioned<br>First web browser Nexus developed<br>HTML developed |
| 2002-2004 | Web 2.0 is born |

## Network Terms and Components

### Channel

Physical medium like cables over which information is exchanged is called **channel**. Transmission channel may be **analog** or **digital**. As the name suggests, analog channels transmit data using **analog signals** while digital channels transmit data using **digital signals**.

In popular network terminology, path over which data is sent or received is called **data channel**. This data channel may be a tangible medium like copper wire cables or broadcast medium like **radio waves**.

## Data Transfer Rate

The speed of data transferred or received over transmission channel, measured per unit time, is called data transfer rate. The smallest unit of measurement is bits per second (bps). 1 bps means 1 bit (0 or 1) of data is transferred in 1 second.

Here are some commonly used data transfer rates −

- 1 Bps = 1 Byte per second = 8 bits per second
- 1 kbps = 1 kilobit per second = 1024 bits per second
- 1 Mbps = 1 Megabit per second = 1024 Kbps
- 1 Gbps = 1 Gigabit per second = 1024 Mbps

## Bandwidth

Data transfer rates that can be supported by a network is called its bandwidth. It is measured in bits per second (bps). Modern day networks provide bandwidth in Kbps, Mbps and Gbps. Some of the factors affecting a network's bandwidth include −

- Network devices used
- Protocols used
- Number of users connected
- Network overheads like collision, errors, etc.

## Throughput

Throughput is the actual speed with which data gets transferred over the network. Besides transmitting the actual data, network bandwidth is used for transmitting error messages, acknowledgement frames, etc.

Throughput is a better measurement of network speed, efficiency and capacity utilization rather than bandwidth.

## Protocol

Protocol is a set of rules and regulations used by devices to communicate over the network. Just like humans, computers also need rules to ensure successful communication. If two people start speaking at the same time or in different languages when no interpreter is present, no meaningful exchange of information can occur.

Similarly, devices connected on the network need to follow rules defining situations like when and how to transmit data, when to receive data, how to give error-free message, etc.

Some common protocols used over the Internet are −

- Transmission Control Protocol
- Internet Protocol
- Point to Point Protocol
- File Transfer Protocol
- Hypertext Transfer Protocol
- Internet Message Access Protocol

## Network Devices

Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called **network devices**. These devices transfer data in a fast, secure and correct way over same or different networks. Network devices may be inter-network or intra-network. Some devices are installed on the device, like NIC card or RJ45 connector, whereas some are part of the network, like router, switch, etc. Let us explore some of these devices in greater detail.

### Modem

Modem is a device that enables a computer to send or receive data over telephone or cable lines. The data stored on the computer is digital whereas a telephone line or cable wire can transmit only analog data.

The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices − **modulator** and **demodulator**. The **modulator** converts digital data into analog data when the data is being sent by the computer. The **demodulator** converts analog data signals into digital data when it is being received by the computer.

### Types of Modem

Modem can be categorized in several ways like direction in which it can transmit data, type of connection to the transmission line, transmission mode, etc.

Depending on direction of data transmission, modem can be of these types −

- **Simplex** − A simplex modem can transfer data in only one direction, from digital device to network (modulator) or network to digital device (demodulator).
- **Half duplex** − A half-duplex modem has the capacity to transfer data in both the directions but only one at a time.
- **Full duplex** − A full duplex modem can transmit data in both the directions simultaneously.

## RJ45 Connector

RJ45 is the acronym for **Registered Jack 45. RJ45 connector** is an 8-pin jack used by devices to physically connect to **Ethernet** based **local area networks (LANs)**. **Ethernet** is a technology that defines protocols for establishing a LAN. The cable used for Ethernet LANs are twisted pair ones and have **RJ45 connector pins** at both ends. These pins go into the corresponding socket on devices and connect the device to the network.

## Ethernet Card

**Ethernet card**, also known as **network interface card (NIC)**, is a hardware component used by computers to connect to **Ethernet LAN** and communicate with other devices on the LAN. The earliest **Ethernet cards** were external to the system and needed to be installed manually. In modern computer systems, it is an internal hardware component. The NIC has **RJ45 socket** where network cable is physically plugged in.

**Ethernet card speeds** may vary depending upon the protocols it supports. Old Ethernet cards had maximum speed of **10 Mbps**. However, modern cards support fast Ethernets up to a speed of **100 Mbps**. Some cards even have capacity of **1 Gbps**.

## Router

A **router** is a **network layer** hardware device that transmits data from one LAN to another if both networks support the same set of protocols. So a **router** is typically connected to at least two LANs and the **internet service provider** (ISP). It receives its data in the form of **packets**, which are **data frames** with their **destination address** added. Router also strengthens the signals before transmitting them. That is why it is also called **repeater**.

Routing Table

A router reads its routing table to decide the best available route the packet can take to reach its destination quickly and accurately. The routing table may be of these two types −

- **Static** − In a static routing table the routes are fed manually. So it is suitable only for very small networks that have maximum two to three routers.
- **Dynamic** − In a dynamic routing table, the router communicates with other routers through protocols to determine which routes are free. This is suited for larger networks where manual feeding may not be feasible due to large number of routers.

## Switch

**Switch** is a network device that connects other devices to **Ethernet** networks through **twisted pair** cables. It uses **packet switching** technique to **receive, store** and **forward data packets** on the network. The switch maintains a list of network addresses of all the devices connected to it.

On receiving a packet, it checks the destination address and transmits the packet to the correct port. Before forwarding, the packets are checked for collision and other network errors. The data is transmitted in full duplex mode

Data transmission speed in switches can be double that of other network devices like hubs used for networking. This is because switch shares its maximum speed with all the devices connected to it. This helps in maintaining network speed even during high traffic. In fact, higher data speeds are achieved on networks through use of multiple switches.

### Gateway

**Gateway** is a network device used to connect two or more dissimilar networks. In networking parlance, networks that use different protocols are **dissimilar networks**. A gateway usually is a computer with multiple **NICs** connected to different networks. A gateway can also be configured completely using software. As networks connect to a different network through gateways, these gateways are usually hosts or end points of the network.

**Gateway** uses **packet switching** technique to transmit data from one network to another. In this way it is similar to a **router**, the only difference being router can transmit data only over networks that use same protocols.

### Wi-Fi Card

**Wi-Fi** is the acronym for **wireless fidelity. Wi-Fi technology** is used to achieve **wireless connection** to any network. **Wi-Fi card** is a **card** used to connect any device to the local network wirelessly. The physical area of the network which provides internet access through Wi-Fi is called **Wi-Fi hotspot**. Hotspots can be set up at home, office or any public space. Hotspots themselves are connected to the network through wires.

A **Wi-Fi card** is used to add capabilities like **teleconferencing, downloading** digital camera images, **video chat**, etc. to old devices. Modern devices come with their in-built **wireless network adapter**.

## Network Topology

The way in which devices are interconnected to form a network is called network topology. Some of the factors that affect choice of topology for a network are −

- **Cost** − Installation cost is a very important factor in overall cost of setting up an infrastructure. So cable lengths, distance between nodes, location of servers, etc. have to be considered when designing a network.
- **Flexibility** − Topology of a network should be flexible enough to allow reconfiguration of office set up, addition of new nodes and relocation of existing nodes.
- **Reliability** − Network should be designed in such a way that it has minimum down time. Failure of one node or a segment of cabling should not render the whole network useless.
- **Scalability** − Network topology should be scalable, i.e. it can accommodate load of new devices and nodes without perceptible drop in performance.

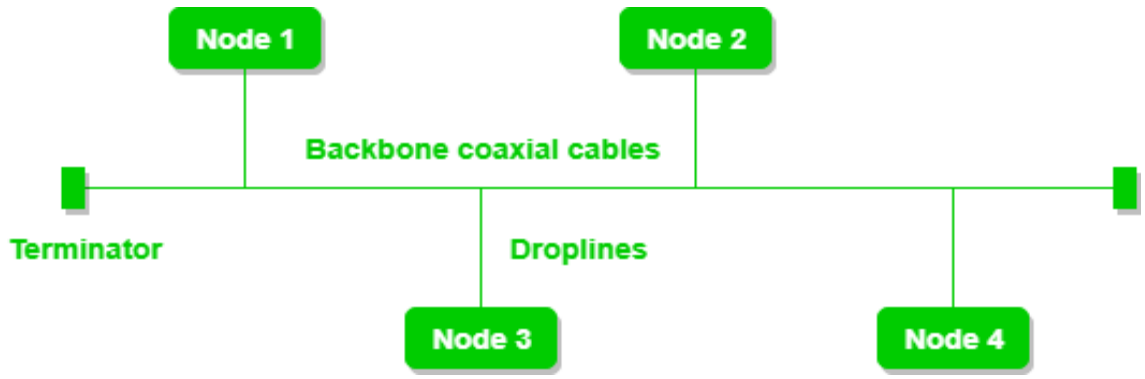
- **Ease of installation** − Network should be easy to install in terms of hardware, software and technical personnel requirements.
- **Ease of maintenance** − Troubleshooting and maintenance of network should be easy.

There are Five types of Network Topology, it includes

- Bus Topology
- Ring Topology
- Star Topology
- Mesh Topology
- Hybrid Topology

**Bus Topology**

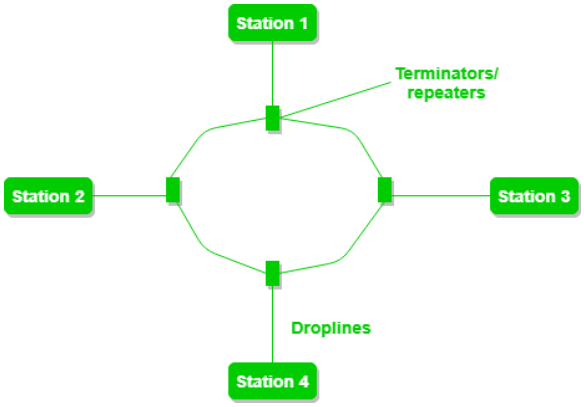
Bus topology is a network type in which every computer and network device is connected to single cable. It transmits the data from one end to another in single direction. No bi-directional feature is in bus topology.




**Ring Topology**

In this topology, it forms a ring connecting devices with its exactly two neighboring devices. A number of repeaters are used for Ring topology with a 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.

The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.




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

**Advantages of this topology :**

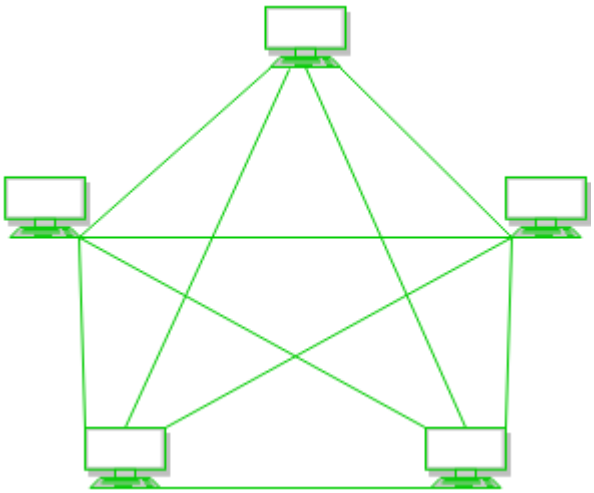
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

**Problems with this topology :**

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

**Mesh Topology :**

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



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

**Advantages of this topology :**

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

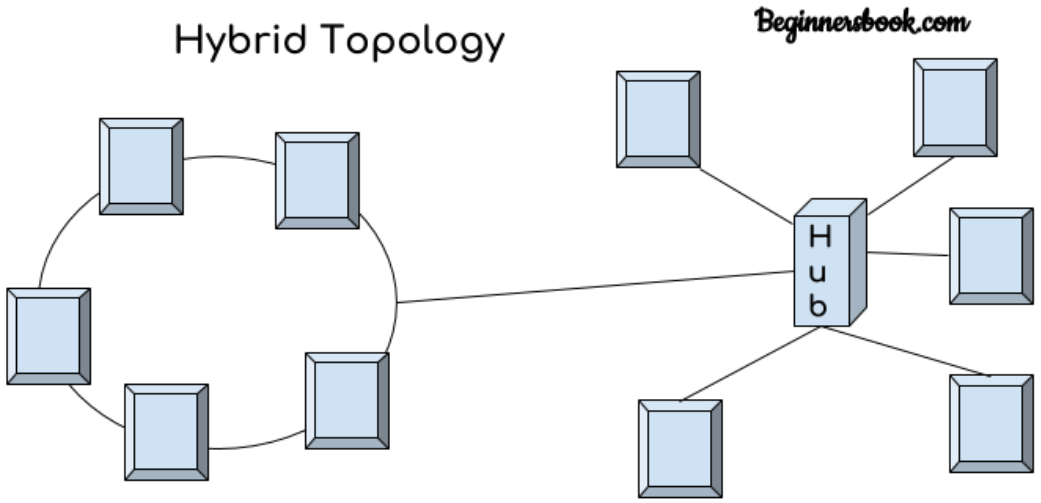
**Problems with this topology :**

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

**Hybrid topology**

A combination of two or more topology is known as hybrid topology.

For example a combination of star and mesh topology is known as hybrid topol




**Advantages of Hybrid topology**

1. We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.
2. Scalable as we can further connect other computer networks with the existing networks with different topologies.

**Disadvantages of Hybrid topology**

1. Fault detection is difficult.
2. Installation is difficult.
3. Design is complex so maintenance is high thus expensive.

## Standards

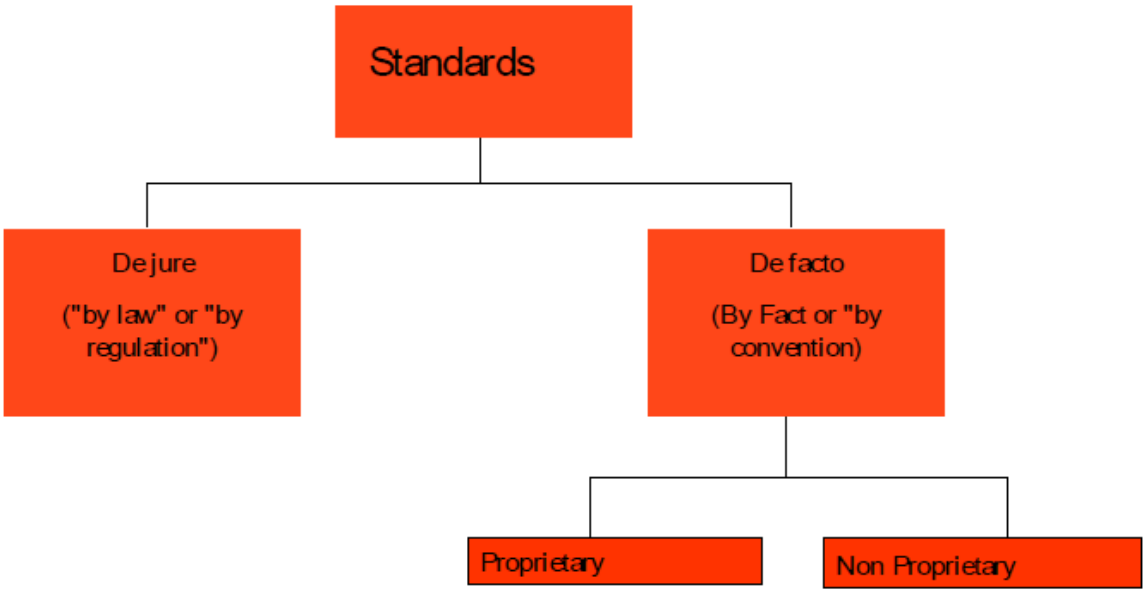
- A standard provides a model for development that makes it possible for a product to work regardless of the individual manufacturer."

Standards are essential in:

- 1. Creating/Maintaining Open and Competitive Markets.
- 2. Guaranteeing National/International Interoperability of data and telecommunications technology and processes.

• Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

**Types of Standards**




De jure

- Those standards that have been legislated by an officially recognized body.

De facto

- Standards that have not been approved by an organized body but have been adopted as standards through widespread use.
- De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

De facto - Proprietary (Closed Standards)

- Standards that are originally invented by a commercial organization as a basis for the operation of its product.
- They are wholly owned by the company.
- They are also called Closed Standards because they close off communication systems. e.g. IGRP & EIGRP Routing Protocols.

Non Proprietary (Open Standards)

• They are originally developed by groups or communities that have passed them into public domains.

• They are also called Open standards because they open communication between different systems.

Standards organizations

Standards are developed mainly by 3 entities:

• Standard Creation Committees

• Forums

• Regulatory Agencies

**Standards creation Communities**

1. **ISO (International Organization for Standards)**

The International Organization for Standardization widely known as ISO, is an international standard-setting body composed of representatives from various national standards organizations. Founded on February 23, 1947, the organization promulgates worldwide proprietary industrial and commercial standards. It has its headquarters in Geneva, Switzerland. While ISO defines itself as a non-governmental organization, its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most non-governmental organizations. In practice, ISO acts as a consortium with strong links to governments ISO, is an international standard-setting body composed of representatives from various national standards organizations the organization promulgates worldwide proprietary industrial and commercial standards.ISO's main products are the International Standards. ISO also publishes Technical Reports, Technical Specifications, Publicly Available Specifications, Technical Corrigenda, and Guides.

2. **ITU (International Telecommunications Union - formerly CCITT)**

The International Telecommunication Union is the specialized agency of the United Nations which is responsible for information and communication technologies. ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards. ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards.ITU also organizes worldwide and regional exhibitions and forums, such as ITU TELECOM WORLD, bringing together representatives of government and the telecommunications and ICT industry to exchange ideas, knowledge and technology.The ITU is active in areas including broadband Internet, latest-generation wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, convergence in fixed-mobile phone, Internet access, data, voice, TV broadcasting, and next-generation networks.

3. **ANSI(American National Standards Institute) standard.**

Though ANSI itself does not develop standards, the Institute oversees the development and use of standards by accrediting the procedures of standards developing organizations ANSI accreditation signifies that the procedures used by standards developing organizations meet the Institute's requirements for openness, balance, consensus, and due process. ANSI was originally formed in 1918, when five engineering societies and three government agencies founded the American Engineering Standards Committee (AESC). In 1928, the AESC became the American Standards Association (ASA). In 1966, the ASA was reorganized and became the United States of America Standards Institute (USASI). The present name was adopted in 1969.Prior to 1918, these five engineering societies:

- American Institute of Electrical Engineers (AIEE, now IEEE)
- American Society of Mechanical Engineers (ASME)
- American Society of Civil Engineers (ASCE)
- American Institute of Mining Engineers (AIME, now American Institute of Mining, Metallurgical, and Petroleum Engineers)
- American Society for Testing and Materials (now ASTM International)

ANSI also designates specific standards as American National Standards, or ANS, when the Institute determines that the standards were developed in an environment that is equitable, accessible and responsive to the requirements of various stakeholders. The American National Standards process involves:

- Consensus by a group that is open to representatives from all interested parties
- Broad-based public review and comment on draft standards
- consideration of and response to comments
- Incorporation of submitted changes that meet the same consensus requirements into a draft standard
- Availability of an appeal by any participant alleging that these principles were not respected during the standards-development process.

4. **IEEE (Institute of Electrical and Electronics Engineers)** IEEE's Constitution defines the purposes of the organization as "scientific and educational, directed toward the advancement of the theory and practice of Electrical, Electronics, Communications and Computer Engineering, as well as Computer Science, the allied branches of engineering and the related arts and sciences." The IEEE is incorporated under the Not-for-Profit Corporation Law of the state of New York, United States. It was formed in 1963 by the merger of the Institute of Radio Engineers (IRE, founded 1912) and the American Institute of Electrical Engineers (AIEE, founded 1884). It has more than 400,000 members in more than 160 countries, 45% outside the United States.In pursuing these goals, the IEEE serves as a major publisher of scientific journals and a conference organizer. It is also a leading developer of industrial standards (having developed over 900 active industry standards) in a broad range of disciplines, including electric power and energy, biomedical technology and health care, information technology, information assurance, telecommunications, consumer electronics, transportation, aerospace, and nanotechnology. IEEE develops and participates in educational activities such as accreditation of electrical engineering programs in institutes of higher learning.

IEEE is one of the leading standards-making organizations in the world. IEEE performs its standards making and maintaining functions through the IEEE Standards Association (IEEE-SA). IEEE standards affect a wide range of industries including: power and energy, biomedical and health care, Information Technology (IT), telecommunications,

transportation, nanotechnology, information assurance, and many more. In 2005, IEEE had close to 900 active standards, with 500 standards under development. One of the more notable IEEE standards is the IEEE 802 LAN/MAN group of standards which includes the IEEE 802.3 Ethernet standard and the IEEE 802.11 Wireless Networking

5. **EIA (Electronic Industries Association)**

The Electronic Industries Alliance (EIA, until 1997 Electronic Industries Association) was a standards and trade organization composed as an alliance of trade associations for electronics manufacturers in the United States. They developed standards to ensure the equipment of different manufacturers was compatible and interchangable.In 1924 the Associated Radio Manufacturers alliance was formed, which was renamed to Radio Manufacturers Association (RMA) the same year. Upcoming new electronic technologies brought new members and further name changes: Radio Television Manufacturers Association (RTMA) (1950), Radio Electronics Television Manufacturers (RETMA) (1953) and Electronics Industries Association (EIA) (1957). The last renaming took place in 1997, when EIA became Electronics Industries Alliance (EIA), reflecting the change away from a pure manufacturers associationA standard defining serial communication between computers and modems e. g. was originally drafted by the radio sector as RS-232. Later it was taken over by the EIA as EIA-232. Later this standard was managed by the TIA and the name was changed to the current TIA-232. Because the EIA was accredited by ANSI to help develop standards in its areas, the standards are often described as e. g. ANSI TIA-232(or formerly as ANSI EIA/TIA-232').

Forums

- 1. Frame Relay Forum
- 2. ATM Forum & ATM consortium
- 3. Internet Society (ISOC) & Internet Engineering Task Force (IETF)

**Regularity Agencies:**

- 1. Federal Communication commission

**Introduction to OSI reference Model**

- The International Organization for Standardization (ISO) developed the Open Systems Interconnection (OSI) reference model in 1977 and finally 1983.
- It has since become the most widely accepted model for understanding

network communication.

- The OSI model attempts to define rules that apply to the following issues:
  - How network devices connect and communicate each other even their languages are different at the same time how it makes a connection between the each device.
  - The methods is used for which device on a network knows when the data to be transmitted and when the data not to be transmitted.
  - Methods to ensure that network transmissions are received correctly and by the right recipient
  - How the physical transmission media are arranged and connected
  - How to ensure that network devices maintain a proper rate of data flow
  - How bits are represented on the network media
  - The OSI model does not work or perform any particular functions in the communications process but the actual work is done by the SW and HW.
  - It also defines which tasks need to be done and which protocols will handle those tasks each of the seven layers.
  - It divides the tasks into several subtasks.
  - The subtasks will be fulfilled by the specific protocols at the specific layer of the OSI model.
  - Protocol stack is also possible i.e when protocols are grouped together to complete a task
  - Each layer of the OSI model has a different protocols are with it. When more than one protocol is need to complete a task, that time the protocols are grouped

    e.g TCP/IP

## Protocols

- The network consists of many other computing platforms running on different version, different Operating System and Application software. So that the network cannot find out which computer has which operating system and AS, So that the common languages is needed to understand each other in different computer.
- That's why the common languages are made, that languages are called

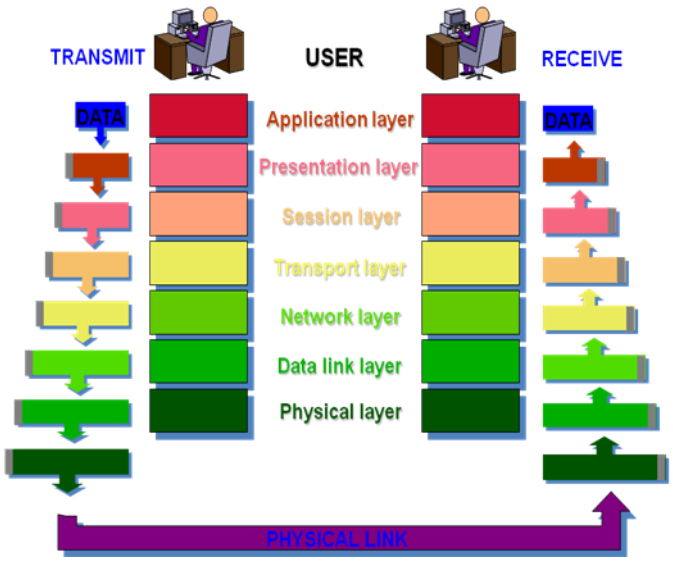
protocol. It is a standard set of instructions and procedures according to communication take place.

- Through this protocol the computer agreed upon ways that computers exchange information.

## Open Systems Interconnection (OSI)

- "The OSI model for network protocols is well-designed and very interoperable."
- "It was developed too late to be accepted by the principal communications customers in industry and the military, who had already invested heavily in TCP/IP."
- And while serving as a good framework for protocols it is not ideal for actual high speed implementations.

## THE 7 LAYERS OF OSI




### 1. Physical Layer (Layer 1) :

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

The functions of the physical layer are :

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

* Hub, Repeater, Modem, Cables are Physical Layer devices.
** Network Layer, Data Link Layer and Physical Layer are also known as **Lower Layers** or **Hardware Layers**.

### 2. Data Link Layer (DLL) (Layer 2) :

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

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

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

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

The functions of the data Link layer are :

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

** Packet in Data Link layer is referred as **Frame**.*
*** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.*
**** Switch & Bridge are Data Link Layer devices.*

## 3. Network Layer (Layer 3) :

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

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

* *Segment* in Network layer is referred as **Packet**.
** Network layer is implemented by networking devices such as routers.

## 4. Transport Layer (Layer 4) :

Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.
**• At sender's side:**
Transport layer receives the formatted data from the upper layers,
performs **Segmentation** and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.
Note: The sender need to know the port number associated with the receiver's application. Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.
**• At receiver's side:**
Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.
The functions of the transport layer are :

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

The services provided by the transport layer :

1. **Connection Oriented Service:** It is a three-phase process which include
   – Connection Establishment

– Data Transfer
– Termination / disconnection
In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.

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

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

## 5. Session Layer (Layer 5) :

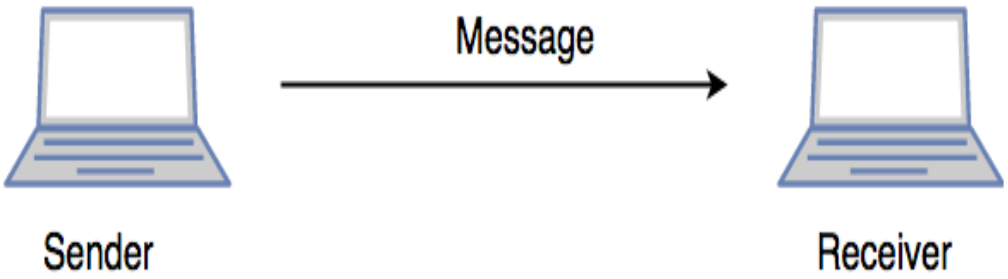
This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
The functions of the session layer are :

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

***All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as "Application Layer".*
***Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers** or **Software Layers**.*

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

be transmitted.




### 6. Presentation Layer (Layer 6) :

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

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

### 7. Application Layer (Layer 7) :

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

The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented in the Internet because of its late invention. Current model being used is the TCP/IP model.

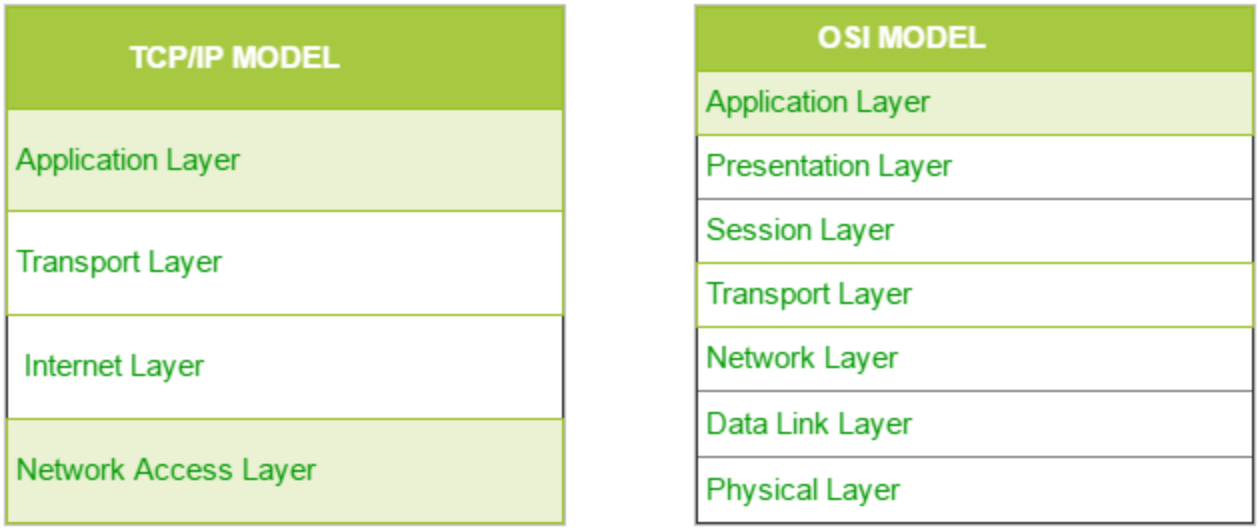
## TCP/IP MODEL

The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it

was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol.
The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :




Difference between TCP/IP and OSI Model:

| TCP/IP | OSI |
|---|---|
| TCP refers to Transmission Control Protocol. | OSI refers to Open Systems Interconnection. |
| TCP/IP has 4 layers. | OSI has 7 layers. |

| | |
|---|---|
| TCP/IP is more reliable | OSI is less reliable |
| TCP/IP does not have very strict boundaries. | OSI has strict boundaries |
| TCP/IP follow a horizontal approach. | OSI follows a vertical approach. |
| TCP/IP uses both session and presentation layer in the application layer itself. | OSI uses different session and presentation layers. |
| TCP/IP developed protocols then model. | OSI developed model then protocol. |
| Transport layer in TCP/IP does not provide assurance delivery of packets. | In OSI model, transport layer provides assurance delivery of packets. |
| TCP/IP model network layer only provides connection less services. | Connection less and connection oriented both services are provided by network layer in OSI model. |
| Protocols cannot be replaced easily in TCP/IP model. | While in OSI model, Protocols are better covered and is easy to replace with the change in technology. |

The first layer is the Process layer on the behalf of the sender and Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

### 1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

### 2. Internet Layer –

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:
   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

### 3. Host-to-Host Layer –

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

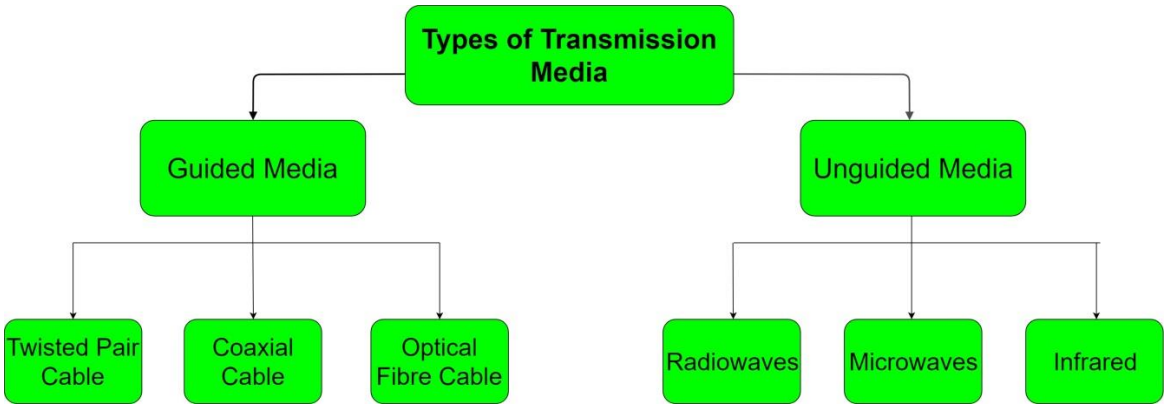
### 4. Application Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

## Transmission Media

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:




**1. Guided Media:**
It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.
Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

**(i) Twisted Pair Cable –**
It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

1. **Unshielded Twisted Pair (UTP):**
   This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.
   Advantages:
   - Least expensive
   - Easy to install
   - High speed capacity
   - Susceptible to external interference
   - Lower capacity and performance in comparison to STP
   - Short distance transmission due to attenuation
2. **Shielded Twisted Pair (STP):**
   This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.
   Advantages:
   - Better performance at a higher data rate in comparison to UTP
   - Eliminates crosstalk
   - Comparitively faster
   - Comparitively difficult to install and manufacture
   - More expensive
   - Bulky

**(ii) Coaxial Cable –**
It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. Coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.
Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive
  Disadvantages:

- Single cable failure can disrupt the entire network

**(iii) Optical Fibre Cable –**
It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for transmission of large volumes of data.
The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

Advantages:

- Increased capacity and bandwidth
- Light weight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile

**2. Unguided Media:**

It is also referred to as Wireless or Unbounded transmission media.No physical medium is required for the transmission of electromagnetic signals.

Features:

- Signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 major types of Unguided Media:

**(i) Radiowaves –**

These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radiowaves for transmission.

Further Categorized as (i) Terrestrial and (ii) Satellite.

**(ii) Microwaves –**

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

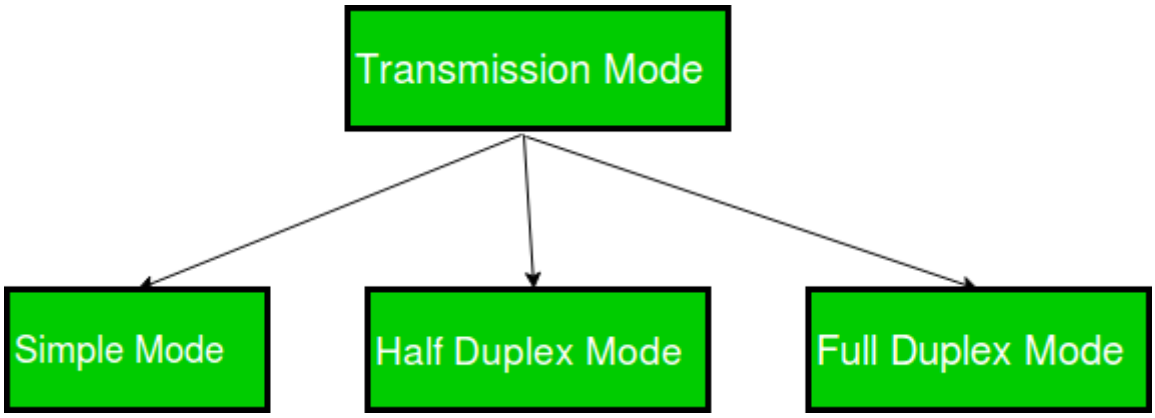
**(iii) Infrared –**

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

## TRANSMISSION MODE:

Transmission mode means transferring of data between two devices. It is also known as communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected. There are three types of transmission mode:-

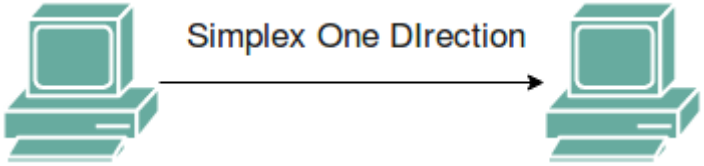
- **Simplex Mode**
- **Half-Duplex Mode**
- **Full-Duplex Mode**




**Simplex Mode**

In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.

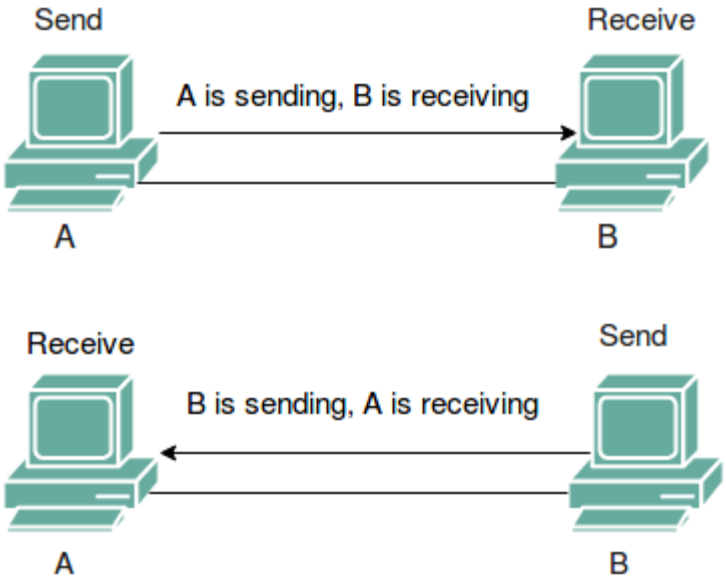
Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.




**Half-Duplex Mode**

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both direction at the same time. The entire capacity of the channel can be utilized for each direction.

Example: Walkie- talkie in which message is sent one at a time and messages are sent in both the directions.



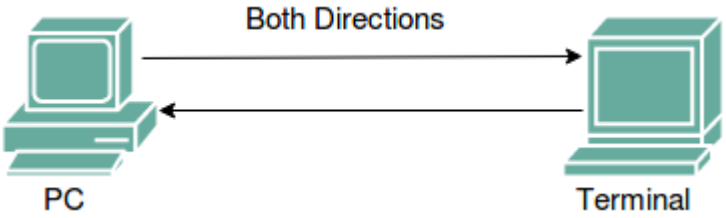
**Full-Duplex Mode**

In full-duplex mode, both stations can transmit and receive simultaneously. In full_duplex mode, signals going in one direction share the capacity of the link with signals going in other direction, this sharing can occur in two ways:

- Either the link must contain two physically separate transmission paths, one for sending and other for receiving.
- Or the capacity is divided between signals travelling in both directions.

Full-duplex mode is used when communication in both direction is required all the time. The capacity of the channel, however must be divided between the two directions.

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




LAN: Wired LAN, Wireless LANs, Connecting LAN and Virtual LAN

- Computer networks for the home and small business use either wired or wireless technology.
- Wired LANs use Ethernet cables and network adapters.
- Two computers can be wired to each other using an Ethernet crossover cable.
- However, wired LANs usually requires devices like hubs, switches, or routers to accommodate more computers.
- Popular WLAN technologies follow one of the three main Wi-Fi communication standards. The benefits of wireless networking depend on the standard employed:
- 802.11b was the first standard to be widely used in WLANs.
- The 802.11a standard is faster but more expensive than 802.11b. The 802.11a standard is commonly found in business networks.
- A common standard, 802.11g, attempts to combine the best of 802.11a and 802.11b. However, it's a more expensive home networking option.
- The newest standard, 802.11ac, operates on the 5 GHz band and offers speeds of more than 3 Gb/s.

| **Wired LAN** | **Wireless LAN** |
|---|---|
| Close proximity to the router is required. | More freedom (within range). |

| | |
|---|---|
| Increased security. | Security risks. |
| Greater control. | Flexibility. |
| Every device must be hard-wired. | Wireless |
| A time-consuming process. | Easy process |
| Takes time for installation | Quick installation |
| Software is used | No use of such software |
| Sufficient for multiple use | Multiple devices decrease speed. |
| Doesn't support firewalls. | Built-in firewall capability. |

**CONNECTING LAN**

1.Those which operate below the physical layer such as a passive hub.

2. Those which operate at the physical layer (a repeater or an active hub).

3. Those which operate at the physical and data link layers (a bridge or a two-layer switch).

4. Those which operate at the physical, data link, and network layers (a router or a three-layer switch).

5. Those which can operate at all five layers (a gateway).

PASSIVE HUBS

- A passive hub is just a connector. It connects the wires coming from different branches.
- In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point.
- This type of a hub is part of the media; its location in the Internet model is below the physical layer.

REPEATERS

- A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data.
- A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern.

Active Hubs

- An active hub is actually a multipart repeater. It is normally used to create connections Between stations in a physical star topology.

Bridges

- A bridge operates in both the physical and the data link layer.
- As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can
- check the physical (MAC) addresses (source and destination) contained in the frame.

ROUTER

- A router is a three-layer device that routes packets based on their logical addresses
- (host-to-host addressing). A router normally connects LANs and WANs in the Internet
- and has a routing table that is used for making decisions about the route. The routing tables are normally dynamic and are updated using routing protocols.

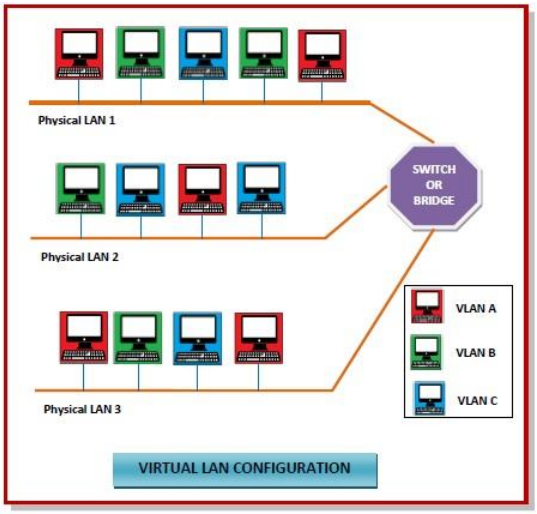
GATEWAY

- A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model.
- A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internetworks that use different models.

For example, a network designed to use the OSI model can be connected to another network using the Internet model. The gateway connecting the two systems can take a frame as it arrives from the first system, move it up to the OSI application layer, and remove the message

**VIRTUAL LAN**

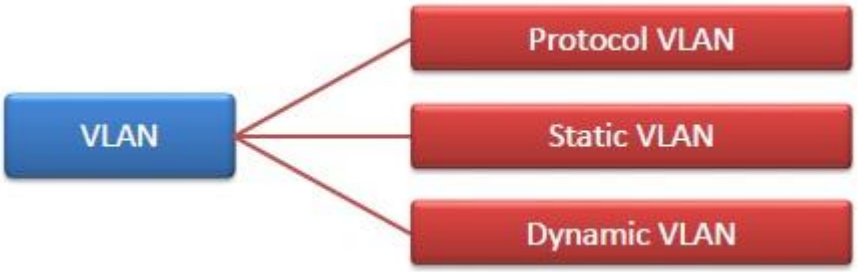
- Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of
- computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network.
- Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprise of a subset of ports on a single or multiple switches or bridges.
- This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.




FEATURES OF LAN

- A VLAN forms sub-network grouping together devices on separate physical LANs.
- VLAN's help the network manager to segment LANs logically into different broadcast domains.
- VLANs function at layer 2, i.e. Data Link Layer of the OSI model.
- There may be one or more network bridges or switches to form multiple, independent VLANs.
- Using VLANs, network administrators can easily partition a single switched network into multiple networks depending upon the functional and security requirements of their systems.
- VLANs eliminate the requirement to run new cables or reconfiguring physical connections in the present network infrastructure.
- VLANs help large organizations to re-partition devices aiming improved traffic management.
- VLANs also provide better security management allowing partitioning of devices according to their security criteria and also by ensuring a higher degree of control connected devices.
- VLANs are more flexible than physical LANs since they are formed by logical connections. This aids is quicker and cheaper reconfiguration of devices when the logical partitioning needs to be changed.

Types of VLAN



- **Protocol VLAN** − Here, the traffic is handled based on the protocol used. A switch or bridge segregates, forwards or discards frames the come to it based upon the traffics protocol.
- **Port-based VLAN** − This is also called static VLAN. Here, the network administrator assigns the ports on the switch / bridge to form a virtual network.
- **Dynamic VLAN** − Here, the network administrator simply defines network membership according to device characteristics.

## TECHNIQUES FOR BANDWIDTH UTILIZATION

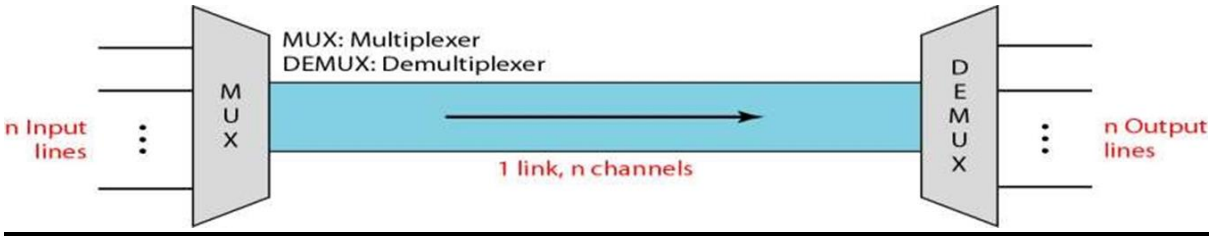
- **Bandwidth** describes the maximum data transfer rate of a network or Internet connection.
- It measures how much data can be sent over a specific connection in a given amount of time.
- For example, a gigabit Ethernet connection has a **bandwidth** of 1,000 Mbps

MULTIPLEXING

- It is the process of combining **multiple signals into one signal**, over a **shared medium**.

- Communication is possible over the air (radio frequency), using a physical media (cable), and light (optical fiber). All mediums are capable of multiplexing.
- **Multiplexing** is achieved by using a device called **Multiplexer** (**MUX**) that combines n input lines to generate a single output line. i.e. many-to-one.
- **Demultiplexing** is the reverse process of multiplexing achieved by using a device called **Demultiplexer** (**DEMUX**) i.e. one-to-many.
- **Multiplexing** was originally developed in the 1800s for telegraphy.

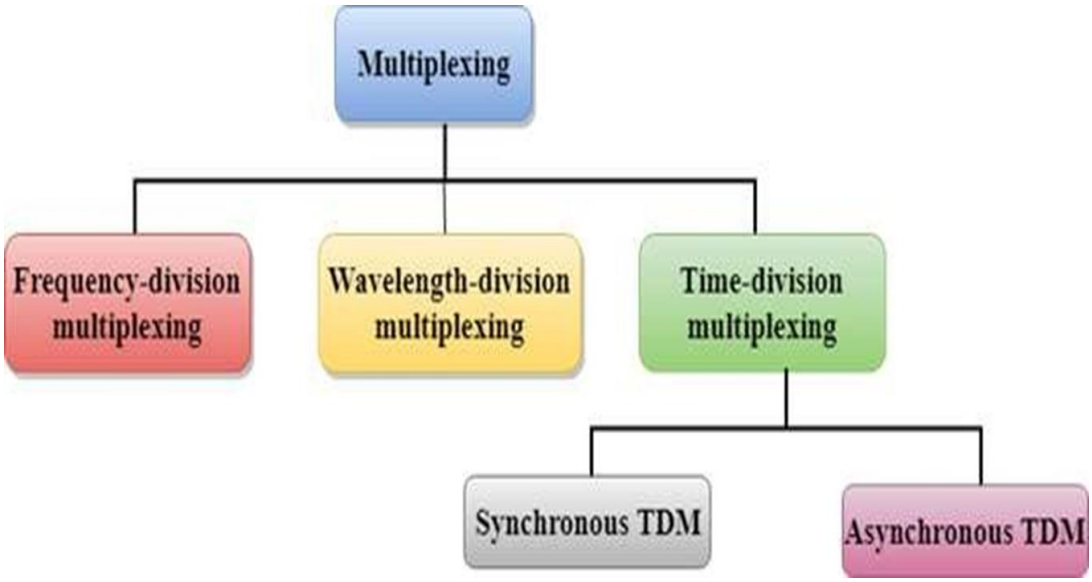
**Multiplexing** is widely **used** in many telecommunications applications, including **telephony, internet communications, digital broadcasting and wireless telephony**




- The word **channel refers to the portion of a link that carries a transmission** between a given pair of lines. One link can have many (*n) channels.*

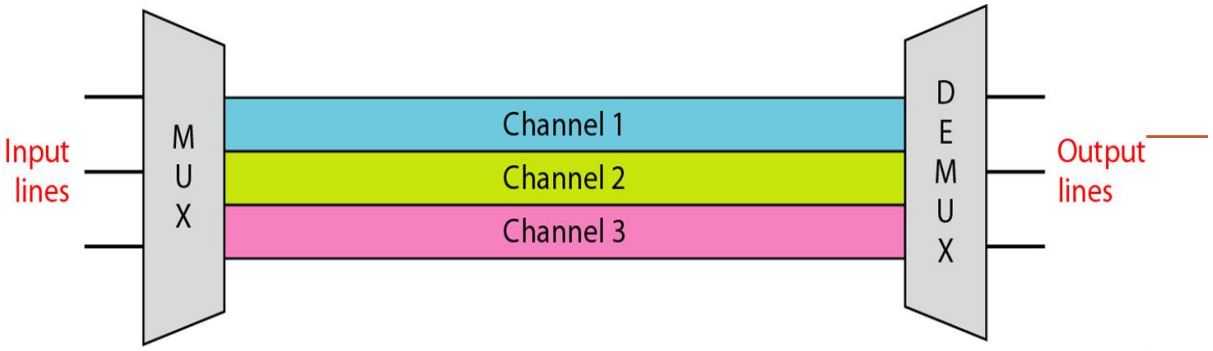
- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the **signals to form a composite signal**.
- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.
- **Advantages of Multiplexing:-**
    - More than one signal can be sent over a single medium.
    - The bandwidth of a medium can be utilized effectively.

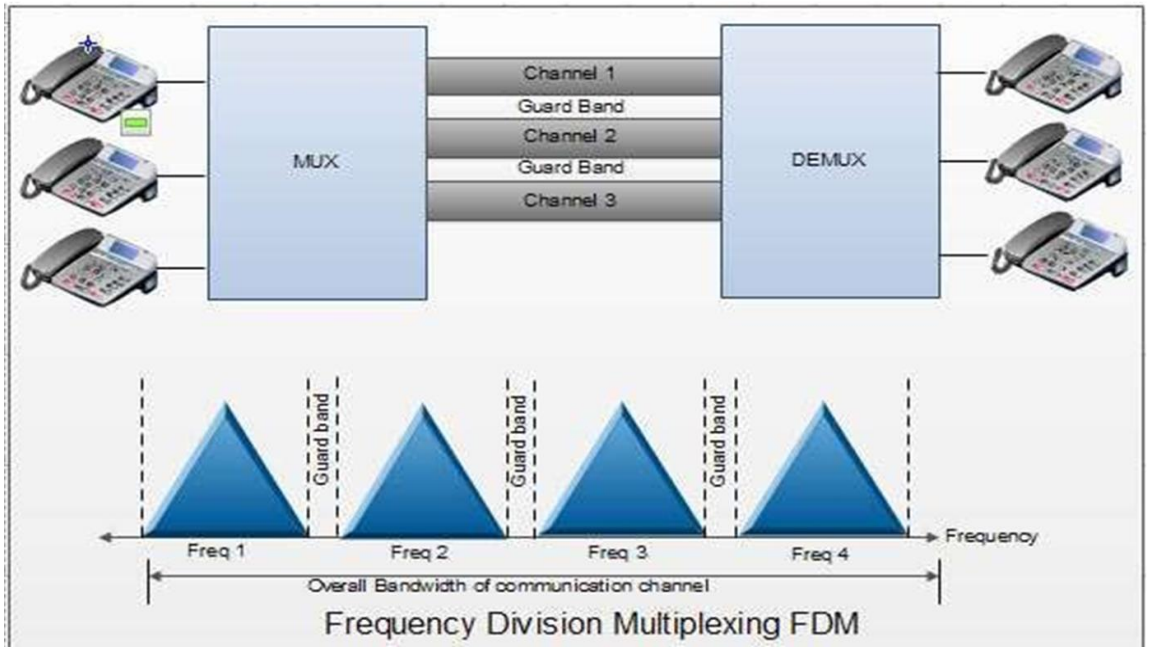
Types of Multiplexing




FDM-FREQUENCY DIVISION MULTIPLEXING

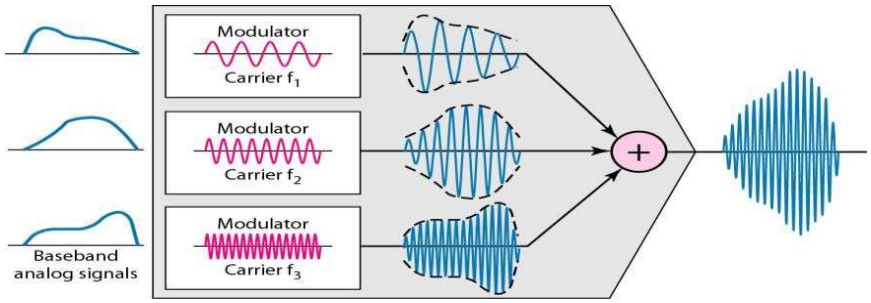
FDM is an analog multiplexing technique that combines analog signals. When the carrier is frequency, FDM is used. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel



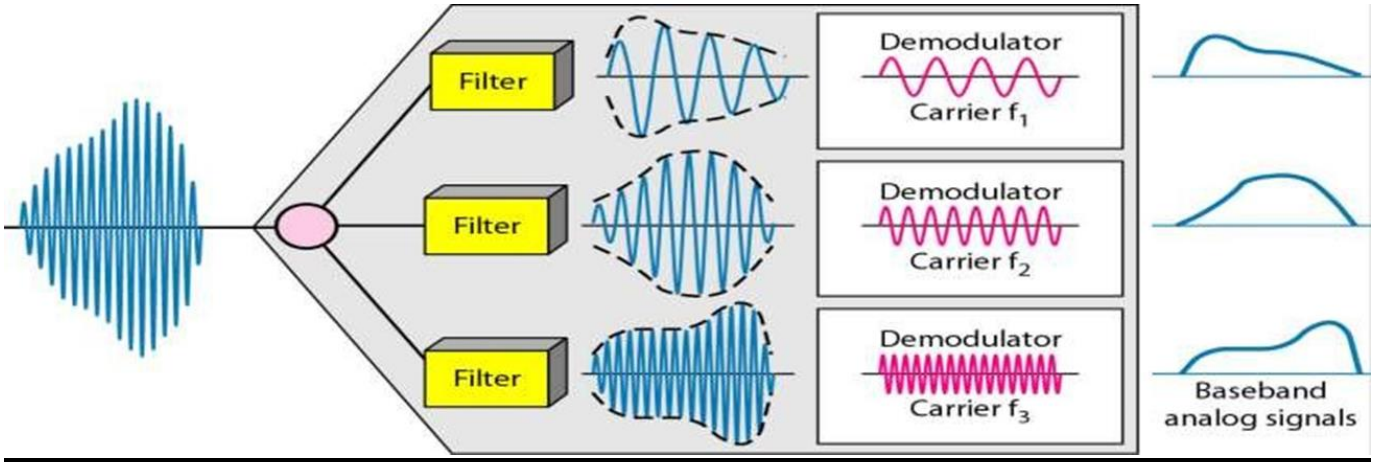




**Multiplexing-FDM**

- A signal of a similar frequency range with the multiplexer, these similar signals modulate different carrier frequencies ( *f1, f2,f3).*
- *The resulting modulated signals* are then combined into a single composite signal that is sent out over a media link that has enough bandwidth to accommodate it.

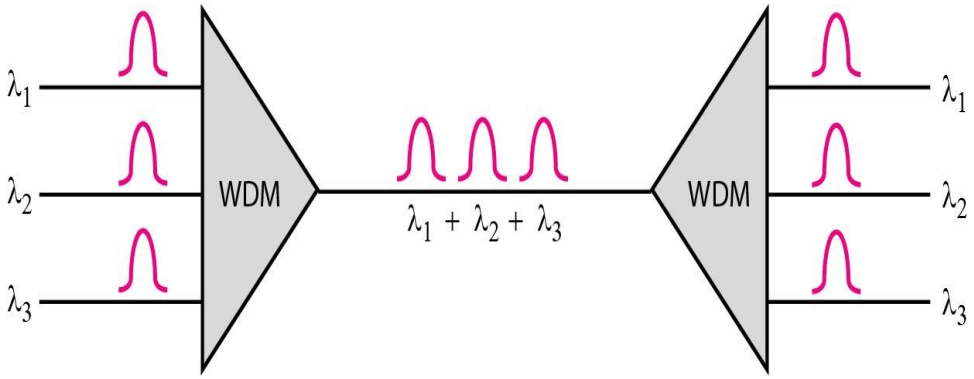



**De multiplexing-FDM**




**WAVELENGTH DIVISION MULTIPLEXING**

WDM is an analog multiplexing technique. Working is same as FDM. In WDM different signals are optical or light signals that are transmitted through optical fiber. Various light waves from different sources are combined to form a composite light signal that is transmitted across the channel to the receiver. At the receiver side, this composite light signal is broken into different light waves by demultiplexer. This Combining and the Splitting of light waves is done by using a PRISM. Prism bends beam of light based on the angle of incidence and the frequency of light wave. Very narrow bands of light from different sources are combined to make a wider band of light. At the receiver, the signals are separated by the demultiplexer.



TIME DIVISION MULTIPLEXING

It is the digital multiplexing technique. A multiplexing technique by which multiple data signals can be transmitted over a common communication channel in different time slots is known as **Time Division Multiplexing (TDM)**.

It allows the division of the overall time domain into various fixed length time slots is known as **time slot or slice.** The users get **complete channel bandwidth** to send signals but for a **fixed time slot.** Here the time domain is divided into several recurrent slots of fixed length, and each signal is allotted a time slot on a **round-robin basis**.

**Types of TDM**

1. Synchronous TDM
2. Asynchronous TDM

**Synchronous TDM –**
The time slots are pre-assigned and fixed. This slot is even given if the source is not ready with data at this time. In this case the slot is transmitted empty. It is used for multiplexing digitized voice stream.

**Asynchronous (or statistical) TDM –**
The slots are allocated dynamically depending on the speed of source or their ready state. It dynamically allocates the time slots according to different input channel's needs, thus saving the channel capacity.

**Spread Spectrum**

In spread spectrum (SS), we combine signals from different sources to fit into a larger bandwidth, but our goals are to prevent eavesdropping and jamming. To achieve these goals, spread spectrum techniques add redundancy.

*Types of Spread Spectrum*

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum Synchronous (DSSS)

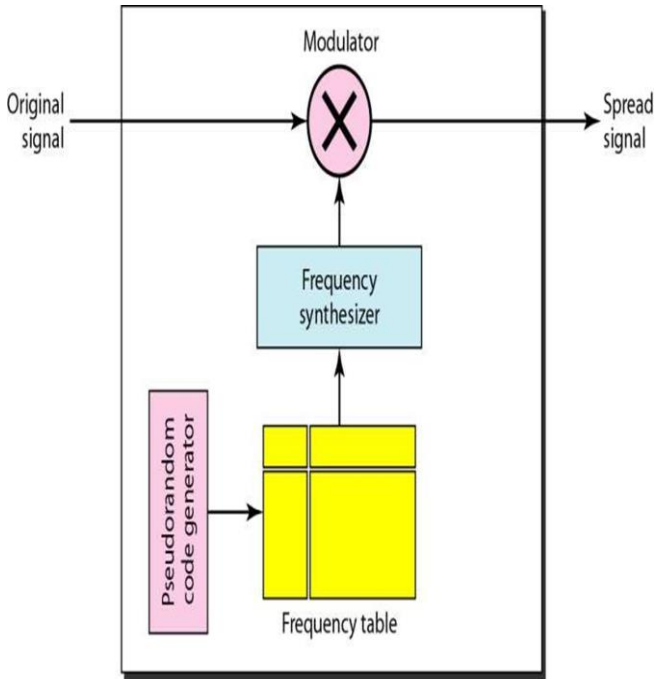
Why Spread Spectrum?

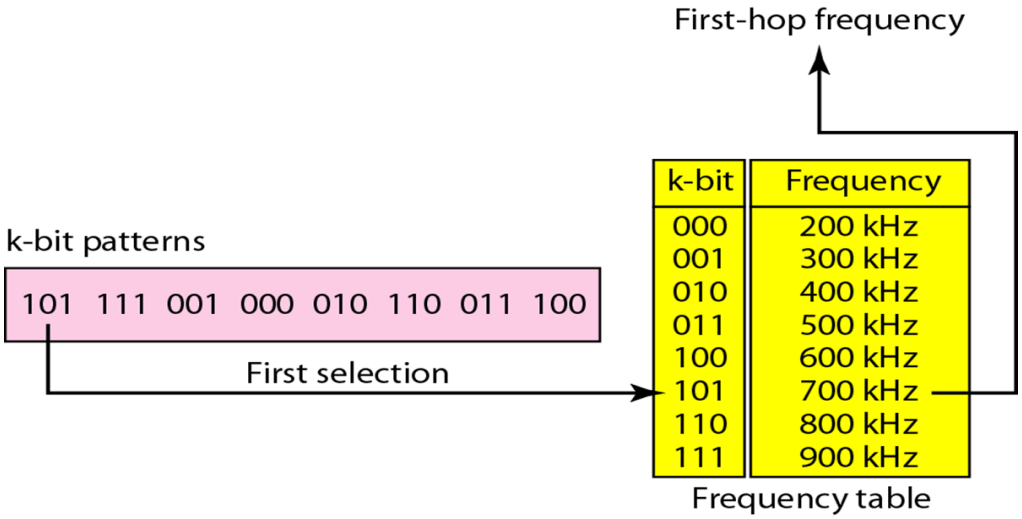
Spread spectrum signals are distributed over a wide range of frequencies and then collected back at the receiver These wideband signals are noise-like and hence difficult to detect or interfere with Initially adopted in military applications, for its resistance to jamming and difficulty of interception.More recently, adopted in commercial wireless communications

**FREQUENCY HOPPING SPREAD SPECTRUM**

- Carrier changes frequency (HOPS) according to a pseudorandom Sequence.
- Pseudorandom sequence is a list of frequencies.
- The carrier hops through this lists of frequencies.
- The carrier then repeats this pattern.
- During ***Dwell Time*** the carrier remains at a certain frequency.
- During ***Hop Time*** the carrier hops to the next frequency.
- This signal is resistant but not immune to narrow band interference

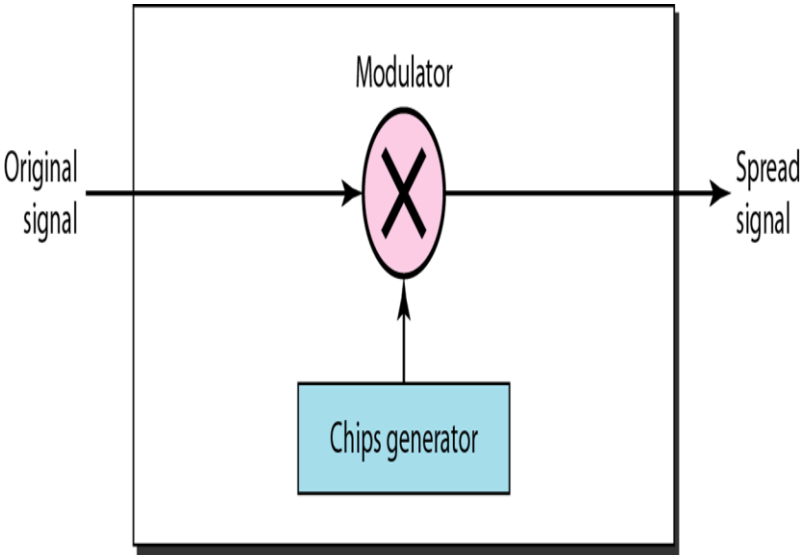
* The amount of time spent on each frequency hop is called as **Dwell time**

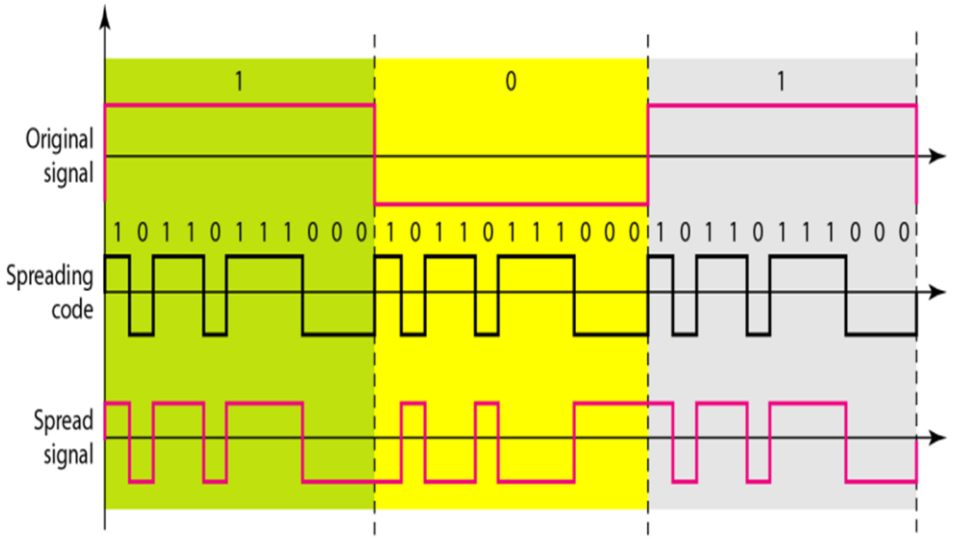





DIRECT SEQUENCE SPREAD SPECTRUM

- Whenever a user wants to send data using this DSSS technique, each and every bit of the user data is multiplied by a secret code, called as **chipping code**.
- This chipping code is nothing but the spreading code which is multiplied with the original message and transmitted.
- The receiver uses the same code to retrieve the original message.




1
0
1
Original signal
1 0 1 1 0 1 1 1 0 0 0
1 0 1 1 0 1 1 1 0 0 0
1 0 1 1 0 1 1 1 0 0 0
Spreading code
Spread signal

## UNIT II DATA LINK LAYER (LLC & MAC)

Logical Link Control : Error Detection and Error Correction - Fundamentals, Block coding, Hamming Distance, CRC; Flow Control and Error control protocols - Stop and Wait, Go back – N ARQ, Selective Repeat ARQ, Sliding Window, Piggybacking, Multiple access protocols : Random Access Protocol, Controlled Access Protocol, Channelization Protocol.

Error Detection and Error Correction

**Error**
A condition when the receiver's information does not match with the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

**Error Detecting Codes (Implemented either at Data link layer or Transport Layer of OSI Model)**
Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message.

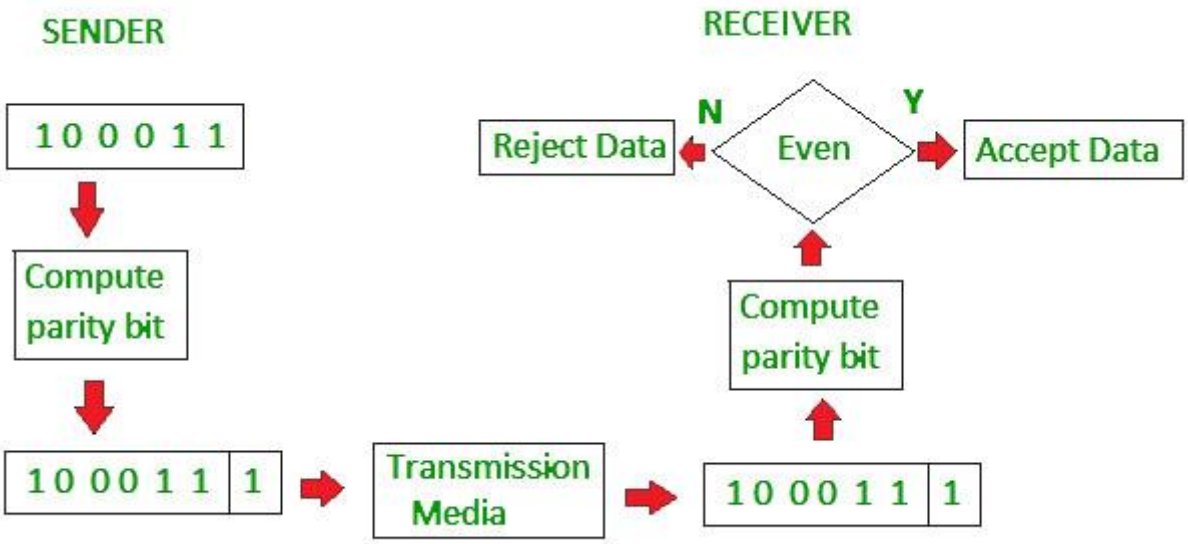
Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors.
Some popular techniques for error detection are:

1. Simple Parity check
2. Two-dimensional Parity check
3. Checksum
4. Cyclic redundancy check

**1. Simple Parity check**
Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

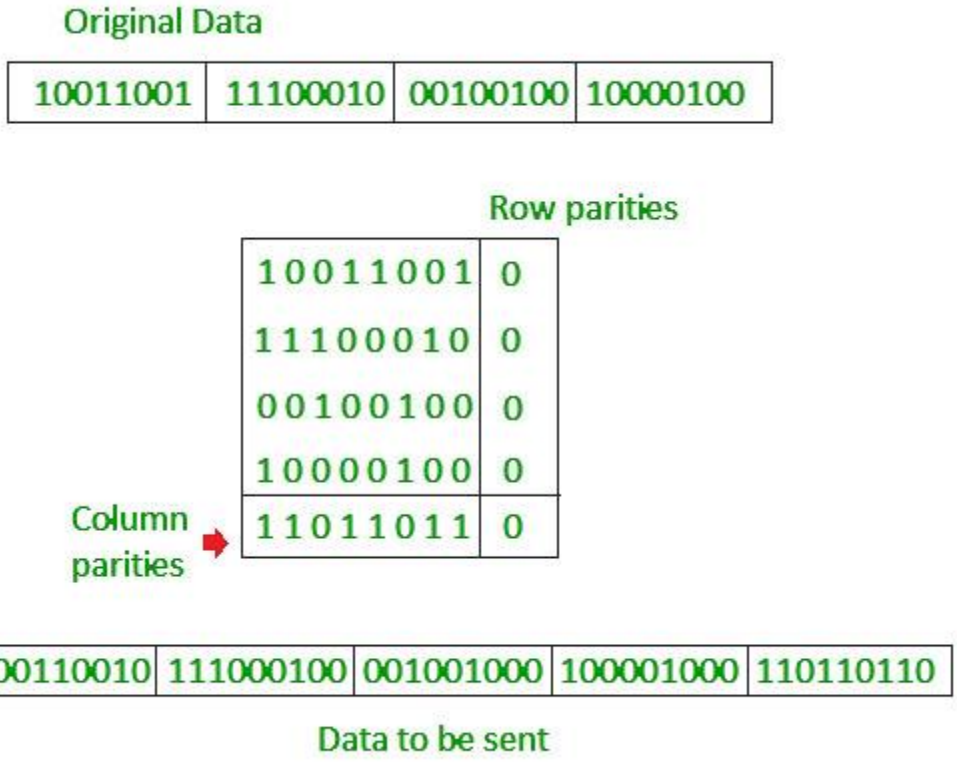
- 1 is added to the block if it contains odd number of 1's, and
- 0 is added if it contains even number of 1's

This scheme makes the total number of 1's even, that is why it is called even parity checking.




**2. Two-dimensional Parity check**

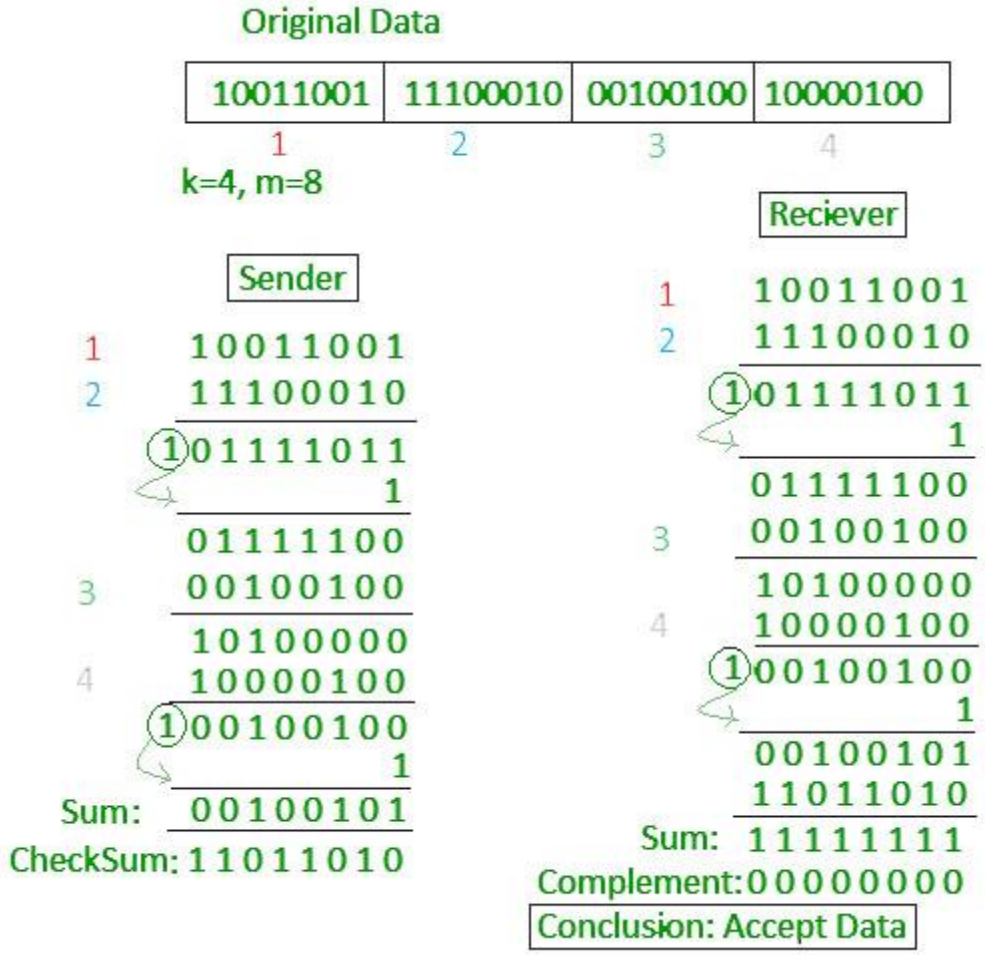
Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.




**3. Checksum**

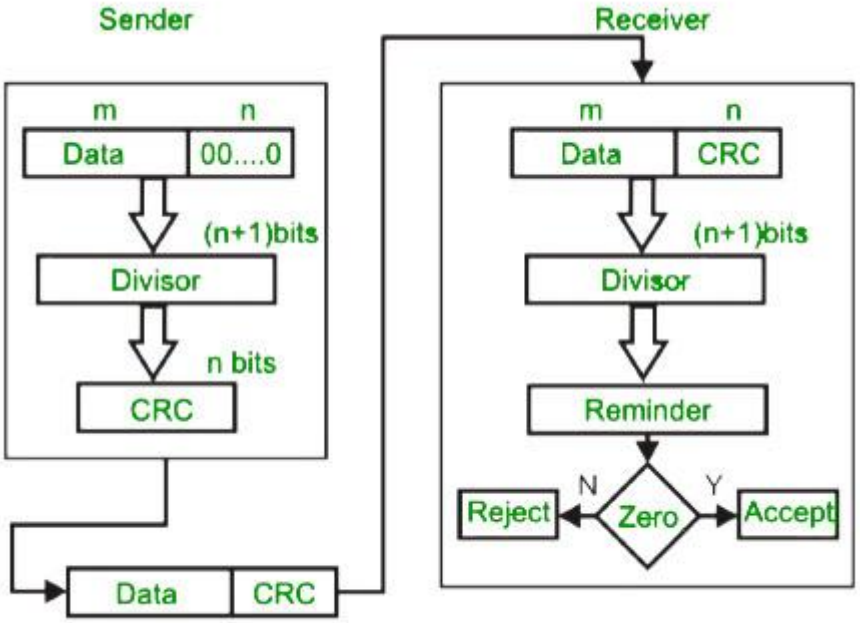
- In checksum error detection scheme, the data is divided into k segments each of m bits.
- In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.

- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.




**4. Cyclic redundancy check (CRC)**

- Unlike checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.




Example

original message
1 0 1 0 0 0 0

@ means X-OR

Generator polynomial
$x^3+1$
$1.x^3+0.x^2+0.x^1+1.x^0$
CRC generator
1 0 0 1 4-bit

If CRC generator is of n bit then append (n-1) zeros in the end of original message

Sender

```
1001 | 1010000000
     @1001
      0011000000
       @1001
        01010000
         @1001
          0011000
           @1001
            01010
             @1001
              0011
```

Message to be transmitted

```
1010000000
    +011
----------
1010000011
```

```
1001 | 1010000011
     @1001
      0011000011
       @1001
        01010011      <- Receiver
         @1001
          0011011
           @1001
            01001
             @1001
              0000
```

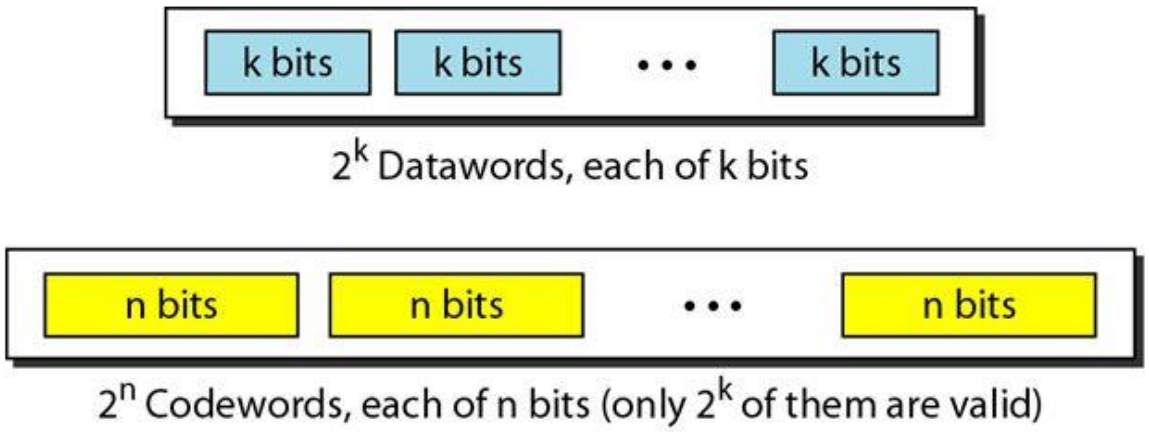
Zero means data is accepted

**BLOCK CODING**

In block coding, we divide our message into blocks, each of k bits, called data words. We add r redundant bits to each block to make the length n = k + r. The resulting n-bit blocks are called code words.

For example, we have a set of data words, each of size k, and a set of code words, each of size of n. With k bits, we can create a combination of 2k data words, with n bits; we can create a combination of 2n code words. Since n > k, the number of possible code words is larger than the number of possible data words.

The block coding process is one-to-one; the same data word is always encoded as the same code word. This means that we have 2n-2k code words that are not used. We call these code words invalid or illegal. The following figure shows the situation




***Error Detection***

If the following two conditions are met, the receiver can detect a change in the original code word by using Block coding technique.

1. The receiver has (or can find) a list of valid code words.

2. The original code word has changed to an invalid one.

The sender creates code words out of data words by using a generator that applies the rules and procedures of encoding (discussed later). Each code word sent to the receiver may change during transmission. If the received code word is the same as one of the valid code words, the word is accepted; the corresponding data word is extracted for use.

If the received code word is not valid, it is discarded. However, if the code word is corrupted during transmission but the received word still matches a valid code word, the error remains undetected. This type of coding can detect only single errors. Two or more errors may remain undetected.

For example consider the following table of data words and Code words:

| *Datawords* | *Codewords* |
|---|---|
| 00 | 000 |
| 01 | 011 |
| 10 | 101 |
| 11 | 110 |

Assume the sender encodes the data word 01 as 011 and sends it to the receiver. Consider the following cases:

1. The receiver receives O11. It is a valid code word. The receiver extracts the data word 01 from it.

2. The code word is corrupted during transmission, and 111 is received (the leftmost bit is corrupted). This is not a valid code word and is discarded.

3. The code word is corrupted during transmission, and 000 is received (the right two bits are corrupted). This is a valid code word. The receiver incorrectly extracts the data word 00. Two corrupted bits have made the error undetectable.

**Error Correction:**

Error correction is much more difficult than error detection. In error detection, the receiver needs to know only that the received code word is invalid, in error correction the receiver needs to find (or guess) the original code word sent. So, we need more redundant bits for error correction than for error detection.

Consider the following table of Data words and Code words.

| *Dataword* | *Codeword* |
|---|---|
| 00 | 00000 |
| 01 | 01011 |
| 10 | 10101 |
| 11 | 11110 |

Assume the data word is 01. The sender consults the table (or uses an algorithm) to create the code word 01011. The code word is corrupted during transmission, and 01001 is received (error in the second bit from the right). First, the receiver finds that the received code word is not in the table. This means an error has occurred. (Detection must come before correction.) The receiver, assuming that there is only 1 bit corrupted, uses the following strategy to guess the correct data word.

1. comparing the received code word with the first code word in the table (01001 versus 00000), the receiver decides that the first code word is not the one that was sent because there are two different bits.

2. By the same reasoning, the original code word cannot be the third or fourth one in the table.

3. The original code word must be the second one in the table because this is the only one that differs from the received code word by 1 bit. The receiver replaces 01001 with 01011 and consults the table to find the data word 01.

**HAMMING CODE**

Hamming code is a set of error-correction codes that can be used to **detect and correct the errors** that can occur when the data is moved or stored from the sender to the receiver. It is **technique developed by R.W. Hamming for error correction**.

**Hamming Distance**

Hamming distance is a metric for comparing two binary data strings. While comparing two binary strings of equal length, Hamming distance is the number of bit positions in which the two bits are different.

The Hamming distance between two strings, a and b is denoted as d(a,b).

It is used for error detection or error correction when data is transmitted over computer networks. It is also using in coding theory for comparing equal length data words.

**Calculation of Hamming Distance**

In order to calculate the Hamming distance between two strings, and , we perform their XOR operation, (a⊕ b), and then count the total number of 1s in the resultant string.

### Example

Suppose there are two strings 1101 1001 and 1001 1101.

11011001 ⊕ 10011101 = 01000100. Since, this contains two 1s, the Hamming distance, d(11011001, 10011101) = 2.

**Minimum Hamming Distance**

In a set of strings of equal lengths, the minimum Hamming distance is the smallest Hamming distance between all possible pairs of strings in that set.

### Example

Suppose there are four strings 010, 011, 101 and 111.

010 ⊕ 011 = 001, d(010, 011) = 1.

010 ⊕ 101 = 111, d(010, 101) = 3.

010 ⊕ 111 = 101, d(010, 111) = 2.

011 ⊕ 101 = 110, d(011, 101) = 2.

011 ⊕ 111 = 100, d(011, 111) = 1.

101 ⊕ 111 = 010, d(011, 111) = 1.

Hence, the Minimum Hamming Distance, $d_{min}$ = 1

## FLOW CONTROL AND ERROR CONTROL

**Flow Control:**
Flow control coordinates that amount of data that can be sent before receiving an acknowledgement. It is one of the most important duties of the data link layer.
Flow control tells the sender how much data to send. It makes the sender wait for some sort of an acknowledgement (ACK) before continuing to send more data.

*Flow Control Techniques: Stop-and-wait, and Sliding Window*

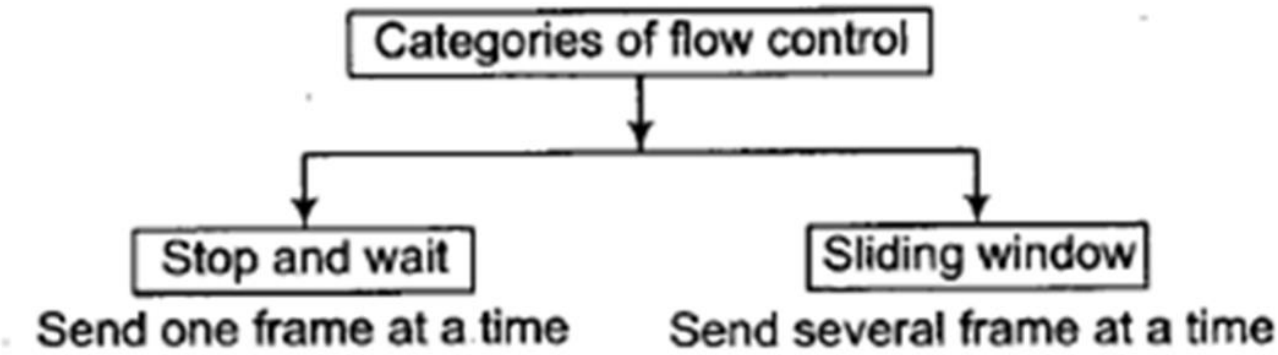
**Error Control:** Error control in the data link layer is based on ARQ (automatic repeat request), which is the retransmission of data. The term error control refers to methods of error detection and retransmission. Every time an error is detected in an exchange, specified frames are retransmitted. This process is called ARQ.
To ensure reliable communication, there needs to exist flow control (managing the amount of data the sender sends), and error control (that data arrives at the destination error free). Flow and error control needs to be done at several layers.
For node-to-node links, flow and error control is carried out in the data-link layer.
For end-point to end-point, flow and error control is carried out in the transport layer.

**Flow & Error control:**

Error Detection and ARQ (error detection with retransmissions) must be combined with methods that intelligently limit the number of 'outstanding' (unACKed) frames.

*Flow & Error control techniques: Stop-and-Wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ*

**Flow Control Techniques:**
One important aspect of the data link layer is flow control.




**STOP AND WAIT**

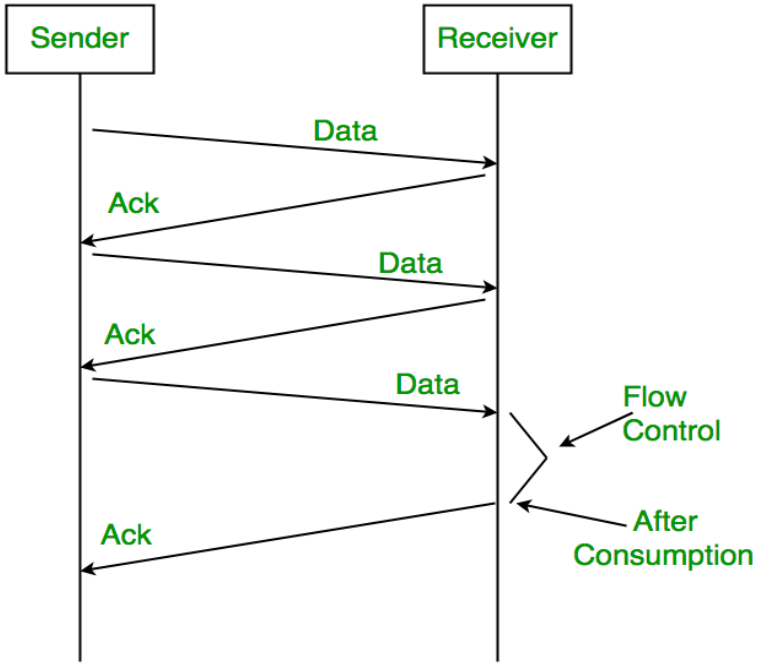
- The sender has to wait for an acknowledgment of every frame that it sends.
- Only when a acknowledgment has been received is the next frame sent.
- This process continues until the sender transmits an End of Transmission (EOT) frame.
- In Stop-and-Wait flow control, the receiver indicates its readiness to receive data for each frame.
- For every frame that is sent, there needs to be an acknowledgment, which takes a similar amount of propagation time to get back to the sender.
- Only one frame can be in transmission at a time.
- This leads to inefficiency if propagation delay is much longer than the transmission delay.

**Advantages of Stop and Wait:**

- It's simple and each frame is checked and acknowledged well.

**Disadvantages of Stop and Wait:**

- Only one frame can be in transmission at a time.
- It is inefficient, if the distance between devices is long. Reason is propagation delay is much longer than the transmission delay.
- The time spent for waiting acknowledgements between each frame can add significant amount to the total transmission time.



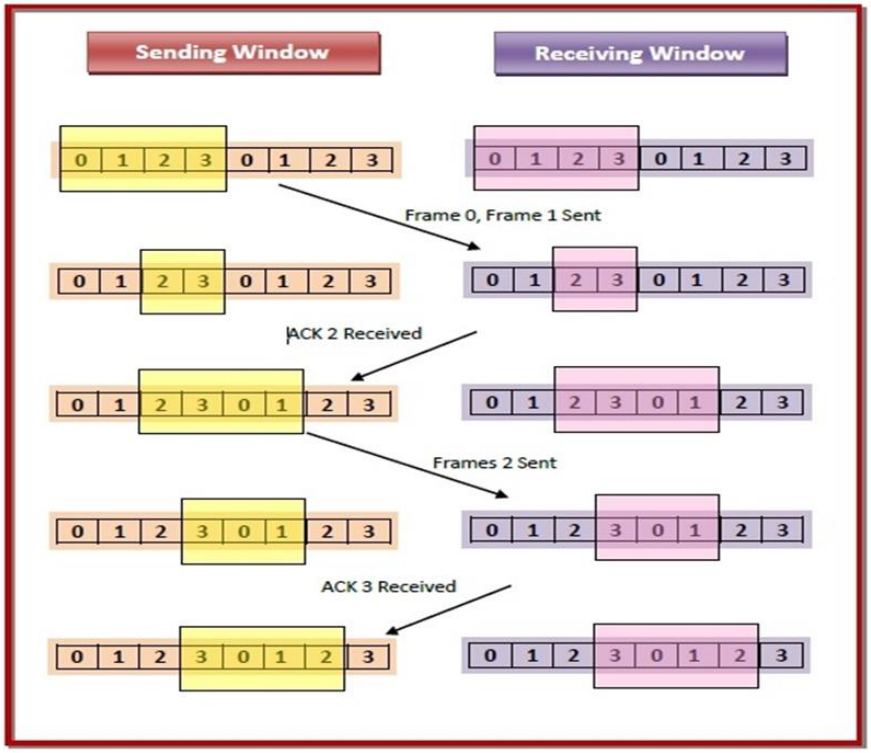

**Sliding Window Flow Control**

- It works by having the sender and receiver have a “window” of frames.
- Each frame has to be numbered in relation to the sliding window. For a window of size n, frames get a number from 0 to n - 1. Subsequent frames get a number mod n.
- The sender can send as many frames as would fit into a window.
- The receiver, upon receiving enough frames, will respond with an acknowledgment of all frames up to a certain point in the window. It is called slide.
- This window can hold frames at either end and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement
- When the receiver sends an ACK, it includes the number of the next frame it expects to receive. When the receiver sends an ACK containing the number 5, it means all frames upto number 4 have been received.

  If the window size is suf□ciently large the sender can continuously transmit packets:

  If W >= (2a+1), sender can transmit continuously. **(Efficiency =1)**

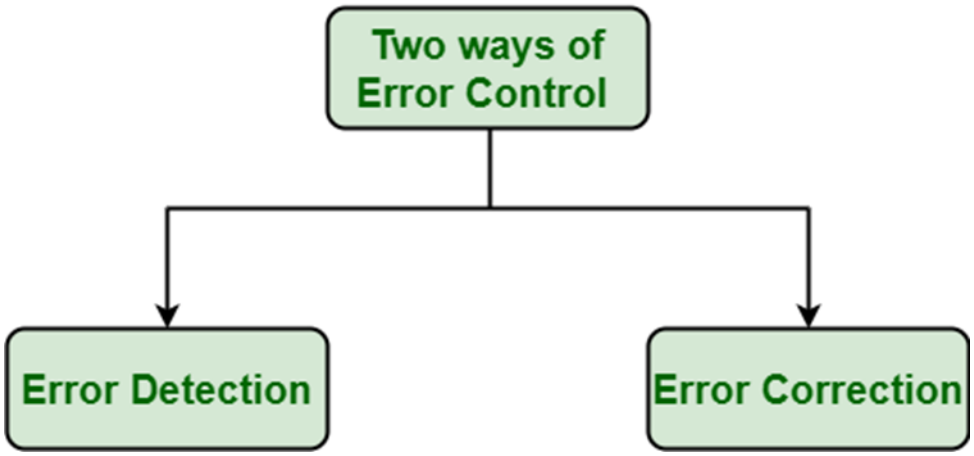
  If W < (2a+1), sender




**ERROR CONTROL IN DATALINK LAYER**

- Data-link layer uses the techniques of error control simply to ensure and confirm that all the data frames or packets, i.e. bit streams of data, are transmitted or transferred from sender to receiver with certain accuracy.

- Error control is basically process in data link layer of detecting or identifying and re-transmitting data frames that might be lost or corrupted during transmission.

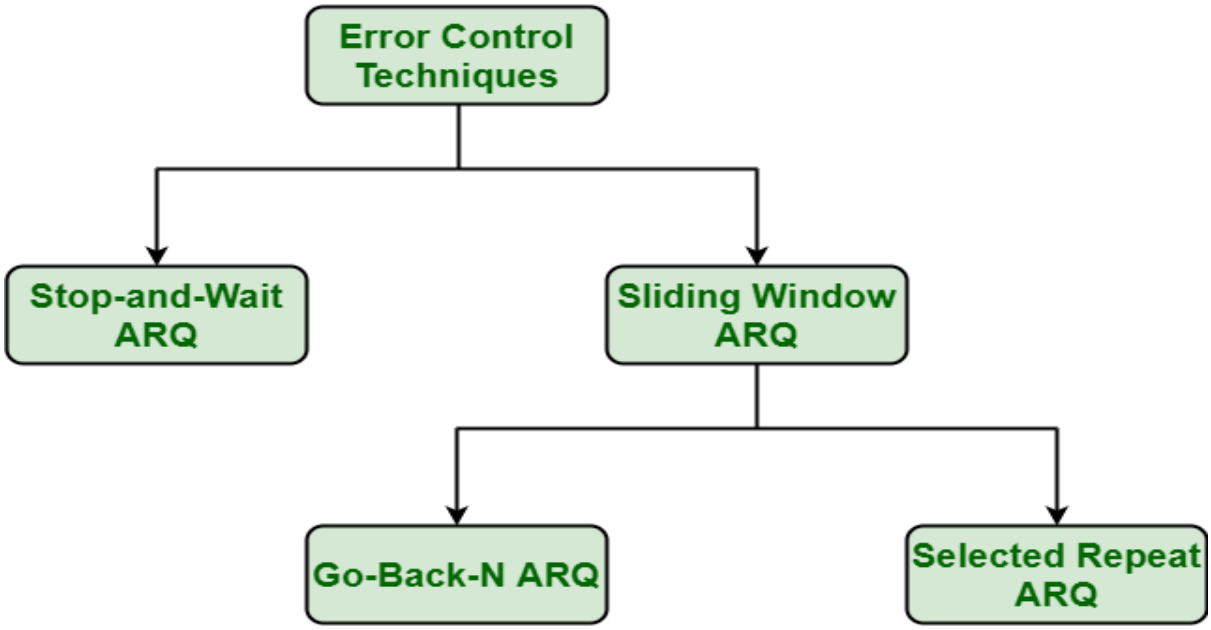


**ERROR DETECTION**

- Error detection, as name suggests, simply means detection or identification of errors. These errors may cause due to noise or any other impairments during transmission from transmitter to the receiver, in communication system. It is class of technique for detecting garbled i.e. unclear and distorted data or message.

**ERROR CORRECTION**

- Error correction, as name suggests, simply means correction or solving or fixing of errors. It simply means reconstruction and rehabilitation of original data that is error-free. But error correction method is very costly and is very hard.




**CHARACTERISTICS**

- Used in Connection-oriented communication.
- It offers error and flow control
- It is used in Data Link and Transport Layers
- Stop and Wait ARQ mainly implements Sliding Window Protocol concept with Window Size 1

**Useful Terms:**

- **Propagation Delay:** Amount of time taken by a packet to make a physical journey from one router to another router.
  Propagation Delay = (Distance between routers) / (Velocity of propagation)
- RoundTripTime (**RTT**) = 2* Propagation Delay
- TimeOut (**TO**) = 2* RTT
- Time To Live (**TTL**) = 2* TimeOut. (Maximum TTL is 180 seconds)

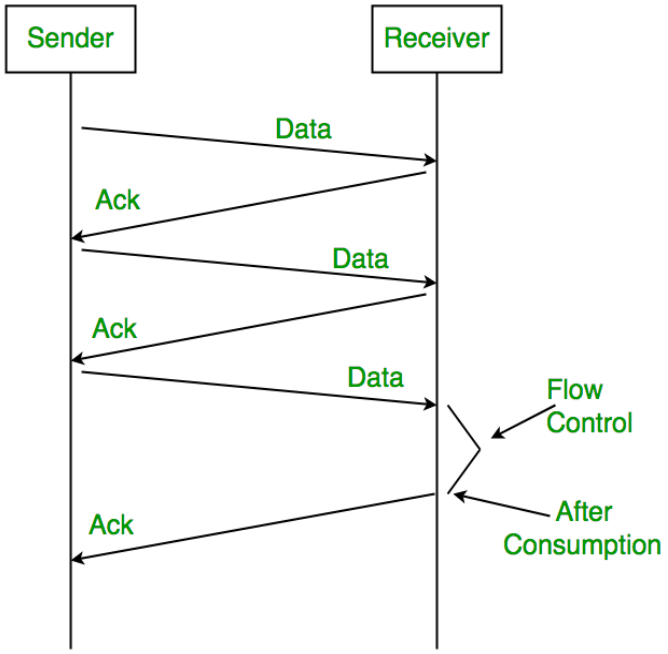
## Simple Stop and Wait

### *Sender:*

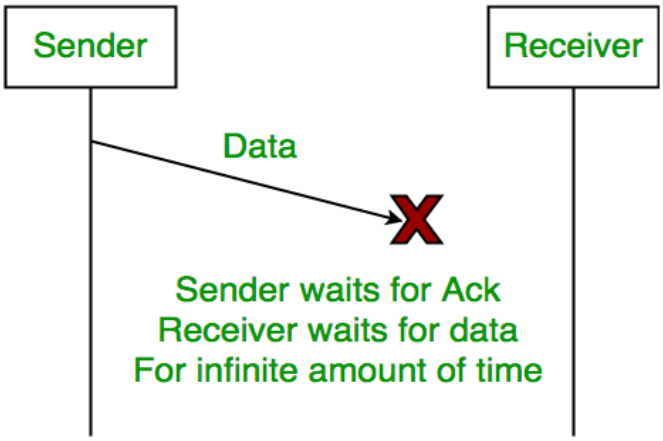
Rule 1) Send one data packet at a time.
Rule 2) Send next packet only after receiving acknowledgement for previous.

### *Receiver:*

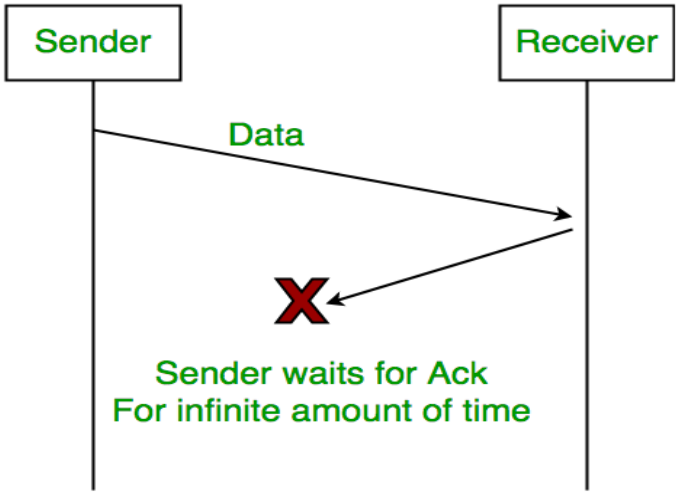
Rule 1) Send acknowledgement after receiving and consuming of data packet.
Rule 2) After consuming packet acknowledgement need to be sent (Flow Control)




**Problems :**
**1. Lost Data**



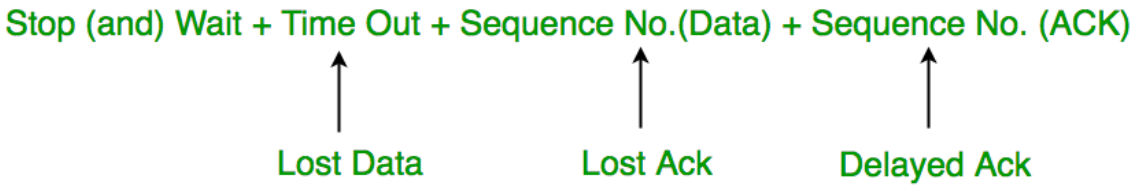
**2.Lost Acknowledgement:**



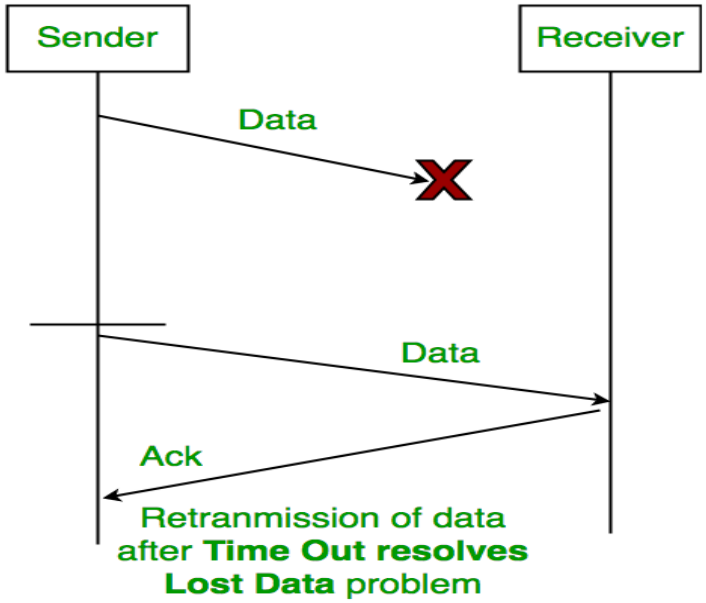

**3. Delayed Acknowledgement/Data:** After timeout on sender side, a long delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

**Stop and Wait ARQ (Automatic Repeat Request)**

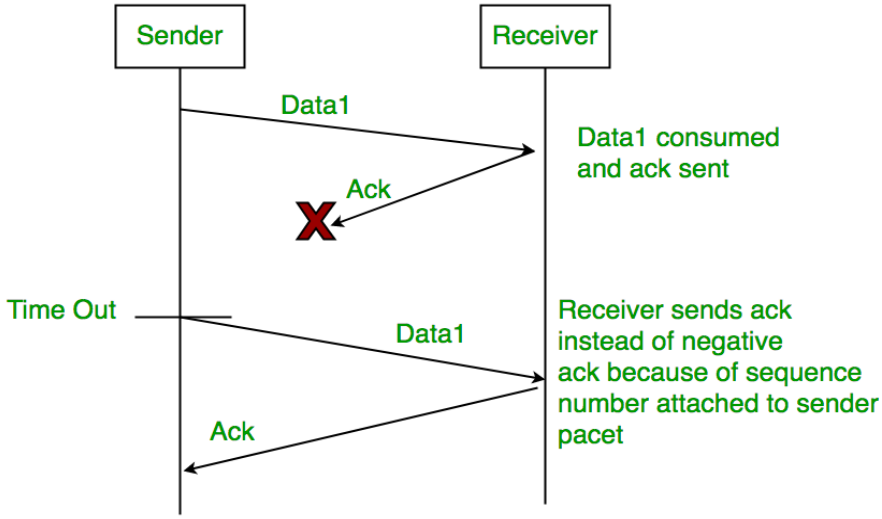
Above 3 problems are resolved by Stop and Wait ARQ (Automatic Repeat Request) that does both error control and flow control.




**1. Time Out:**



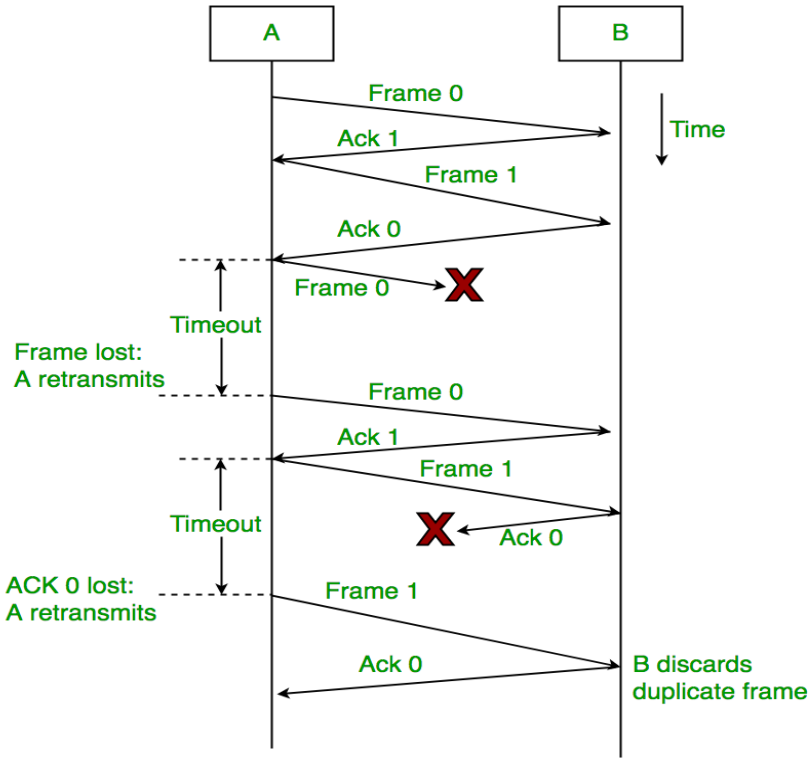
**2. Sequence Number (Data)**




**3. Delayed Acknowledgement:**
This is resolved by introducing sequence number for acknowledgement also.

## Working of Stop and Wait ARQ:

1) Sender A sends a data frame or packet with sequence number 0.
2) Receiver B, after receiving data frame, sends and acknowledgement with sequence number 1 (sequence number of next expected data frame or packet)
There is only one bit sequence number that implies that both sender and receiver have buffer for one frame or packet only.



### *Characteristics of Stop and Wait ARQ:*

- It uses link between sender and receiver as half duplex link
- Throughput = 1 Data packet/frame per RTT
- If Bandwidth*Delay product is very high, then stop and wait protocol is not so useful. The sender has to keep waiting for acknowledgements before sending the processed next packet.
- It is an example for "**Closed Loop OR connection oriented** " protocols
- It is an special category of SWP where its window size is 1
- Irrespective of number of packets sender is having stop and wait protocol requires only 2 sequence numbers 0 and 1

The Stop and Wait ARQ solves main three problems, but may cause big performance issues as sender always waits for acknowledgement even if it has next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you are connected to some server in some other country though a high speed connection). To solve this problem, we can send more than one packet at a time with a larger sequence numbers. We will be discussing these protocols in next articles.

So Stop and Wait ARQ may work fine where propagation delay is very less for example LAN connections, but performs badly for distant connections like satellite connection.

## SLIDING WINDOW PROTOCOL

- The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).
- In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

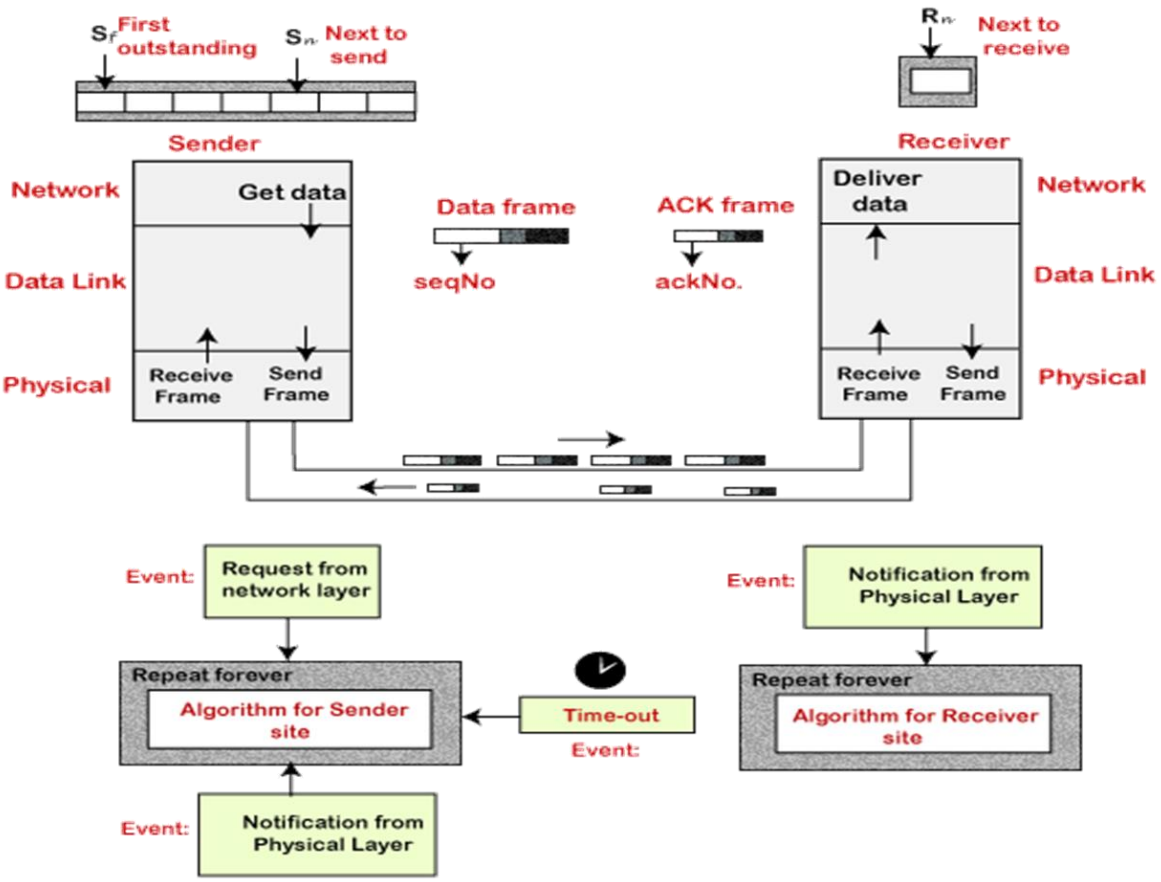
- Sliding window protocol has two types:

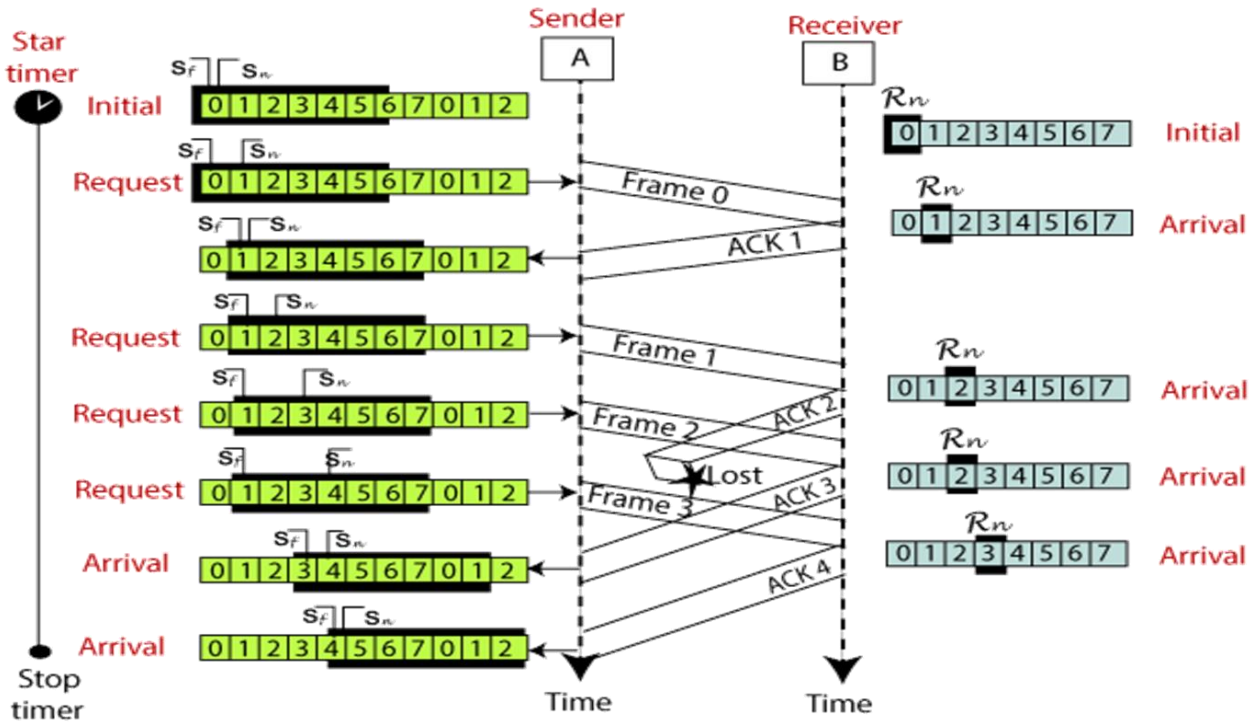
1) Go-Back-N ARQ

2) Selective Repeat ARQ

## GO-BACK-N ARQ

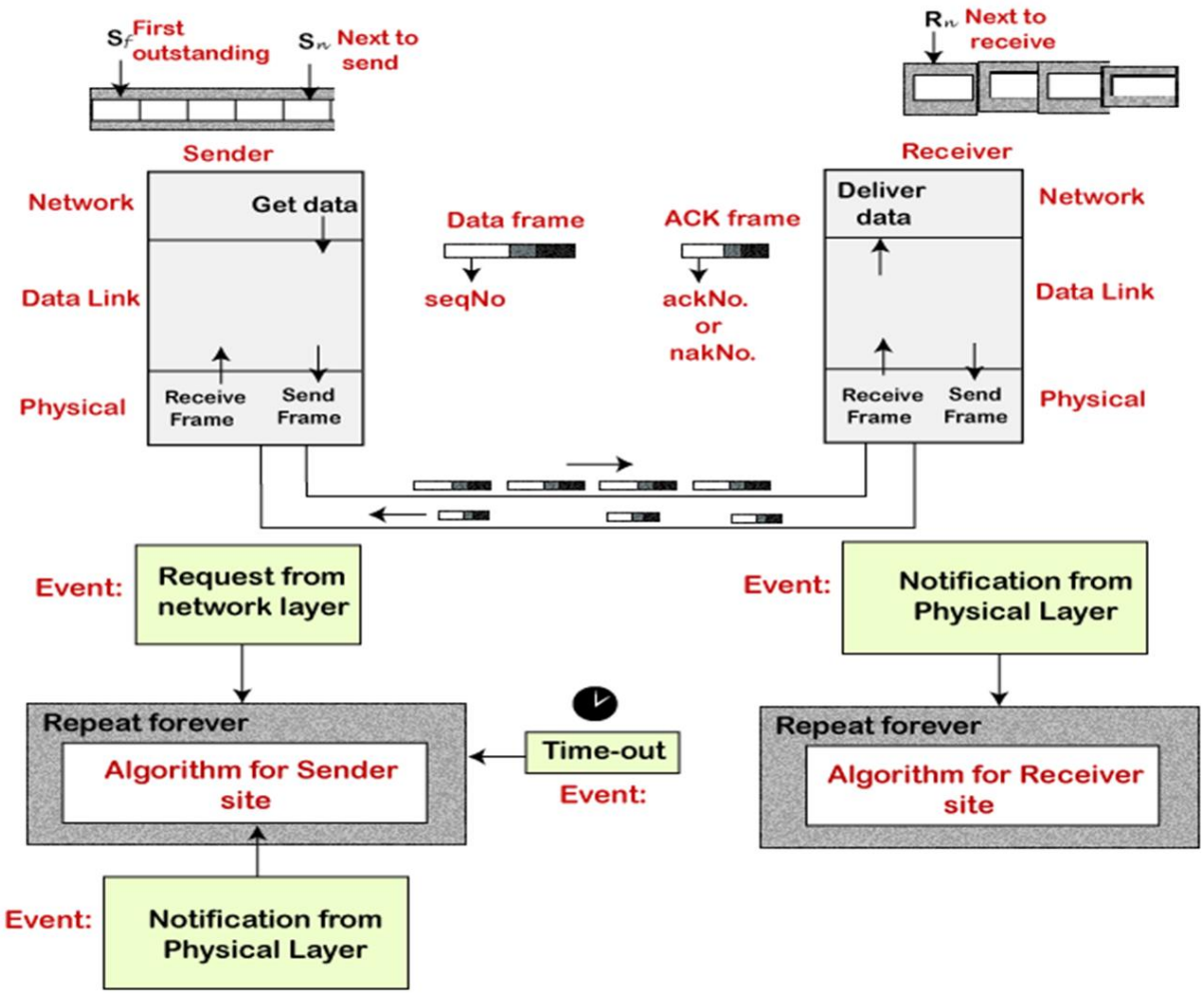
- Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request.
- It is a data link layer protocol that uses a sliding window method.
- In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.
- The size of the sender window is N in this protocol. For example, Go-Back-8, the size of the sender window, will be 8. The receiver window size is always 1.
- If the receiver receives a corrupted frame, it cancels it. The receiver does not accept a corrupted frame. When the timer expires, the sender sends the correct frame again.

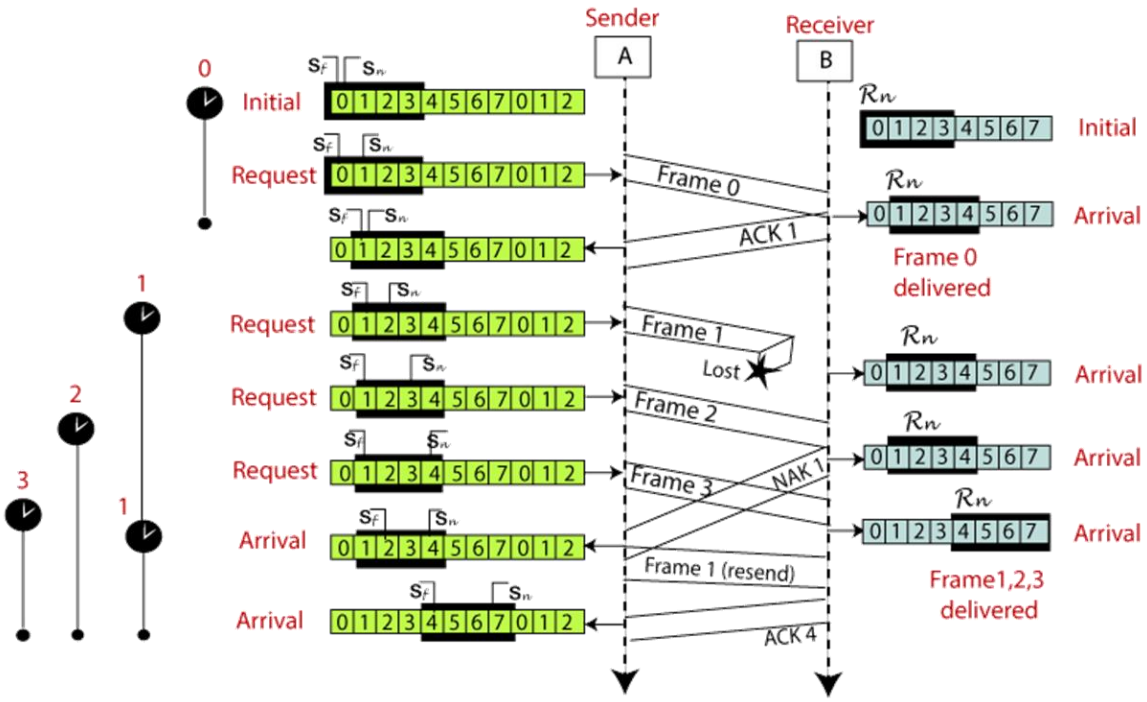

$S_f$ First outstanding
$S_n$ Next to send
$R_n$ Next to receive
Sender
Receiver
Network
Get data
Data Link
Physical
Receive Frame
Send Frame
Data frame
seqNo
ACK frame
ackNo.
Deliver data
Network
Data Link
Physical
Receive Frame
Send Frame
Event:
Request from network layer
Repeat forever
Algorithm for Sender site
Time-out
Event:
Event:
Notification from Physical Layer
Event:
Notification from Physical Layer
Repeat forever
Algorithm for Receiver site


Star timer
Stop timer
Sender
A
Receiver
B
Initial
Request
Arrival
Frame 0
ACK 1
Frame 1
Frame 2
ACK 2
Lost
Frame 3
ACK 3
ACK 4
Time
Time
Initial
Arrival
Arrival
Arrival
Arrival

**Selective Repeat ARQ**

- It is a data link layer protocol that uses a sliding window method. The Go-back-N ARQ protocol works well if it has fewer errors. But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again. So, we use the Selective Repeat ARQ protocol.
- In this protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.
- If the receiver receives a corrupt frame, it does not directly discard it.
- It sends a negative acknowledgment to the sender.
- The sender sends that frame again as soon as on the receiving negative acknowledgment. There is no waiting for any time-out to send that frame.






**Differences**

| Go-Back-N ARQ | Selective Repeat ARQ |
|---|---|
| If a frame is corrupted or lost in it,all subsequent frames have to be sent again. | In this, only the frame is sent again, which is corrupted or lost. |
| If it has a high error rate,it wastes a lot of bandwidth. | There is a loss of low bandwidth. |
| It is less complex. | It is more complex because it has to do sorting and searching as well. And it also requires more storage. |
| It does not require sorting. | In this, sorting is done to get the frames in the correct order. |
| It does not require searching. | The search operation is performed in it. |
| It is used more. | It is used less because it is more complex. |

**Piggy Backing**

- A technique called piggybacking is used to improve the efficiency of the bidirectional protocols. When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.

- The major advantage of piggybacking is better use of available channel bandwidth.

- The major disadvantage of piggybacking Additional complexity and If the data link layer waits too long before transmitting the acknowledgement, then re-transmission of frame would take place.

**MULTILPE ACCESS PROTOCOL**

The Data Link Layer is responsible for transmission of data between two nodes. Its main functions are-

Data Link Control
Multiple Access Control

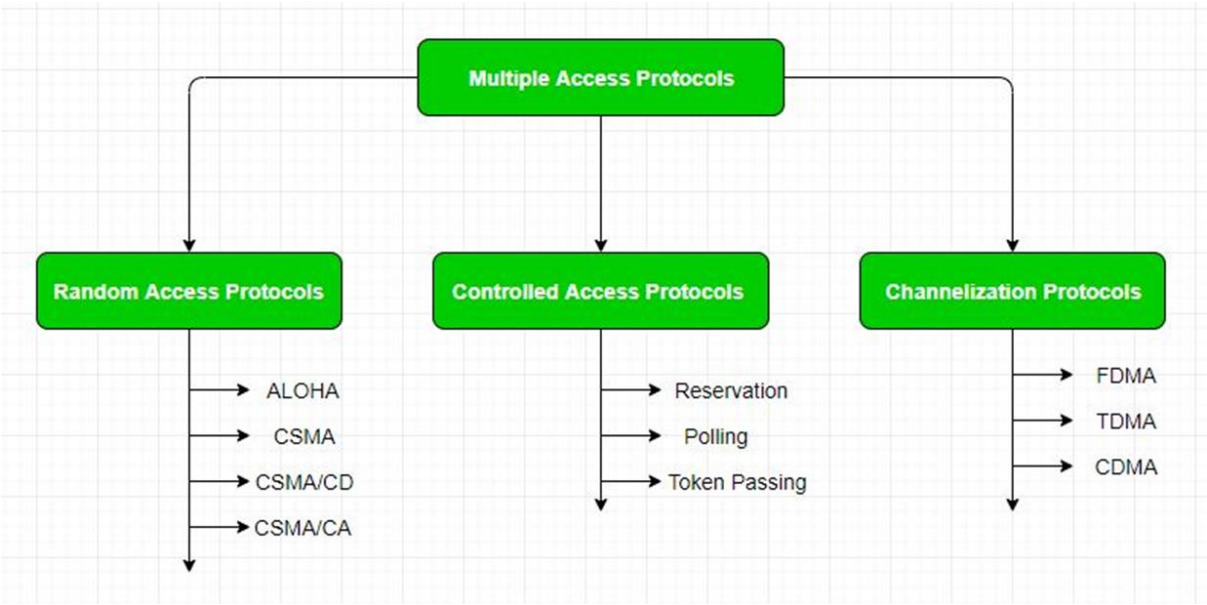
**Data Link control –**

The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control.

- Multiple Access Control: If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk.

- For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created( data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.
- Thus, protocols are required for sharing data on non-dedicated channels.

**Categorize of multiple Access Control**




**RANDOM ACCESS PROTOCOL**

- In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state( idle or busy). It has two features:
- There is no fixed time for sending data
- There is no fixed sequence of stations sending data.

**1(A) ALOHA –** It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

- **Pure Aloha:**
  When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.
- **Slotted Aloha:**
  It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

**2 CSMA –** Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay.

- For example, if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

**3. CSMA/CD –** Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected.

**4. CSMA/CA –** Carrier sense multiple access with collision avoidance. The process of

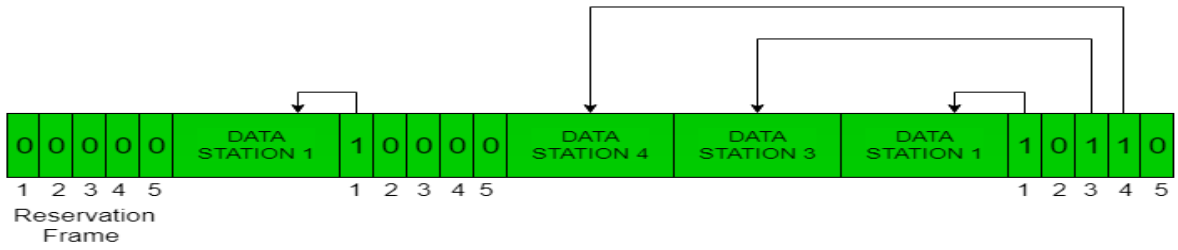
collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.

**Controlled Access Protocols**

- In controlled access, the stations seek information from one another to find which station has the right to send. It allows only one node to send at a time, to avoid collision of messages on shared medium.
  The three controlled-access methods are:
- Reservation
- Polling
- Token Passing

**RESERVATION**

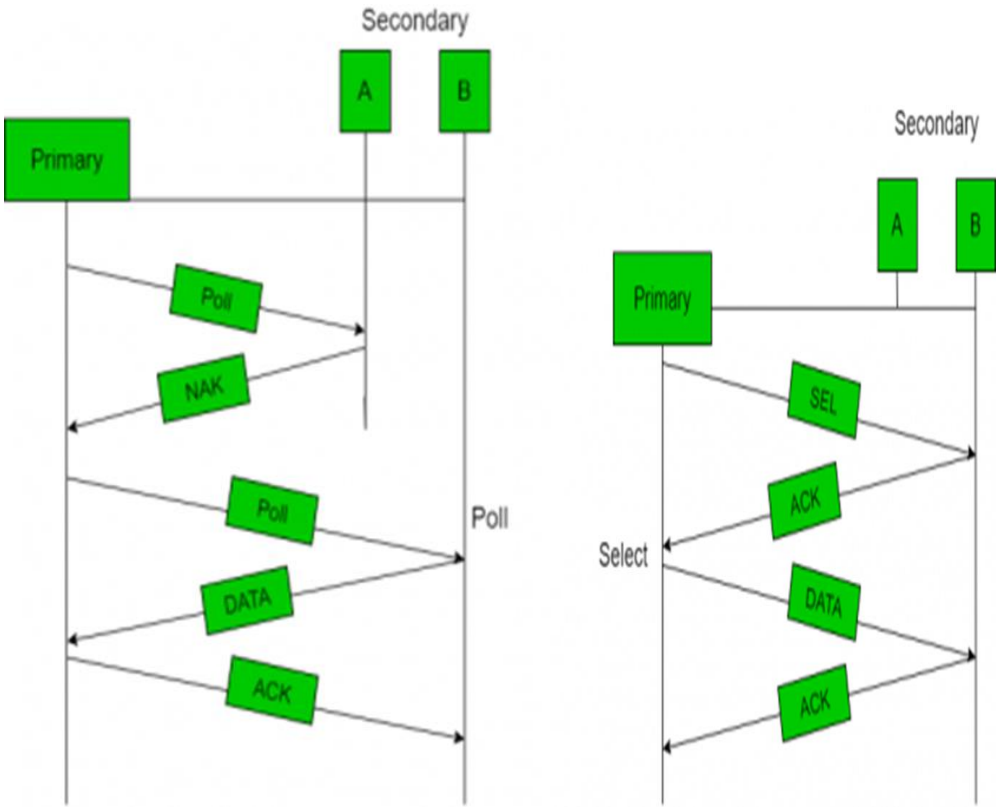
- In the reservation method, a station needs to make a reservation before sending data.
- The time line has two kinds of periods:
  - Reservation interval of fixed time length
  - Data transmission period of variable frames.
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.
- In general, i $^{th}$ station may announce that it has a frame to send by inserting a 1 bit into i $^{th}$ slot. After all N slots have been checked, each station knows which stations wish to transmit.
- The stations which have reserved their slots transfer their frames in that order.
- After data transmission period, next reservation interval begins.
- Since everyone agrees on who goes next, there will never be any collisions.
- The following figure shows a situation with five stations and a five slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.
-




**POLLING**

- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.

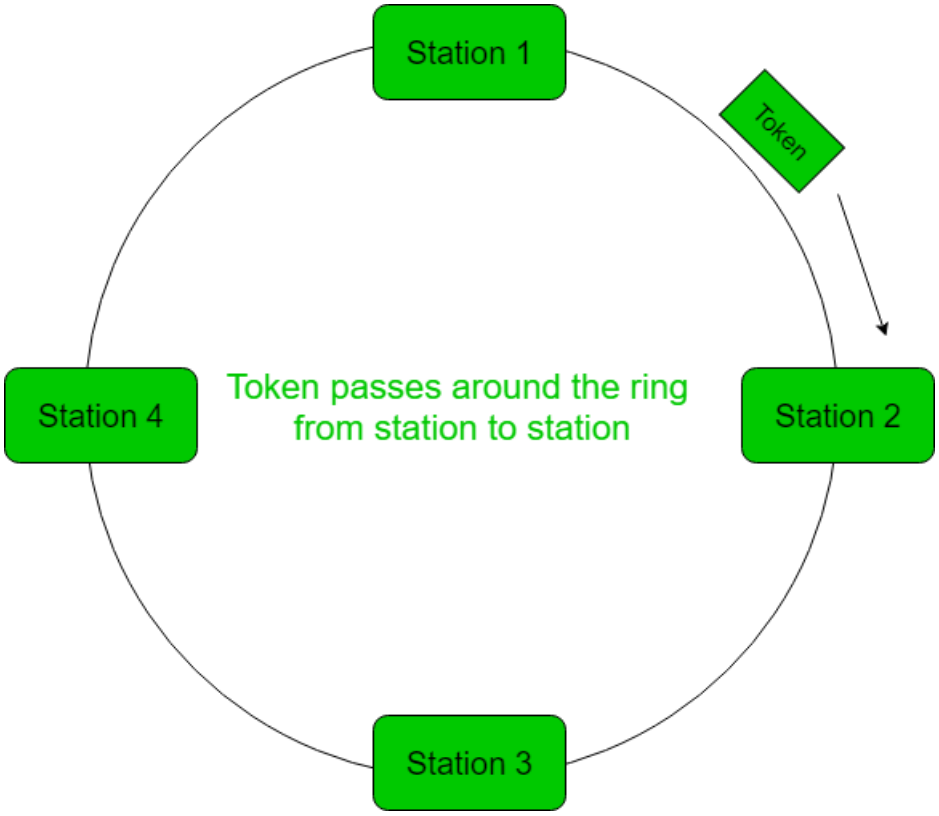
- The message sent by the controller contains the address of the node being selected for granting access.
- Although all nodes receive the message but the addressed one responds to it and sends data, if any. If there is no data, usually a “poll reject”(NAK) message is sent back.
- Problems include high overhead of the polling messages and high dependence on the reliability of the controller.




**TOKEN PASSING**

- In token passing scheme, the stations are connected logically to each other in form of ring and access of stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in the some predefined order.
- In Token ring, token is passed from one station to another adjacent station in the ring whereas in case of Token bus, each station
  uses the bus to send the token to the next station in some predefined order.
- In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply.
- After sending a frame, each station must wait for all N stations (including itself) to send the token to their neighbours and the other N – 1 stations to send a frame, if they have one.
- There exist problems like duplication of token or token is lost or insertion of new station, removal of a station, which need be tackled for correct and reliable operation

of this scheme.




**CHANNELIZATION**

In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

- **Frequency Division Multiple Access (FDMA) –** The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no to bands overlap to avoid crosstalk and noise.
- **Time Division Multiple Access (TDMA) –** In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.

  **Code Division Multiple Access (CDMA) –** One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly data from different stations can be transmitted simultaneously in different code languages.

# UNIT III NETWORK LAYER

Logical addressing – IPV4, IPV6; Address mapping – ARP, RARP, ICMP, BOOTP and DHCP; Routing algorithm-Link state algorithm, Distance vector routing algorithm, Hierarchical routing algorithm; Routing in the Internet-RIP, OSPF,BGP; Broadcast & Multicast routing- DVMRP, PIM.

**Internet Protocol**

It is a set of technical rules that defines how computers communicate over a network.

**IPV4**

- It is the first version of Internet Protocol to be widely used and accounts for most of today's Internet traffic.
- Address Size: 32 bits
- Address Format: Dotted Decimal Notation: 192.149.252.76
- Number of Addresses: 232 = 4,294,967,296 Approximately
- IPv4 header has 20 bytes
- IPv4 header has many fields (13 fields)
- It is subdivided into classes <A-E>.
- The address uses a subnet mask.
- IPv4 has a lack of security.

**IP ADDRESS-IPV4**


IPv4 ip address (32 bits)

**PARTS OF IPV4**

- **Network part:**
  The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.

- **Host Part:**
  The host part uniquely identifies the machine on your network. This a part of the IPv4 address is assigned to every host. For each host on the network, the network part is the same, however, the host half must vary.
- **Subnet number:**
  This is the non-obligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.


**IPV4- FEATURES**

- Source and destination addresses are 32 bits (4 bytes) in length.
- Identification of packet flow for QoS handling by routers is absent within the IPv4header.
- Fragmentation is performed by both routers and the sending host.
- The header includes a checksum.
- Address Resolution Protocol (ARP) uses broadcast ARP request frames to resolve an IPv4 address to a link-layer address.
- ICMP router discovery is used to determine the IPv4 address of the best default gateway and is optional.
- Broadcast addresses are used to send traffic to all nodes on a subnet.
- Must be configured either manually or through DHCP.
- Uses host address resource records in the Domain Name System to map host names to IPv4 addresses.
- Uses pointer resource records in the INADDR, ARPA DNS domain to map IPv4addresses to host names.
- Must support a 576 byte packet size (possibly fragmented).

**IPV4 HEADER**

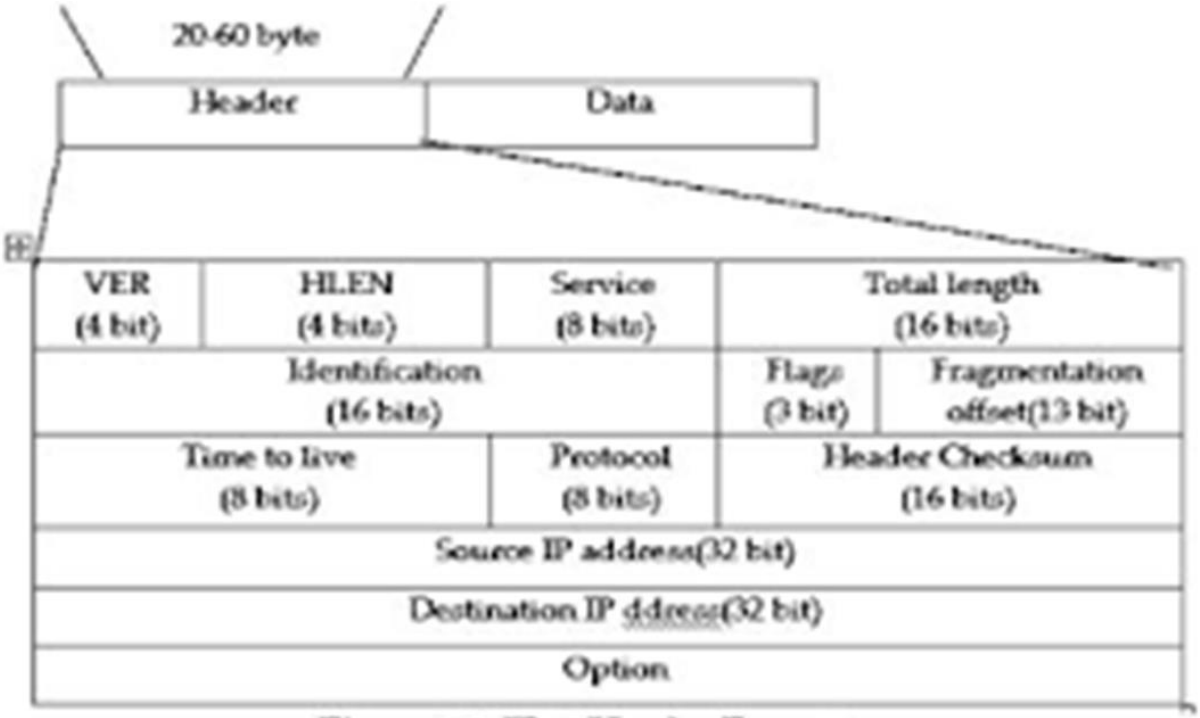


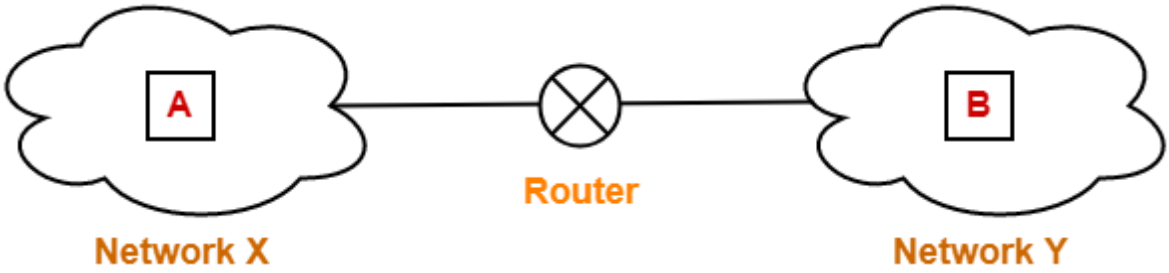

Figure 4.6. IPv4 Header Format

- *Version* is for the IPv4 version (0100).
- *IHL* represents the total length of the header length in 32-bit words. Since IHL is 4 bits, the max header size is 15 32-bit words.
- The *DS (Differentiated services) Field* is used to specify preferential handling for certain packets, e.g. those involved in VoIP.
- *Total Length* is the length of the datagram in octets.
- Identification − If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
- Flags − As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- Fragment Offset − This offset tells the exact position of the fragment in the original IP Packet.
- *Time to Live* is used to stop routing loops. It's decremented by 1 at each router. If it reaches 0, the packet is dropped.
- *Protocol* indicates the protocol used in the packet's data. Common values are 6 (TCP), and 17 (UDP).

- *Header Checksum* is used to verify that the header wasn't corrupted during transmission.
- The *Source Address* and *Destination Address* fields contain the IPv4 addresses of the sender and the recipient.

**IP FRAGMENTATION**

- IP Fragmentation is a process of dividing the datagram into fragments during its transmission.
- It is done by intermediary devices such as routers at the destination host at network layer.




**Need-**

- Each network has its maximum transmission unit (MTU).
- It dictates the maximum size of the packet that can be transmitted through it.
- Data packets of size greater than MTU can not be transmitted through the network.
- So, datagrams are divided into fragments of size less than or equal to MTU.

**Datagram Fragmentation-**

When router receives a datagram to transmit further, it examines the following-

- Size of the datagram
- MTU of the destination network
- DF bit value in the IP header

Then, following cases are possible-

**Case-01:**

- Size of the datagram is found to be smaller than or equal to MTU.
- In this case, router transmits the datagram without any fragmentation.

**Case-02:**

- Size of the datagram is found to be greater than MTU and DF bit set to 1.
- In this case, router discards the datagram.

**Case-03:**

- Size of the datagram is found to be greater than MTU and DF bit set to 0.
- In this case, router divides the datagram into fragments of size less than or equal to MTU.
- Router attaches an IP header with each fragment making the following changes in it.
- Then, router transmits all the fragments of the datagram.

**Changes Made By Router-**

Router makes the following changes in IP header of each fragment-

- It changes the value of total length field to the size of fragment.
- It sets the MF bit to 1 for all the fragments except the last one.
- For the last fragment, it sets the MF bit to 0.
- It sets the fragment offset field value.
- It recalculates the header checksum.

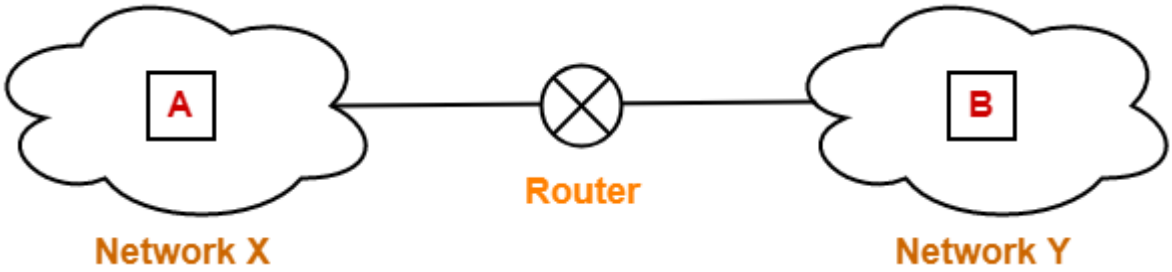
**IP Fragmentation Examples-**

Now, lets us discuss some examples of IP fragmentation to understand how the fragmentation is actually carried out.

**Example-01:**

Consider-

- There is a host A present in network X having MTU = 520 bytes.
- There is a host B present in network Y having MTU = 200 bytes.
- Host A wants to send a message to host B.



Consider router receives a datagram from host A having-

- Header length = 20 bytes
- Payload length = 500 bytes
- Total length = 520 bytes
- DF bit set to 0

Now, router works in the following steps-

**Step-01:**

Router examines the datagram and finds-

- Size of the datagram = 520 bytes
- Destination is network Y having MTU = 200 bytes
- DF bit is set to 0

Router concludes-

- Size of the datagram is greater than MTU.
- So, it will have to divide the datagram into fragments.
- DF bit is set to 0.
- So, it is allowed to create fragments of the datagram.

**Step-02:**

Router decides the amount of data that it should transmit in each fragment.

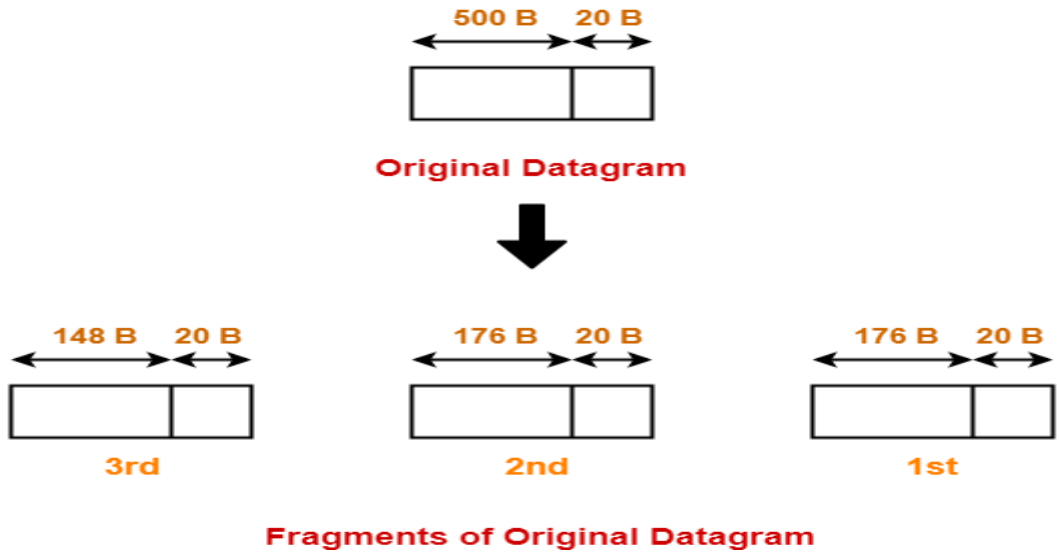
Router knows-

- MTU of the destination network = 200 bytes.
- So, maximum total length of any fragment can be only 200 bytes.
- Out of 200 bytes, 20 bytes will be taken by the header.
- So, maximum amount of data that can be sent in any fragment = 180 bytes.

**Step-03:**

Router creates three fragments of the original datagram where-

- First fragment contains the data = 176 bytes
- Second fragment contains the data = 176 byes
- Third fragment contains the data = 148 bytes




The information contained in the IP header of each fragment is-

**Header Information Of 1st Fragment-**

- Header length field value = 20 / 4 = 5
- Total length field value = 176 + 20 = 196
- MF bit = 1
- Fragment offset field value = 0
- Header checksum is recalculated.
- Identification number is same as that of original datagram.

**Header Information Of 2nd Fragment-**

- Header length field value = 20 / 4 = 5
- Total length field value = 176 + 20 = 196
- MF bit = 1
- Fragment offset field value = 176 / 8 = 22
- Header checksum is recalculated.
- Identification number is same as that of original datagram.

**Header Information Of 3rd Fragment-**

- Header length field value = 20 / 4 = 5

- Total length field value = 148 + 20 = 168
- MF bit = 0
- Fragment offset field value = (176 + 176) / 8 = 44
- Header checksum is recalculated.
- Identification number is same as that of original datagram.

Router transmits all the fragments.

**Step-04:**

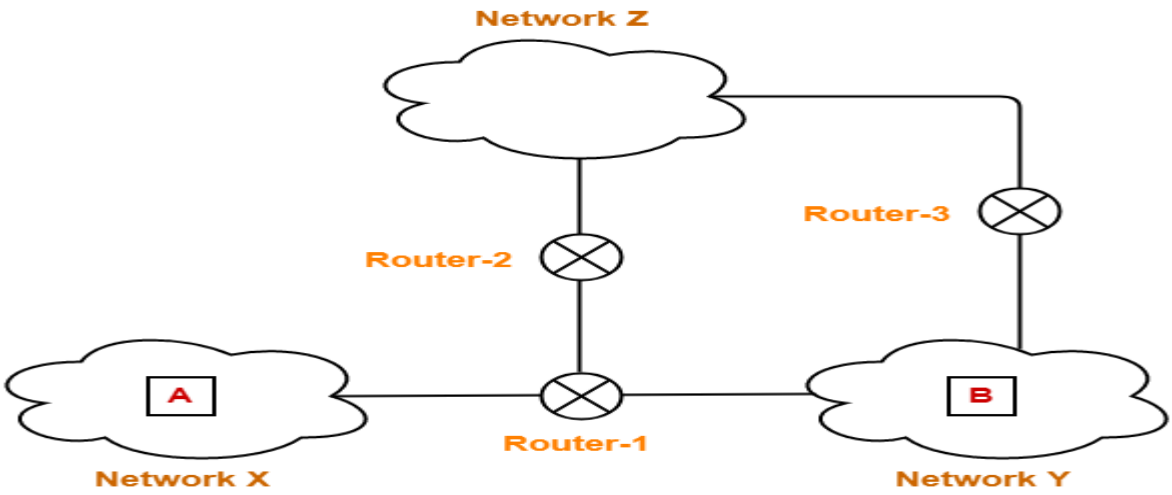
At destination side,

- Receiver receives 3 fragments of the datagram.
- Reassembly algorithm is applied to combine all the fragments to obtain the original datagram.

**Example-02:**

Consider-

- There is a host A present in network X having MTU = 520 bytes.
- There is a host B present in network Y having MTU = 200 bytes.
- There exists a network Z having MTU = 110 bytes.
- Host A wants to send a message to host B.




Consider Router-1 receives a datagram from host A having-

- Header length = 20 bytes
- Payload length = 500 bytes
- Total length = 520 bytes
- DF bit set to 0

Consider Router-1 divides the datagram into 3 fragments as discussed in Example-01.

Then,

- First fragment contains the data = 176 bytes
- Second fragment contains the data = 176 byes
- Third fragment contains the data = 148 bytes

Now, consider-

- First and third fragment reaches the destination directly.
- However, second fragment takes its way through network Z and reach the destination through Router-3.

**Journey Of Second Fragment-**

Now, let us discuss the journey of fragment-2 and how it finally reaches the destination.

Router-2 receives a datagram (second fragment of original datagram) where-

- Header length = 20 bytes
- Payload length = 176 bytes
- Total length = 196 bytes
- DF bit set to 0

Now, Router-2 works in the following steps-

**Step-01:**

Router-2 examines the datagram and finds-

- Size of the datagram = 196 bytes
- Destination is network Z having MTU = 110 bytes
- DF bit is set to 0

Router-2 concludes-

- Size of the datagram is greater than MTU.
- So, it will have to divide the datagram into fragments.
- DF bit is set to 0.
- So, it is allowed to create fragments of the datagram.

**Step-02:**

Router-2 decides the amount of data that it should transmit in each fragment.

Router-2 knows-

- MTU of the destination network = 110 bytes.
- So, maximum total length of any fragment can be only 110 bytes.
- Out of 110 bytes, 20 bytes will be taken by the header.
- So, maximum amount of data that can be sent in any fragment = 90 bytes.

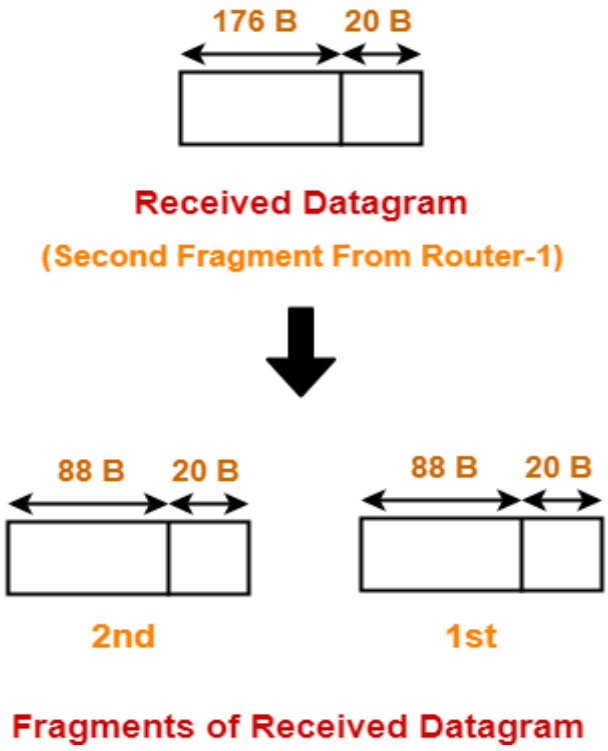
Following the rule,

- Router-2 decides to send maximum 88 bytes of data in one fragment.
- This is because it is the greatest value that is a multiple of 8 and less than MTU.

**Step-03:**

Router-2 creates two fragments of the received datagram where-

- First fragment contains the data = 88 bytes
- Second fragment contains the data = 88 byes




The information contained in the IP header of each fragment is-

**Header Information Of 1st Fragment-**

- Header length field value = 20 / 4 = 5
- Total length field value = 88 + 20 = 108
- MF bit = 1

- Fragment offset field value = 176 / 8 = 22
- Header checksum is recalculated.
- Identification number is same as that of original datagram.

**Header Information Of 2nd Fragment-**

- Header length field value = 20 / 4 = 5
- Total length field value = 88 + 20 = 108
- MF bit = 1
- Fragment offset field value = (176 + 88) / 8 = 33
- Header checksum is recalculated.
- Identification number is same as that of original datagram.

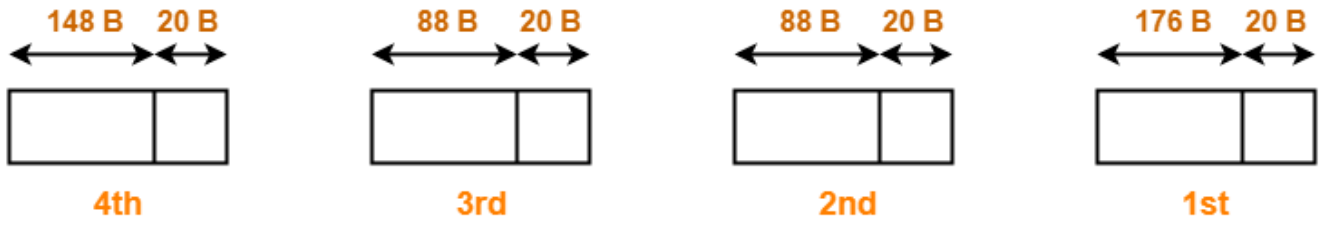
Router-2 transmits both the fragments which reaches the destination through Router-3.

Router-3 performs no fragmentation.

**Step-04:**

At destination side,

- Receiver receives 4 fragments of the datagram.
- Reassembly algorithm is applied to combine all the fragments to obtain the original datagram.




Fragments Received By Receiver

**Reassembly Algorithm-**

Receiver applies the following steps for reassembly of all the fragments-

1. It identifies whether datagram is fragmented or not using MF bit and Fragment offset field.
2. It identifies all the fragments belonging to the same datagram using identification field.
3. It identifies the first fragment. Fragment with offset field value = 0 is the first fragment.
4. It identifies the subsequent fragments using total length, header length and fragment offset.

5. It repeats step-04 until MF bit = 0.

Fragment Offset field value for the next subsequent fragment

= ( Payload length of the current fragment / 8 ) + Offset field value of the current fragment

= ( Total length – Header length / 8 ) + Offset field value of the current fragment

**Fragmentation Overhead-**

- Fragmentation of datagram increases the overhead.
- This is because after fragmentation, IP header has to be attached with each fragment.

Total Overhead

= (Total number of fragmented datagrams – 1) x size of IP header

Efficiency = Useful bytes transferred / Total bytes transferred

**OR**

Efficiency = Data without header / Data with header

Bandwidth Utilization or Throughput = Efficiency x Bandwidth

**Advantages of IPv4**

- IPv4 security permits encryption to keep up privacy and security.
- IPV4 network allocation is significant and presently has quite 85000 practical routers.
- It becomes easy to attach multiple devices across an outsized network while not NAT.
- This is a model of communication so provides quality service also as economical knowledge transfer.
- IPV4 addresses are redefined and permit flawless encoding.

- Routing is a lot of scalable and economical as a result of addressing is collective more effectively.
- Data communication across the network becomes a lot of specific in multicast organizations.

**Disadvantages of IPv4**

- Limits net growth for existing users and hinders the use of the net for brand new users.
- Internet Routing is inefficient in IPv4.
- IPv4 has high System Management prices and it's labor intensive, complex, slow & frequent to errors.
- Security features are non-obligatory.
- Difficult to feature support for future desires as a result of adding it on is extremely high overhead since it hinders the flexibility to attach everything over IP.

**IPV6**

Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IP v6 is 128-bits address having an address space of 2^128, which is way bigger than IPv4. In IPv6 we use Colon-Hexa representation. There are 8 groups and each group represents 2 Bytes


In IPv6 representation, we have three addressing methods :

- Unicast
- Multicast
- Anycast

**Unicast Address:** Unicast Address identifies a single network interface. A packet sent to unicast address is delivered to the interface identified by that address.

**Multicast Address:** Multicast Address is used by multiple hosts, called as Group, acquires a multicast destination address. These hosts need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address.

**Anycast Address:** Anycast Address is assigned to a group of interfaces. Any packet sent to anycast address will be delivered to only one member interface (mostly nearest host possible).

**Types of IPv6 address:**

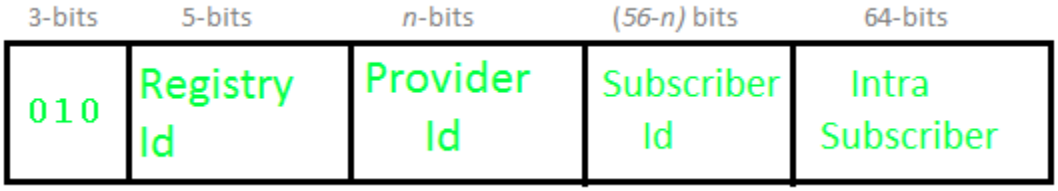
We have 128 bits in IPv6 address but by looking at first few bits we can identify what type of address it is.

| PREFIX | ALLOCATION | FRACTION OF ADDRESS SPACE |
|---|---|---|
| 0000 0000 | Reserved | 1/256 |
| 0000 0001 | Unassigned (UA) | 1/256 |
| 0000 001 | Reserved for NSAP | 1/128 |
| 0000 01 | UA | 1/64 |
| 0000 1 | UA | 1/32 |
| 0001 | UA | 1/16 |
| 001 | Global Unicast | 1/8 |
| 010 | UA | 1/8 |
| 011 | UA | 1/8 |
| 100 | UA | 1/8 |
| 101 | UA | 1/8 |
| 110 | UA | 1/8 |
| 1110 | UA | 1/16 |
| 1111 0 | UA | 1/32 |
| 1111 10 | UA | 1/64 |
| 1111 110 | UA | 1/128 |
| 1111 1110 0 | UA | 1/512 |
| 1111 1110 10 | Link-Local Unicast Addresses | 1/1024 |

| PREFIX | ALLOCATION | FRACTION OF ADDRESS SPACE |
|---|---|---|
| 1111 1110 11 | Site-Local Unicast Addresses | 1/1024 |
| 1111 1111 | Multicast Address | 1/256 |

**Note :** In IPv6, all 0's and all 1's can be assigned to any host, there is not any restriction like IPv4.

**Provider based Unicast address :**
These are used for global communication.

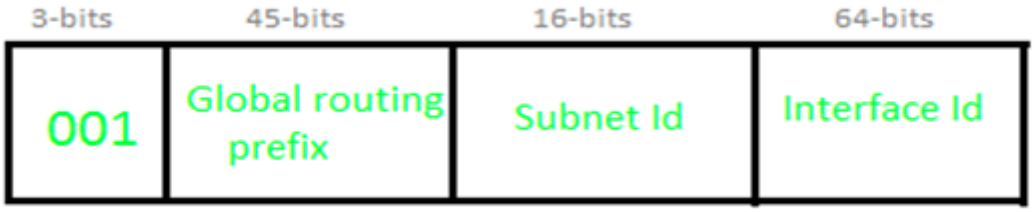



First 3 bits identifies it as of this type.
**Registry Id (5-bits) :** Registry Id identifies the region to which it belongs. Out of 32 (i.e. 2^5), only 4 registry id's are being used.

| Registry Id | Registry |
|---|---|
| 10000 | Multi regional (IANA) |
| 01000 | RIPE NCC |
| 11000 | INTER NIC |
| 00100 | APNIC |

**Provider Id :** Depending on the number of service providers that operates under a region, certain bits will be allocated to Provider Id field. This field need not be fixed. Let's say if Provider Id = 10 bits then Subscriber Id will be 56 – 10 = 46 bits.
**Subscriber Id :** After Provider Id is fixed, remaining part can be used by ISP as normal IP address.
**Intra Subscriber :** This part can be modified as per need of organization that is using the service.

**Geography based Unicast address :**




**Global routing prefix :** Global routing prefix contains all the details of Latitude and Longitude. As of now, it is not being used. In Geography based Unicast address routing will be

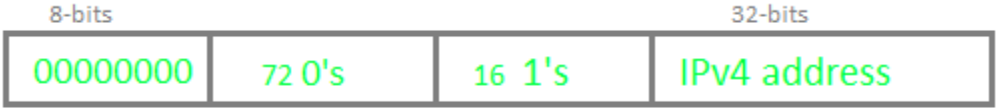
based on location.
**Interface Id :** In IPv6, instead of using Host Id, we use the term Interface Id.

**Some special addresses:**
**Unspecified –**


**Loopback –**

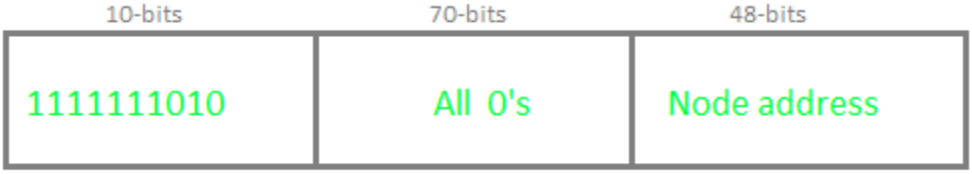

**IPv4 Compatible –**


**IPv4 mapped –**




**Local Unicast Addresses :**
There are two types of Local Unicast addresses defined- *Link local* and *Site Local*.

**Link local address:**




Link local address is used for addressing on a single link. It can also be used to communicate with nodes on the same link. Link local address always begins with 1111111010 (i.e. FE80). Router will not forward any packet with Link local address.

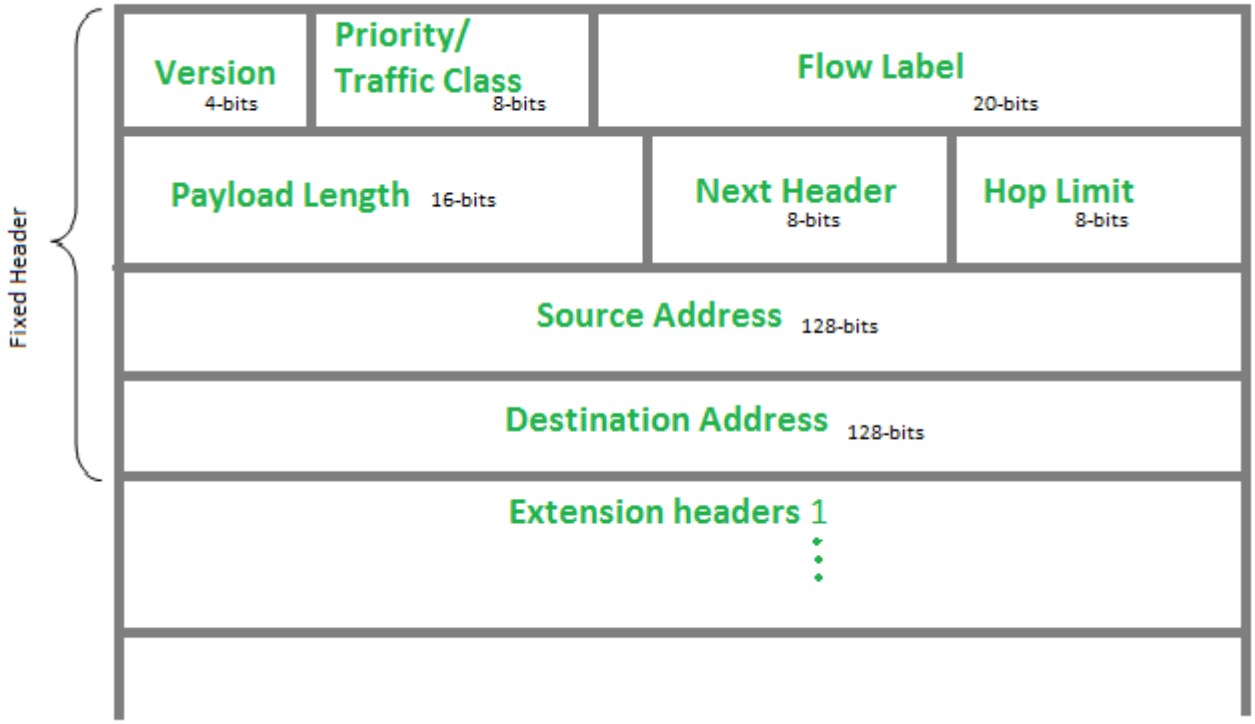
**Site local address:**


Site local addresses are equivalent to private IP address in IPv4. Likely, some address space is reserved, which can only be routed within an organization. First 10-bits are set to 1111111011, which is why Site local addresses always begin with FEC0. Following 32 bits are Subnet ID, which can be used to create subnet within organization. Node address is used to uniquely identify the link; therefore, we use 48-bits MAC address here.

**IPV6-HEADER**

IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. Let's look at the header of IP version 6 and understand how it is different from IPv4 header.

**IP version 6 Header Format :**




**Version (4-bits) :** Indicates version of Internet Protocol which contains bit sequence 0110.
**Traffic Class (8-bits) :** The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on priority of the packet. If congestion occurs on router then packets with least priority will be discarded. As of now only 4-bits are being used (and remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.

Priority assignment of Congestion controlled traffic :

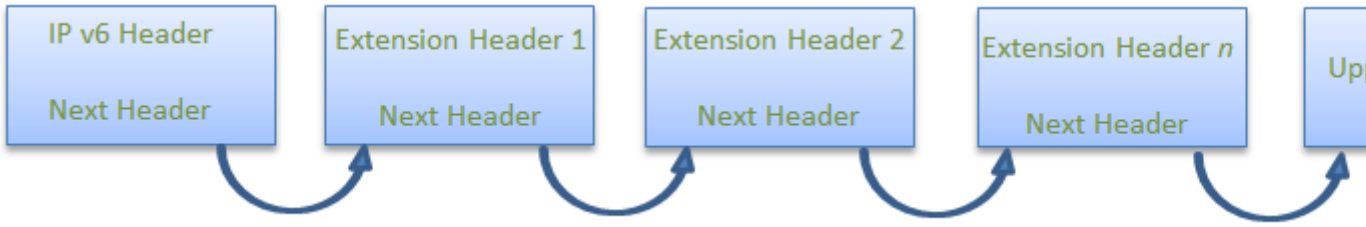
| Priority | Meaning |
|---|---|
| 0 | No Specific traffic |
| 1 | Background data |
| 2 | Unattended data traffic |
| 3 | Reserved |
| 4 | Attended bulk data traffic |
| 5 | Reserved |
| 6 | Interactive traffic |
| 7 | Control traffic |

Uncontrolled data traffic is mainly used for Audio/Video data. So we give higher priority to Uncontrolled data traffic.
Source node is allowed to set the priorities but on the way routers can change it. Therefore, destination should not expect same priority which was set by source node.

**Flow Label (20-bits) :** Flow Label field is used by source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real time service. In order to distinguish the flow, intermediate router can use source address, destination address and flow label of the packets. Between a source and destination multiple flows may exist because many processes might be running at the same time. Routers or Host that do not support the functionality of flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, source is also supposed to specify the lifetime of flow.
**Payload Length (16-bits) :** It is a 16-bit (unsigned integer) field, indicates total size of the payload which tells routers about amount of information a particular packet contains in its payload. Payload Length field includes extension headers(if any) and upper layer packet. In case length of payload is greater than 65,535 bytes (payload up to 65,535 bytes can be indicated with 16-bits), then the payload length field will be set to 0 and jumbo payload option is used in the Hop-by-Hop options extension header.
**Next Header (8-bits) :** Next Header indicates type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packet, such as TCP, UDP.
**Hop Limit (8-bits) :** Hop Limit field is same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and packet is discarded if value decrements to 0. This is used to discard the packets that are stuck in infinite loop because of some routing error.
**Source Address (128-bits) :** Source Address is 128-bit IPv6 address of the original source of the packet.
**Destination Address (128-bits) :** Destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.

**Extension Headers :** In order to rectify the limitations of *IPv4 Option Field*, Extension Headers are introduced in IPversion 6. The extension header mechanism is very important part

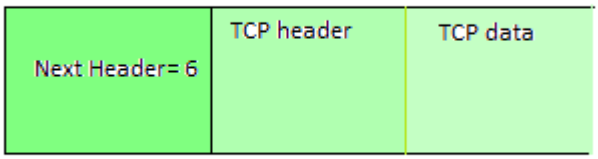
of the IPv6 architecture. Next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.



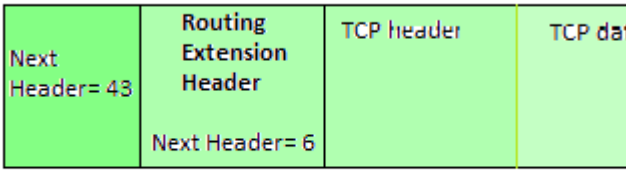

IPv6 packet may contain zero, one or more extension headers but these should be present in their recommended order:

| Order | Header Type | Next Header Code |
|---|---|---|
| 1 | Basic IPv6 Header | - |
| 2 | Hop-by-Hop Options | 0 |
| 3 | Destination Options (with Routing Options) | 60 |
| 4 | Routing Header | 43 |
| 5 | Fragment Header | 44 |
| 6 | Authentication Header | 51 |
| 7 | Encapsulation Security Payload Header | 50 |
| 8 | Destination Options | 60 |
| 9 | Mobility Header | 135 |
| | No next header | 59 |
| Upper Layer | TCP | 6 |
| Upper Layer | UDP | 17 |
| Upper Layer | ICMPv6 | 58 |

Example: *TCP is used in IPv6 packet*




Example2:




**Rule :** Hop-by-Hop option header(if present) should always be placed after IPv6 base header.
**Conventions :**

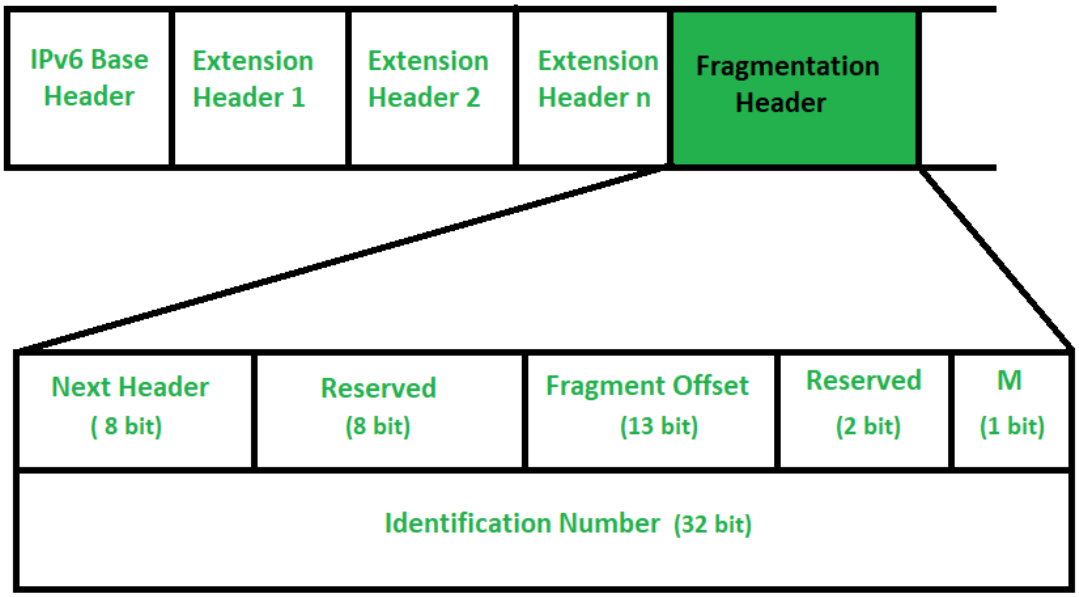
1. Any extension header can appear at most once except Destination Header because Destination Header is present two times in above list itself.
2. If Destination Header is present before Routing Header then it will be examined by all intermediate nodes specified in routing header.
3. If Destination Header is present just above Upper layer then it will be examined only by Destination node.

Given order in which all extension header should be chained in IPv6 packet and working of each extension header **:**

| Ext. Header | Description |
|---|---|
| Hop-by-Hop Options | Examined by all devices on the path |
| Destination Options (with routing options) | Examined by destination of the packet |
| Routing Header | Methods to take routing decision |
| Fragment Header | Contains parameters of fragmented datagram done by source |
| Authentication Header | verify authenticity |
| Encapsulating Security Payload | Carries Encrypted data |

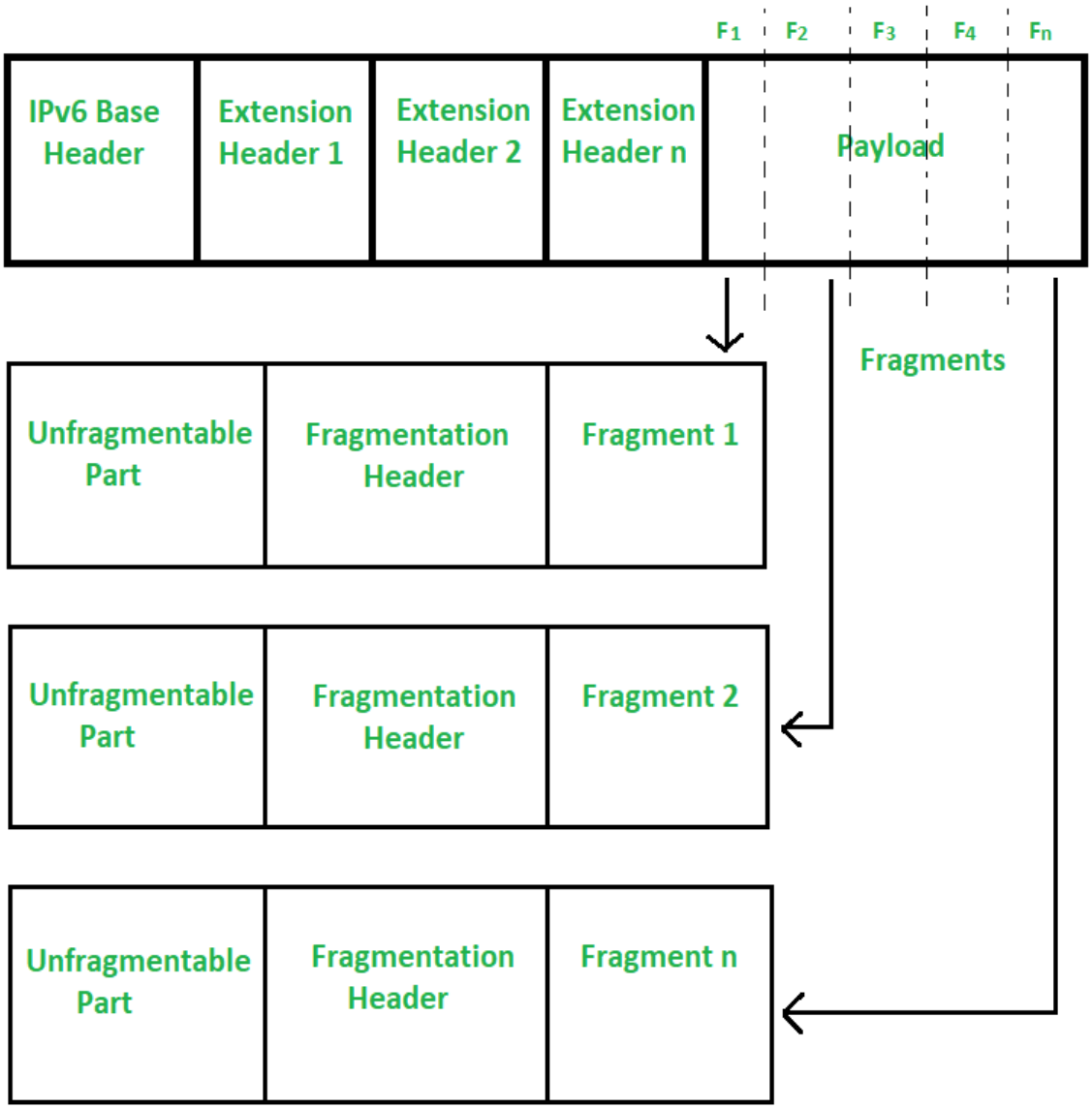
## IPV6 FRAGMENTATION HEADER

In IPv4 fragmentation is done whenever required, at destination or at routers whereas in IPv6 only source is supposed to do fragmentation but not routers. This can only be done when source knows path Maximum Transmission Unit (MTU). In Ipv6 “do not fragment” bit is always 1 where case is not same in IPv4 and ‘More fragment’ bit is only flag in fragmentation header which is of one bit. Two bits are reserved for future use as you can see in picture below.
Internet Protocol Version 6 Fragmentation Header –




- **Next Header –**
  The Next Header is an 8-bit field that identifies type of header present after Fragmentation header.
- **Reserved –**
  It is an 8 bit field which is completely zero as of now. In future, we might find something useful to fill here. Also again an extra 2-bit field is reserved for later purposes.
- **Fragment Offset –**
  It is exactly same as than in IPv4 which is of size 13 bits. Just as we did to scale up fragment offset in IPv4 we will do same in IPv6.
- **More Fragment (M) –**
  More fragment bit in here is denoted by “M”. It’s a one-bit field that tells us if there are more fragments coming after it. If more fragment bit is zero then it means its last fragment and if 1 then it could be any packet except being last one.
- **Identification Number –**
  The identification number field which is same for all fragments of a particular packet is double in size as that of in IPv4. In packet identifier field is of 32 bits and In IPv4 it was of 16 bits.

The IPv6 sender may perform fragmentation at source because an IPv6 router cannot perform a fragmentation, so if packet is too large for next hop, router will generate an ICMP packet to let the source know that packet is too large in size.




The fragmentation header tries to minimize use of fragmentation as much as possible by supporting minimum packet size of 1280 Bytes. As shown in above picture how fragmentation is taken place according to MTU that sender knows.

IPv6 and other Extension headers are **unfragmentable** part because every fragment has to go through nodes or routers and at every router, information stored in these extensions headers are required. That is why IPv6 packet is divided into two parts. One is unfragmentable part and other is **fragmentable** part. The unfragmentable part does not encounter any modification in between and another part being fragmentable is divided into many small fragments as fragment 1, fragment 2, and so on.

After small fragments being created fragmentation header and particular fragment ( as fragment 1 ) is connected to unfragmentable part and is send to destination. Payload length may change after fragmentation and after fragmentation header is added corresponding fields like next header, identification number, fragment offset, and more fragment bits are filled appropriately.

**Advantages of IPv6**

- Reliability
- **Faster Speeds:** IPv6 supports multicast rather than broadcast in IPv4.This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.
- **Stringer Security:** IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.
- Routing efficiency
- Most importantly it's the final solution for growing nodes in Global-network.

**Disadvantages of IPv6**

- **Conversion:** Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.
- **Communication:** IPv4 and IPv6 machines cannot communicate directly with each other. They need an intermediate technology to make that possible.

| | **IPV4** | **IPV6** |
|---|---|---|
| | IPv4 has 32-bit address length | IPv6 has 128-bit address length |
| | It Supports Manual and DHCP address configuration | It supports Auto and renumbering address configuration |
| | In IPv4 end to end connection integrity is Unachievable | In IPv6 end to end connection integrity is Achievable |
| | It can generate 4.29×109 address space | Address space of IPv6 is quite large it can produce 3.4×1038 address space |
| | Security feature is dependent on application | IPSEC is inbuilt security feature in the IPv6 protocol |
| | Address representation of IPv4 is in decimal | Address Representation of IPv6 is in hexadecimal |
| | Fragmentation performed by Sender and forwarding routers | In IPv6 fragmentation performed only by sender |

| | | |
|---|---|---|
| | In IPv4 Packet flow identification is not available | In IPv6 packetflow identification are Available and uses flow label field in the header |
| | In IPv4 checksumfield is available | In IPv6 checksumfield is not available |
| | It has broadcast Message Transmission Scheme | In IPv6 multicast and any cast message transmission scheme is available |
| | In IPv4 Encryption and Authentication facility not provided | In IPv6 Encryption and Authentication are provided |
| | IPv4 has header of 20-60 bytes. | IPv6 has header of 40 bytes fix |

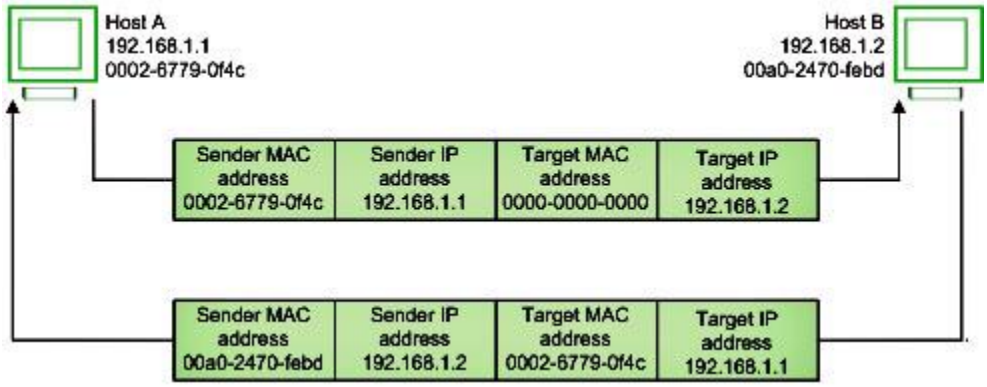
**Address Resolution Protocol (ARP) –**

- Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address. This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.

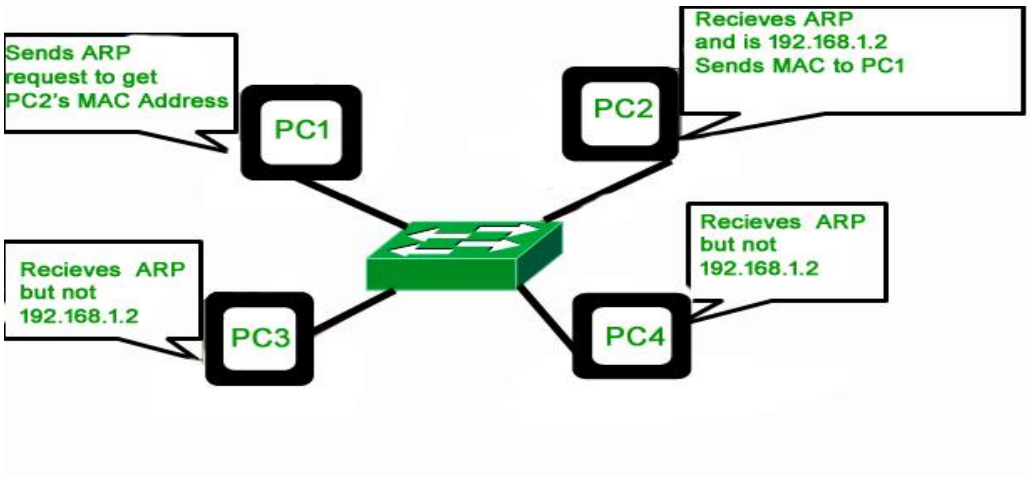
**There are four types of Address Resolution Protocol, which is given below:**

- Proxy ARP
- Gratuitous ARP
- Reverse ARP (RARP)
- Inverse ARP

Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address.
In order to send the data to destination, having IP address is necessary but not sufficient; we also need the physical address of the destination machine. ARP is used to get the physical address (MAC address) of destination machine.




Before sending the IP packet, the MAC address of destination must be known. If not so, then sender broadcasts the ARP-discovery packet requesting the MAC address of intended destination. Since ARP-discovery is broadcast, every host inside that network will get this message but the packet will be discarded by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP-reply) to the sender of ARP-discovery packet. After the original sender receives the ARP-reply, it updates ARP-cache and start sending unicast message to the destination.




## Reverse Address Resolution Protocol (RARP) –

Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router's ARP table. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.
When a new machine is setup or any machine which don't have memory to store IP address, needs an IP address for its own use. So the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.

A special host configured inside the local area network, called as RARP-server is responsible to reply for these kind of broadcast packets. Now the RARP server attempt to find out the entry in IP to MAC address mapping table. If any entry matches in table, RARP server send the response packet to the requesting device along with IP address.

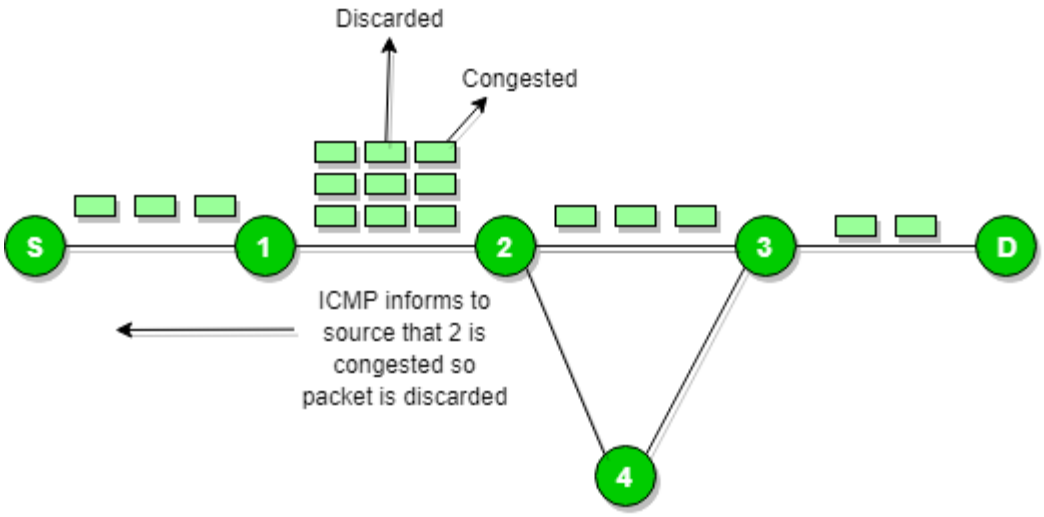
- LAN technologies like Ethernet, Ethernet II, Token Ring and Fiber Distributed Data Interface (FDDI) support the Address Resolution Protocol.
- RARP is not being used in today's networks. Because we have much great featured protocols like BOOTP (Bootstrap Protocol) and DHCP( Dynamic Host Configuration Protocol).

**ICMP- Internet Control Message Protocol**

Since IP does not have a inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide an error control. It is used for reporting errors and management queries. It is a supporting protocol and used by networks devices like routers for sending the error messages and operations information.
e.g. the requested service is not available or that a host or router could not be reached.

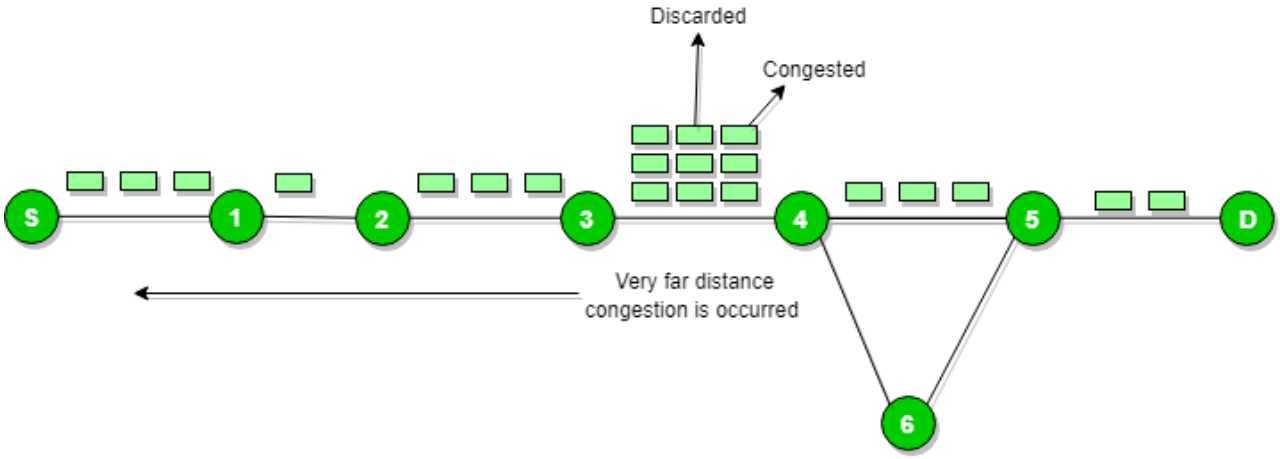
**Source quench message :**

Source quench message is request to decrease traffic rate for messages sending to the host(destination). Or we can say, when receiving host detects that rate of sending packets (traffic rate) to it is too fast it sends the source quench message to the source to slow the pace down so that no packet can be lost.




ICMP will take source IP from the discarded packet and informs to source by sending source quench message.

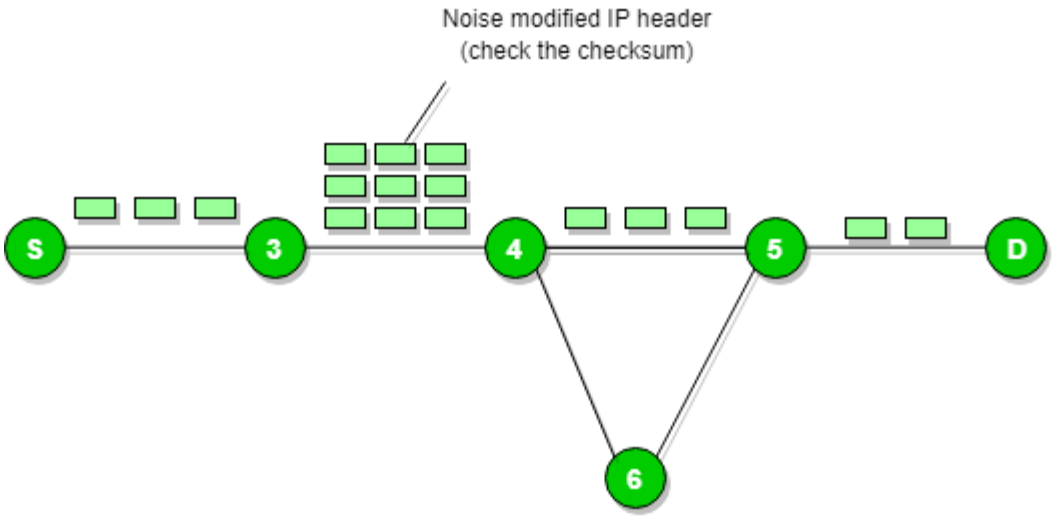
Then source will reduce the speed of transmission so that router will free for congestion.




When the congestion router is far away from the source the ICMP will send hop by hop source quench message so that every router will reduce the speed of transmission.

**Parameter problem :**

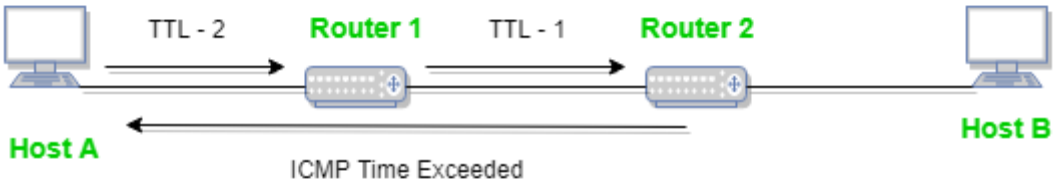
Whenever packets come to the router then calculated header checksum should be equal to recieved header checksum then only packet is accepted by the router.

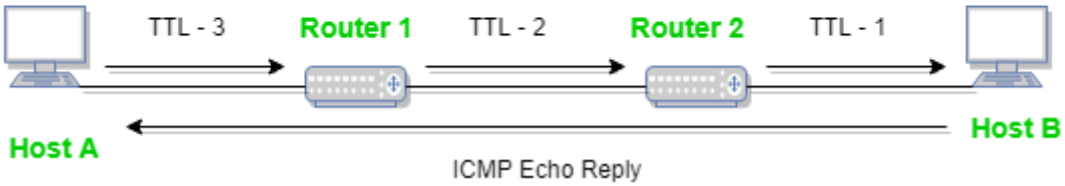



If there is mismatch packet will be dropped by the router.

ICMP will take the source IP from the discarded packet and informs to source by sending parameter problem message.

**Time exceeded message :**

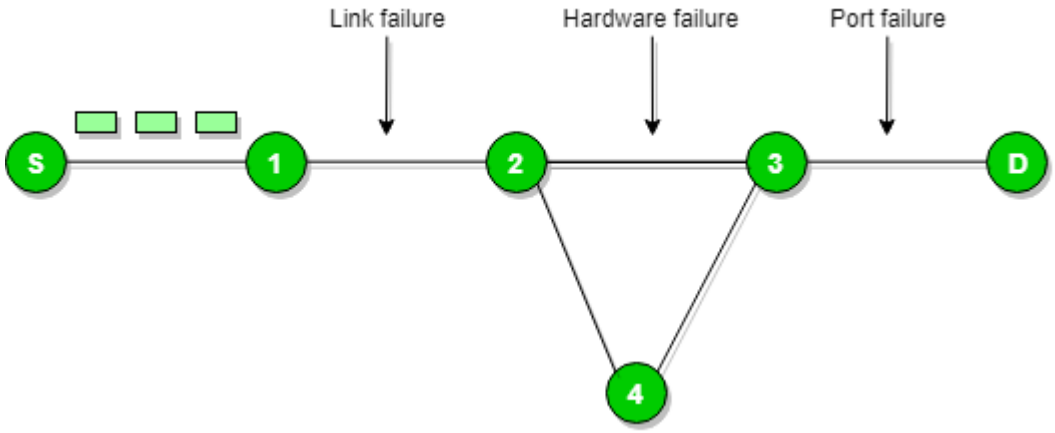




When some fragments are lost in a network then the holding fragment by the router will be droped then ICMP will take source IP from discarded packet and informs to the source, of discarded datagram due to time to live field reaches to zero, by sending time exceeded message.

**Destination un-reachable :**

Destination unreachable is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.




There is no necessary condition that only router give the ICMP error message some time destination host send ICMP error message when any type of failure (link failure,hardware failure,port failure etc) happen in the network.

**Redirection message :**

Redirect requests data packets be sent on an alternate route. The message informs to a host to update its routing information (to send packets on an alternate route).

**Ex.** If host tries to send data through a router R1 and R1 sends data on a router R2 and there is a direct way from host to R2. Then R1 will send a redirect message to inform the host that there is a best way to the destination directly through R2 available. The host then sends data packets for the destination directly to R2.
The router R2 will send the original datagram to the intended destination.
But if datagram contains routing information then this message will not be sent even if a better route is available as redirects should only be sent by gateways and should not be sent by Internet hosts.

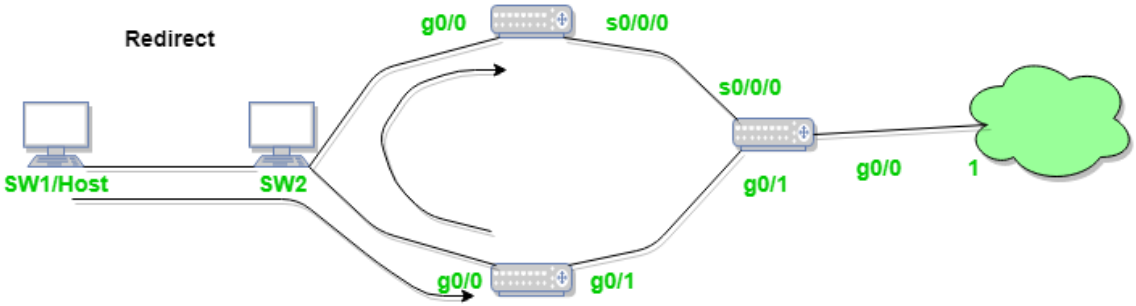


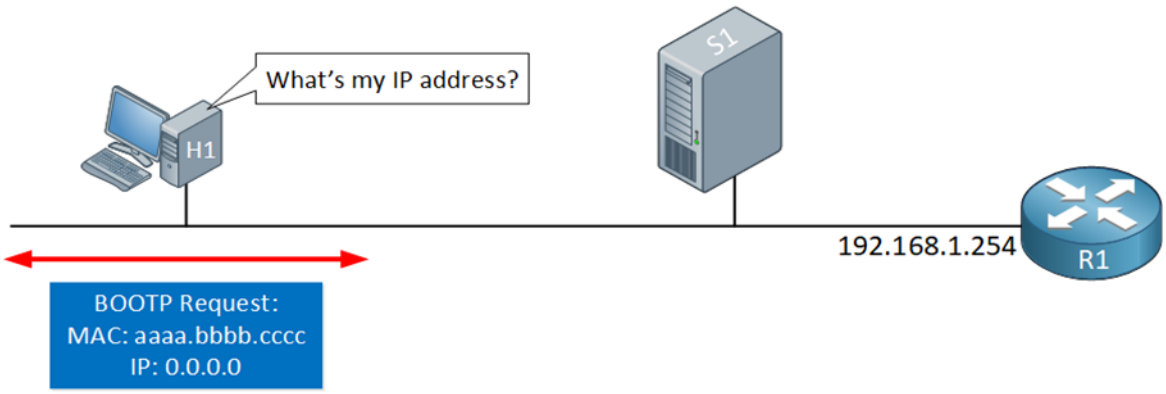

**Figure** - ICMP redirect Verification CCNP 2.0 100 - 101 (v - 71)

- ICMP Redirect
- ICMP Redirect for host
- ICMP Redirect for network
- How ICMP redirect work
- ICMP Redirect verification step by step

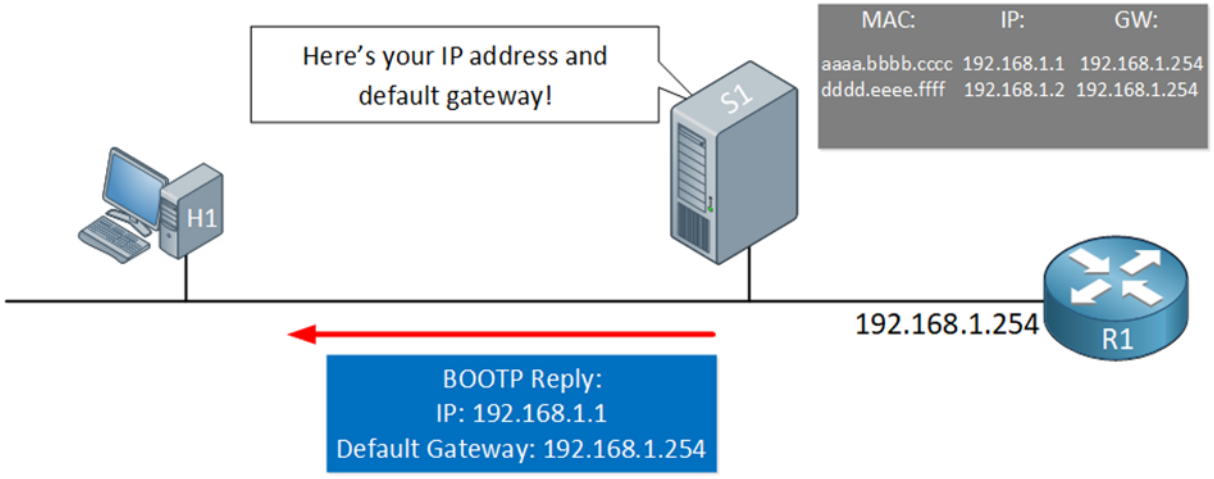
Whenever a packet is forwarded in a wrong direction later it is re-directed in a current direction then ICMP will send re-directed message.

**BOOTP-BOOTSTRAP PROTOCOL**

- BOOTP (Bootstrap Protocol) is the successor of RARP (Reverse ARP) and the predecessor of DHCP.
- BOOTP uses the UDP transport protocol and rides on top of IP so it can be routed. BOOTP supports relay servers so you can have a central BOOTP server that assigns IP addresses to hosts in all of your subnets.
- BOOTP uses UDP port 67 and 68.
- BOOTP uses a static database that you have to fill yourself.




- The host sends a BOOTP request and uses UDP source port 68 and destination port 67. This packet is a broadcast so everything in the broadcast domain receives it. On our network, we have a BOOTP server listening on UDP port 67.




- The server sees the broadcast packet from the host and since it's listening on UDP port 67, it processes the packet. The server then looks in its database to find a matching entry for the MAC address of the host. When there is a match, it returns the information to the host with a unicast packet.
- Nowadays, we don't use BOOTP as it has been replaced by DHCP. Since DHCP was built on BOOTP, if you look at a DHCP capture, you will see bootstrap terminology in the packets.

**DHCP-Dynamic Host Configuration Protocol**

- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.
- DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments)

DHCP does the following:

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.
- DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

The DHCP lease process works as follows:

- First of all, a client (network device) must be connected to the internet.
- DHCP clients request an IP address. Typically, client broadcasts a query for this information.
- DHCP server responds to the client request by providing IP server address and other configuration information. This configuration information also includes time period, called a lease, for which the allocation is valid.
- When refreshing an assignment, a DHCP clients request the same parameters, but the DHCP server may assign a new IP address. This is based on the policies set by the administrator.

**Components of DHCP**

- DHCP Server: DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.

- DHCP client: DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
- IP address pool: IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- Subnet: Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
- Lease: Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
- DHCP relay: A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

There are following benefits of DHCP:

- Centralized administration of IP configuration: DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

**BENEFITS OF DHCP**

- Dynamic host configuration: DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.
- Seamless IP host configuration: The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.
- Flexibility and scalability: Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

**Routing algorithm**

- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.
- The Routing algorithm is divided into two categories:

**Adaptive Routing algorithm**

- An adaptive routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decisions based on the topology and network traffic.
- The main parameters related to this algorithm are hop count, distance and estimated transit time.

**Non-Adaptive Routing algorithm**

- Non Adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

**LINK STATE ALGORITHM**

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

- The three keys to understand the Link State Routing algorithm:
- Knowledge about the neighborhood: Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
- Flooding: Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.

- Information sharing: A router sends the information to every other router only when the change occurs in the information.
- Link State Routing has two phases:

  Reliable Flooding

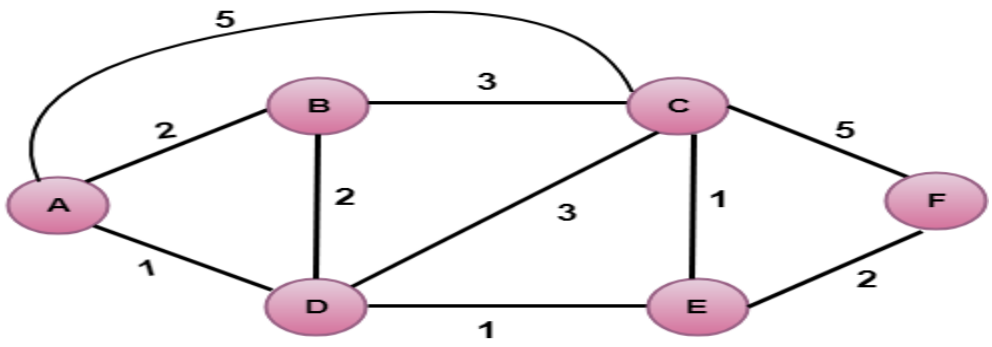
- Initial state: Each node knows the cost of its neighbors.
- Final state: Each node knows the entire graph.

  Route Calculation

- Each node uses Dijkstra's algorithm on the graph to calculate the optimal routes to all nodes
- The Link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.
- The Dijkstra's algorithm is an iterative, and it has the property that after $k^{th}$ iteration of the algorithm, the least cost paths are well known for k destination nodes.

**Dijkstra's algorithm-Procedure**

- Step-1: The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database
- Step-2: Now the node selects one node, among all the nodes not in the tree like structure, which is nearest to the root, and adds this to the tree.The shape of the tree gets changed .
- Step-3: After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.
- Step-4: The node repeats the Step 2. and Step 3. until all the nodes are added in the tree




**Vertex-A**

Step 1:

The first step is an initialization step. The currently known least cost path from A to its directly attached neighbors, B, C, D are 2,5,1 respectively. The cost from A to B is set to 2, from A to D is set to 1 and from A to C is set to 5. The cost from A to E and F are set to infinity as they are not directly linked to A.

| Step | N | D(B),P(B) | D(C),P(C) | D(D),P(D) | D(E),P(E) | D(F),P(F) |
|---|---|---|---|---|---|---|
| 1 | A | 2,A | 5,A | 1,A | ∞ | ∞ |

Step 2:

In the above table, we observe that vertex D contains the least cost path in step 1. Therefore, it is added in N. Now, we need to determine a least-cost path through D vertex.

**a) Calculating shortest path from A to B**

1. v = B, w = D
2. D(B) = min( D(B) , D(D) + c(D,B) )
3. = min( 2, 1+2)>
4. = min( 2, 3)
5. The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

**b) Calculating shortest path from A to C**

1. v = C, w = D
2. D(B) = min( D(C) , D(D) + c(D,C) )
3. = min( 5, 1+3)
4. = min( 5, 4)
5. The minimum value is 4. Therefore, the currently shortest path from A to C is 4.</p>

**c) Calculating shortest path from A to E**

1. v = E, w = D
2. D(B) = min( D(E) , D(D) + c(D,E) )
3. = min( ∞, 1+1)
4. = min(∞, 2)
5. The minimum value is 2. Therefore, the currently shortest path from A to E is 2.

*Note: The vertex D has no direct link to vertex E. Therefore, the value of D(F) is infinity.*

| Step | N | D(B),P(B) | D(C),P(C) | D(D),P(D) | D(E),P(E) | D(F),P(F) |
|---|---|---|---|---|---|---|
| 1 | A | 2,A | 5,A | 1,A | ∞ | ∞ |
| 2 | AD | 2,A | 4,D | | 2,D | ∞ |

Step 3:

In the above table, we observe that both E and B have the least cost path in step 2. Let's consider the E vertex. Now, we determine the least cost path of remaining vertices through E.

**a) Calculating the shortest path from A to B.**

1. v = B, w = E
2. D(B) = min( D(B) , D(E) + c(E,B) )
3. = min( 2 , 2+ ∞ )
4. = min( 2, ∞)
5. The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

**b) Calculating the shortest path from A to C.**

1. v = C, w = E
2. D(B) = min( D(C) , D(E) + c(E,C) )
3. = min( 4 , 2+1 )
4. = min( 4,3)
5. The minimum value is 3. Therefore, the currently shortest path from A to C is 3.

**c) Calculating the shortest path from A to F.**

1. v = F, w = E
2. D(B) = min( D(F) , D(E) + c(E,F) )
3. = min( ∞ , 2+2 )
4. = min(∞ ,4)
5. The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

| Step | N | D(B),P(B) | D(C),P(C) | D(D),P(D) | D(E),P(E) | D(F),P(F) |
|---|---|---|---|---|---|---|
| 1 | A | 2,A | 5,A | 1,A | ∞ | ∞ |
| 2 | AD | 2,A | 4,D | | 2,D | ∞ |
| 3 | ADE | 2,A | 3,E | | | 4,E |

Step 4:

In the above table, we observe that B vertex has the least cost path in step 3. Therefore, it is added in N. Now, we determine the least cost path of remaining vertices through B.

**a) Calculating the shortest path from A to C.**

1. v = C, w = B
2. D(B) = min( D(C) , D(B) + c(B,C) )
3. = min( 3 , 2+3 )
4. = min( 3,5)
5. The minimum value is 3. Therefore, the currently shortest path from A to C is 3.

**b) Calculating the shortest path from A to F.**

1. v = F, w = B
2. D(B) = min( D(F) , D(B) + c(B,F) )
3. = min( 4, ∞)
4. = min(4, ∞)
5. The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

| Step | N | D(B),P(B) | D(C),P(C) | D(D),P(D) | D(E),P(E) | D(F),P(F) |
|---|---|---|---|---|---|---|
| 1 | A | 2,A | 5,A | 1,A | ∞ | ∞ |
| 2 | AD | 2,A | 4,D | | 2,D | ∞ |
| 3 | ADE | 2,A | 3,E | | | 4,E |
| 4 | ADEB | | 3,E | | | 4,E |

Step 5:

In the above table, we observe that C vertex has the least cost path in step 4. Therefore, it is added in N. Now, we determine the least cost path of remaining vertices through C.

**a) Calculating the shortest path from A to F.**

1. v = F, w = C
2. D(B) = min( D(F) , D(C) + c(C,F) )
3. = min( 4, 3+5)
4. = min(4,8)
5. The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

| Step | N | D(B),P(B) | D(C),P(C) | D(D),P(D) | D(E),P(E) | D(F),P(F) |
|---|---|---|---|---|---|---|
| 1 | A | 2,A | 5,A | 1,A | ∞ | ∞ |
| 2 | AD | 2,A | 4,D | | 2,D | ∞ |
| 3 | ADE | 2,A | 3,E | | | 4,E |
| 4 | ADEB | | 3,E | | | 4,E |
| 5 | ADEBC | | | | | 4,E |

Final table:

| Step | N | D(B),P(B) | D(C),P(C) | D(D),P(D) | D(E),P(E) | D(F),P(F) |
|---|---|---|---|---|---|---|
| 1 | A | 2,A | 5,A | 1,A | ∞ | ∞ |
| 2 | AD | 2,A | 4,D | | 2,D | ∞ |
| 3 | ADE | 2,A | 3,E | | | 4,E |
| 4 | ADEB | | 3,E | | | 4,E |
| 5 | ADEBC | | | | | 4,E |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | ADEBCF | | | | | |

Disadvantage:

Heavy traffic is created in Line state routing due to Flooding. Flooding can cause an infinite looping, this problem can be solved by using Time-to-leave field

**DISTANCE VECTOR ROUTING ALGORITHM**

A **distance-vector routing (DVR)** protocol requires that a router inform its neighbors of topology changes periodically. Historically known as the old ARPANET routing algorithm (or known as Bellman-Ford algorithm).

**Bellman Ford Basics –** Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances,based on a chosen metric, are computed using information from the neighbors' distance vectors.

Information kept by DV router -

- Each router has an ID
- Associated with each link connected to a router,
- there is a link cost (static or dynamic).
- Intermediate hops

Distance Vector Table Initialization -

- Distance to itself = 0
- Distance to ALL other routers = infinity number.

**Distance Vector Algorithm –**

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
    - It receives a distance vector from a neighbor containing different information than before.
    - It discovers that a link to a neighbor has gone down.

The DV calculation is based on minimizing the cost to each destination

Dx(y) = Estimate of least cost from x to y

C(x,v) = Node x knows cost to each neighbor v

Dx = [Dx(y): y ∈ N ] = Node x maintains distance vector

Node x also maintains its neighbors' distance vectors

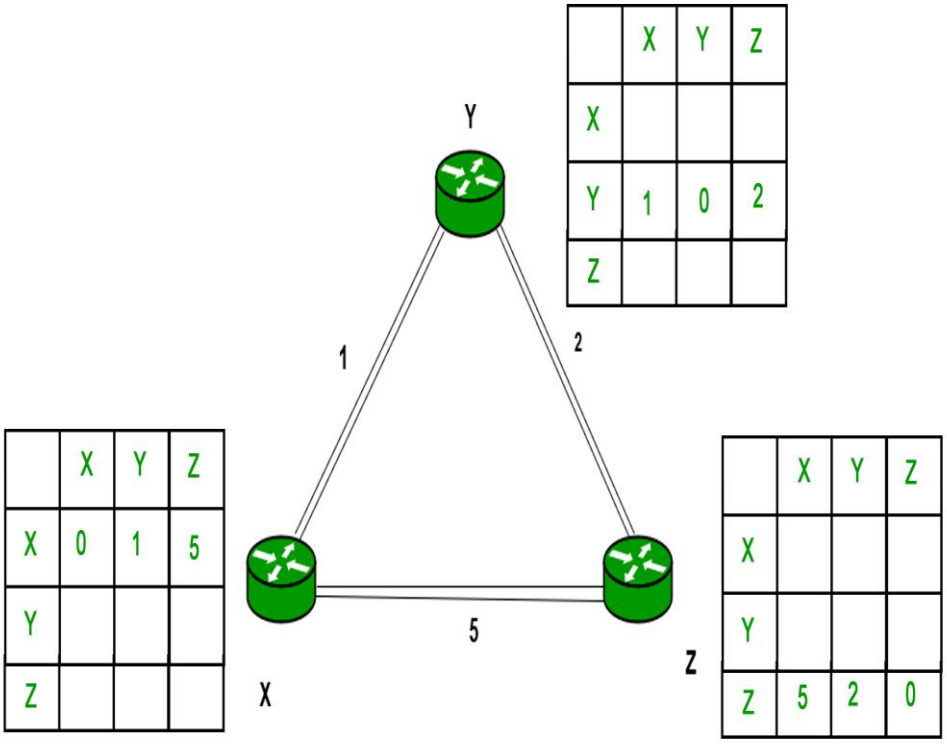
– For each neighbor v, x maintains Dv = [Dv(y): y ∈ N ]

**NOTE:**

- From time-to-time, each node sends its own distance vector estimate to neighbors.

- When a node x receives new DV estimate from any neighbor v, it saves v's distance vector and it updates its own DV using B-F equation:
- Dx(y) = min { C(x,v) + Dv(y), Dx(y) } for each node y ∈ N

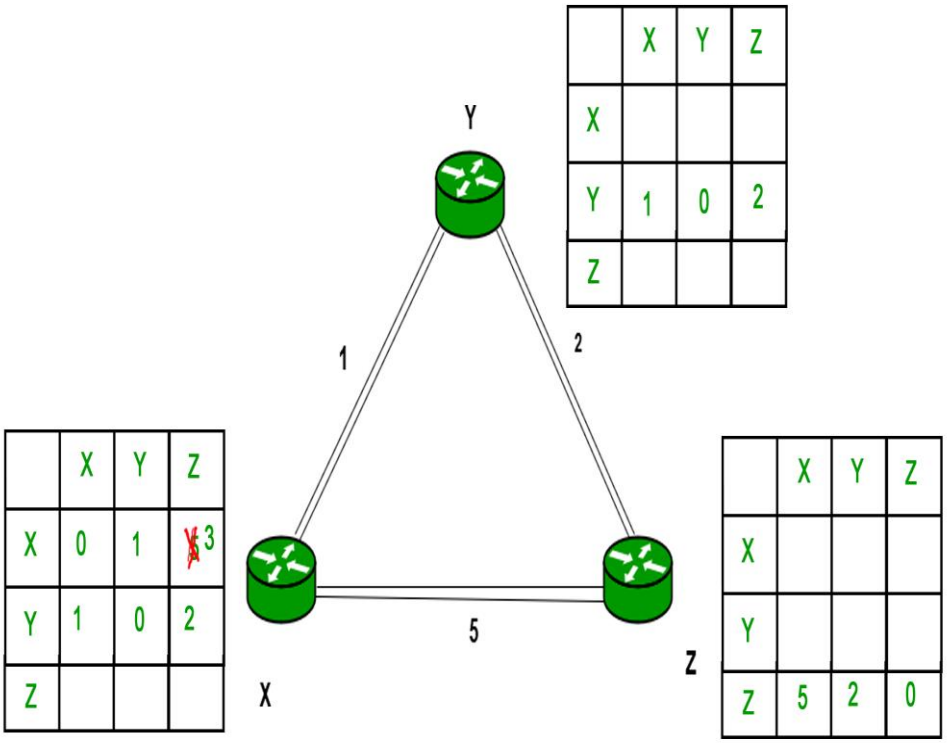
**Example –** Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



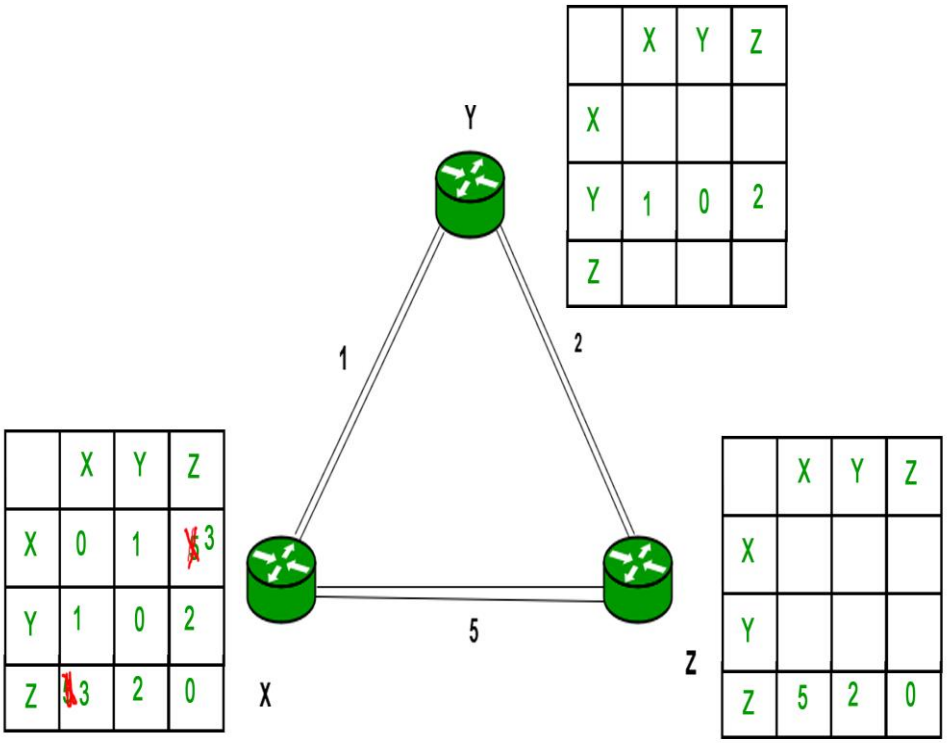

Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

Dx(y) = min { C(x,v) + Dv(y)} for each node y ∈ N

As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.




Similarly for Z also –

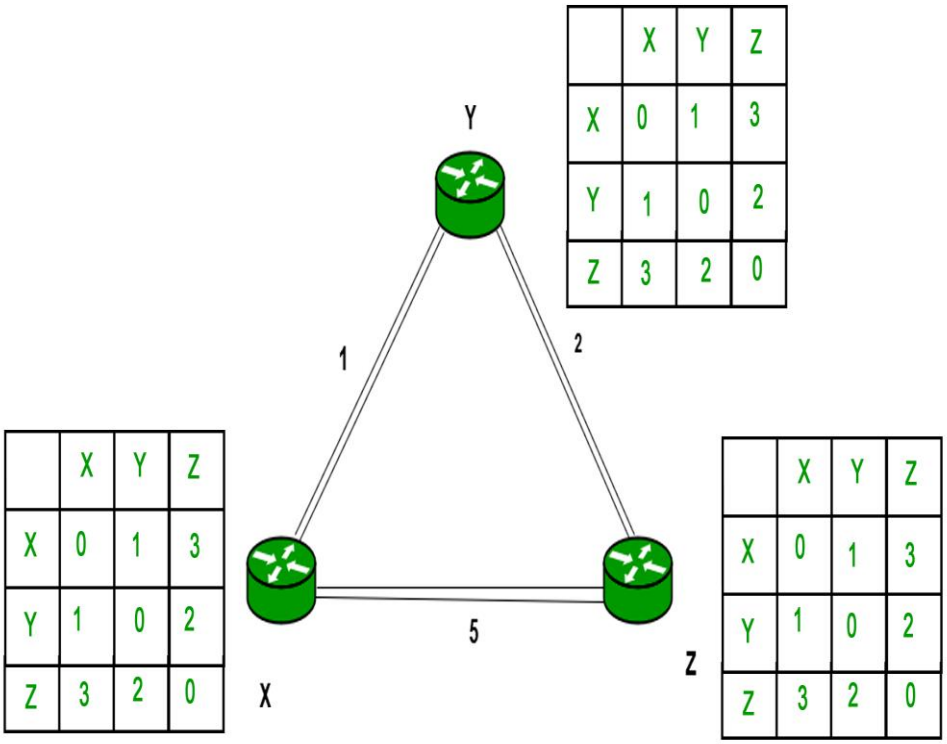



| | X | Y | Z |
|---|---|---|---|
| X | | | |
| Y | 1 | 0 | 2 |
| Z | | | |

| | X | Y | Z |
|---|---|---|---|
| X | 0 | 1 | 3 |
| Y | 1 | 0 | 2 |
| Z | 3 | 2 | 0 |

| | X | Y | Z |
|---|---|---|---|
| X | | | |
| Y | | | |
| Z | 5 | 2 | 0 |

Finally the routing table for all –




**Advantages of Distance Vector routing –**

- It is simpler to configure and maintain than link state routing.

**Disadvantages of Distance Vector routing –**

- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.
- It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.
- For larger networks, distance vector routing results in larger routing tables than link state since each router must know about all other routers. This can also lead to congestion on WAN links.

**Hierarchical Routing Algorithm**

Hierarchical Routing is the method of routing in networks that is based on hierarchical addressing.

- Routing is based on two level of hierarchical routing in which IP address is divided into a network, person and a host person.

- Gateways use only the network a person tell an IP data until gateways delivered it directly.
- It addresses the growth of routing tables. Routers are further divided into regions and they know the route of their own regions only. It works like a telephone routing.
- Example –
  City, State, Country, Continent.
- This is essentially a 'Divide and Conquer' strategy. The network is divided into different regions and a router for a particular region knows only about its own domain and other routers.

Thus, the network is viewed at two levels:

- The Sub-network level, where each node in a region has information about its peers in the same region and about the region's interface with other regions. Different regions may have different 'local' routing algorithms. Each local algorithm handles the traffic between nodes of the same region and also directs the outgoing packets to the appropriate interface.
- The Network Level, where each region is considered as a single node connected to its interface nodes. The routing algorithms at this level handle the routing of packets between two interface nodes, and is isolated from intra-regional transfer.

In Hierarchical routing, the interfaces need to store information about:

- All nodes in its region which are at one level below it.
- Its peer interfaces.
- At least one interface at a level above it, for outgoing packages.

**Advantages of Hierarchical Routing :**

- Substantially lesser calculations and updates of routing tables.

**Disadvantage :**

- Once the hierarchy is imposed on the network, it is followed and possibility of direct paths is ignored. This may lead to sub optimal routing.

**RIP Protocol**

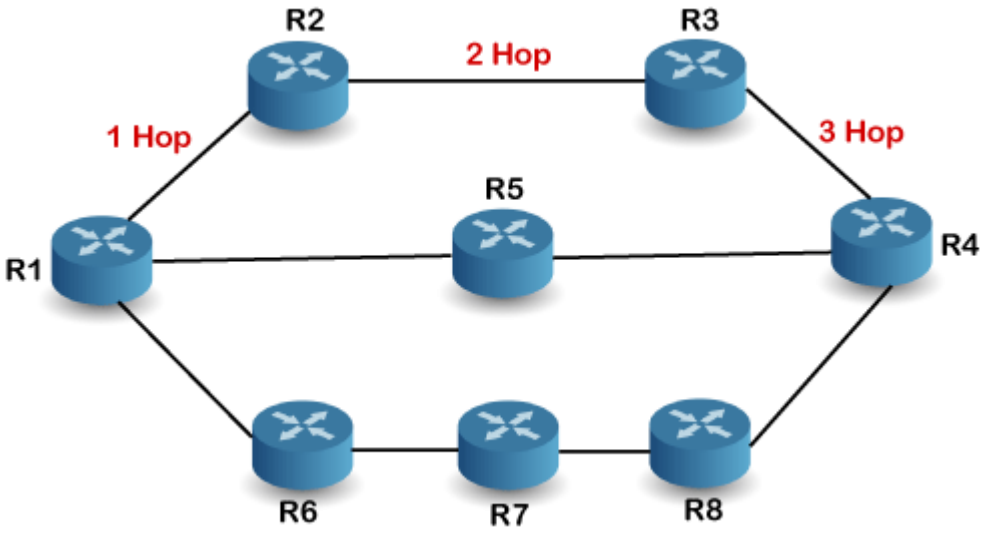
RIP stands for Routing Information Protocol. RIP is an intra-domain routing protocol used within an autonomous system. Here, intra-domain means routing the packets in a defined domain, for example, web browsing within an institutional area. To understand the RIP protocol, our main focus is to know the structure of the packet, how many fields it contains, and how these fields determine the routing table.

**Before understanding the structure of the packet, we first look at the following points:**

- RIP is based on the distance vector-based strategy, so we consider the entire structure as a graph where nodes are the routers, and the links are the networks.
- In a routing table, the first column is the destination, or we can say that it is a network address.
- The cost metric is the number of hops to reach the destination. The number of hops available in a network would be the cost. The hop count is the number of networks required to reach the destination.
- In RIP, infinity is defined as 16, which means that the RIP is useful for smaller networks or small autonomous systems. The maximum number of hops that RIP can contain is 15 hops, i.e., it should not have more than 15 hops as 16 is infinity.
- The next column contains the address of the router to which the packet is to be sent to reach the destination.

**How is hop count determined?**

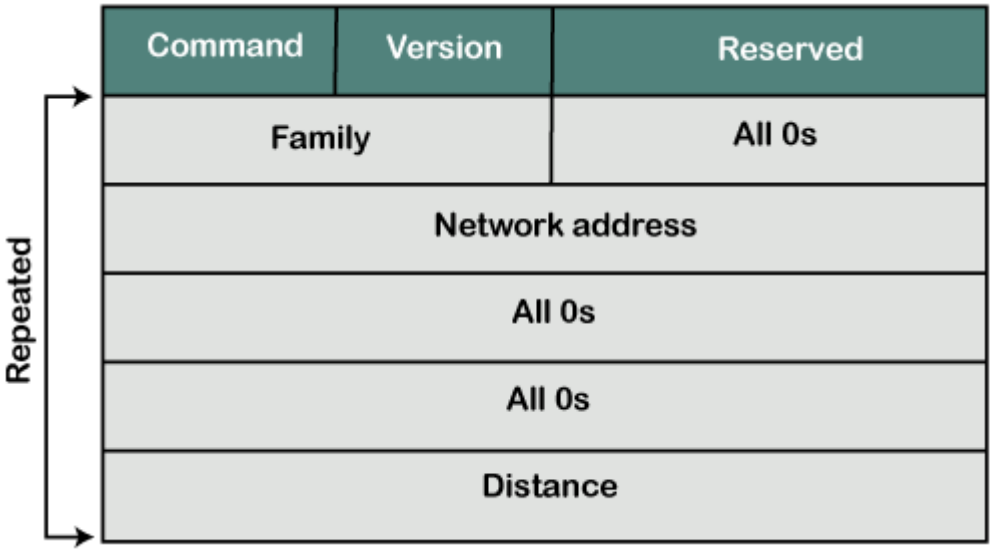
When the router sends the packet to the network segment, then it is counted as a single hop.




In the above figure, when the router 1 forwards the packet to the router 2 then it will count as 1 hop count. Similarly, when the router 2 forwards the packet to the router 3 then it will count as 2 hop count, and when the router 3 forwards the packet to router 4, it will count as 3 hop count. In the same way, RIP can support maximum upto 15 hops, which means that the 16 routers can be configured in a RIP.

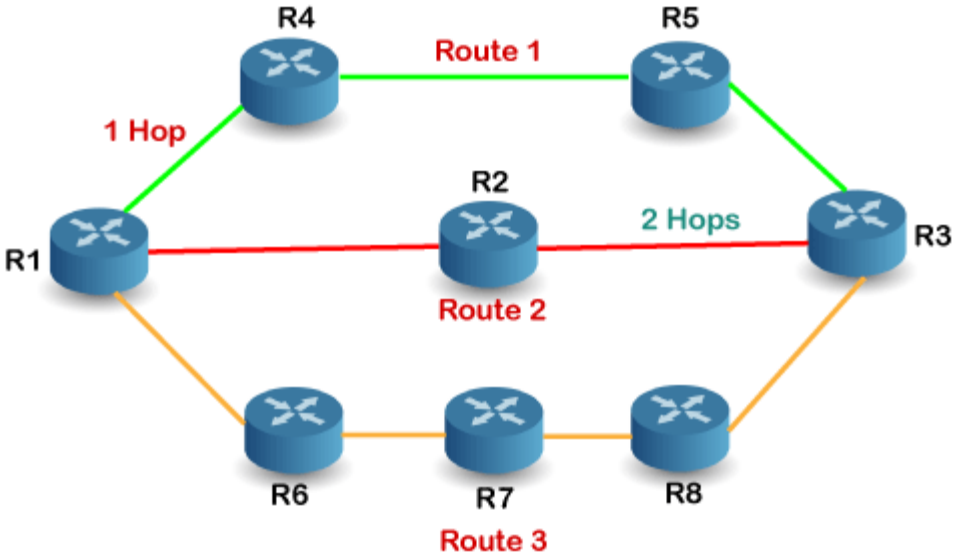
**RIP Message Format**

Now, we look at the structure of the RIP message format. The message format is used to share information among different routers. The RIP contains the following fields in a message:



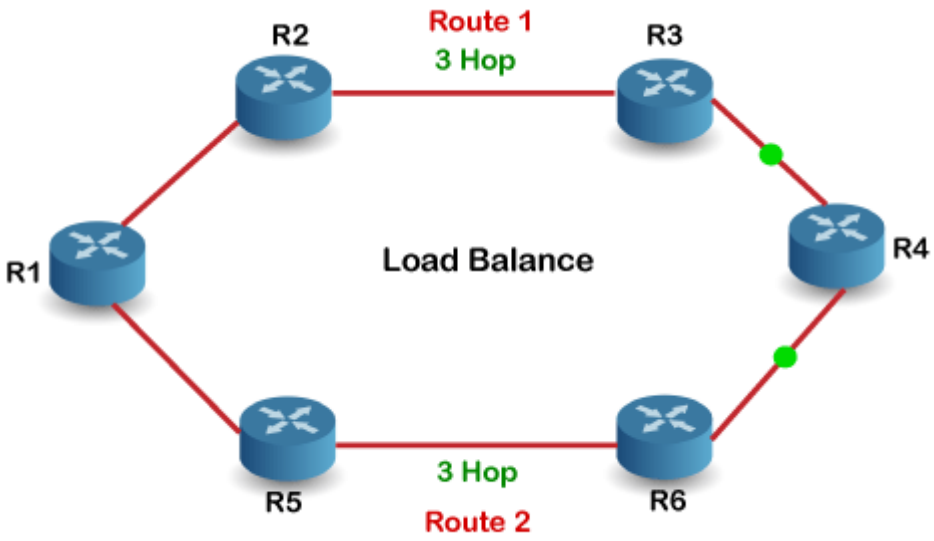

- Command: It is an 8-bit field that is used for request or reply. The value of the request is 1, and the value of the reply is 2.
- Version: Here, version means that which version of the protocol we are using. Suppose we are using the protocol of version1, then we put the 1 in this field.
- Reserved: This is a reserved field, so it is filled with zeroes.
- Family: It is a 16-bit field. As we are using the TCP/IP family, so we put 2 value in this field.
- Network Address: It is defined as 14 bytes field. If we use the IPv4 version, then we use 4 bytes, and the other 10 bytes are all zeroes.
- Distance: The distance field specifies the hop count, i.e., the number of hops used to reach the destination.

How does the RIP work?



If there are 8 routers in a network where Router 1 wants to send the data to Router 3. If the network is configured with RIP, it will choose the route which has the least number of hops. There are three routes in the above network, i.e., Route 1, Route 2, and Route 3. The Route 2 contains the least number of hops, i.e., 2 where Route 1 contains 3 hops, and Route 3 contains 4 hops, so RIP will choose Route 2.

Let's look at another example.

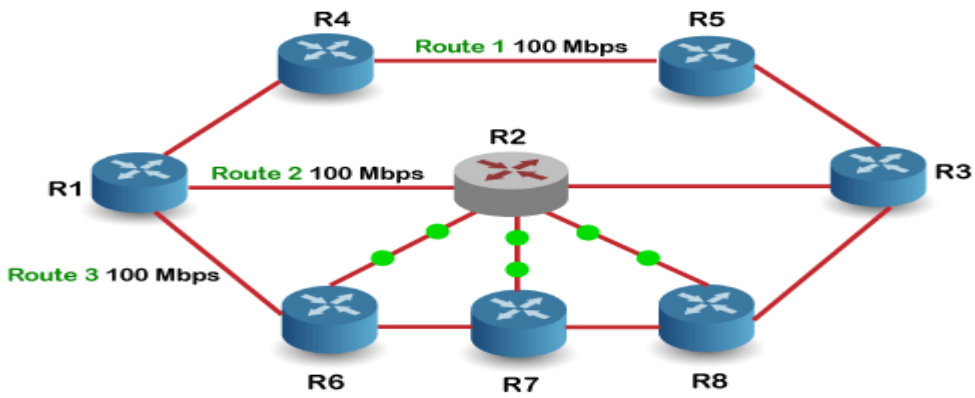



Suppose R1 wants to send the data to R4. There are two possible routes to send data from r1 to r2. As both the routes contain the same number of hops, i.e., 3, so RIP will send the data to both the routes simultaneously. This way, it manages the load balancing, and data reach the destination a bit faster.

Disadvantages of RIP

**The following are the disadvantages of RIP:**

- In RIP, the route is chosen based on the hop count metric. If another route of better bandwidth is available, then that route would not be chosen. Let's understand this scenario through an example.



We can observe that Route 2 is chosen in the above figure as it has the least hop count. The Route 1 is free and data can be reached more faster; instead of this, data is sent to the Route 2 that makes the Route 2 slower due to the heavy traffic. This is one of the biggest disadvantages of RIP.

- The RIP is a classful routing protocol, so it does not support the VLSM (Variable Length Subnet Mask). The classful routing protocol is a protocol that does not include the subnet mask information in the routing updates.
- It broadcasts the routing updates to the entire network that creates a lot of traffic. In RIP, the routing table updates every 30 seconds. Whenever the updates occur, it sends the copy of the update to all the neighbors except the one that has caused the update. The sending of updates to all the neighbors creates a lot of traffic. This rule is known as a split-horizon rule.
- It faces a problem of Slow convergence. Whenever the router or link fails, then it often takes minutes to stabilize or take an alternative route; This problem is known as Slow convergence.
- RIP supports maximum 15 hops which means that the maximum 16 hops can be configured in a RIP
- The Administrative distance value is 120 (Ad value). If the Ad value is less, then the protocol is more reliable than the protocol with more Ad value.
- The RIP protocol has the highest Ad value, so it is not as reliable as the other routing protocols.

How RIP updates its Routing table

The following timers are used to update the routing table:

- **RIP update timer : 30 sec**

The routers configured with RIP send their updates to all the neighboring routers every 30 seconds.

- **RIP Invalid timer : 180 sec**

The RIP invalid timer is 180 seconds, which means that if the router is disconnected from the network or some link goes down, then the neighbor router will wait for 180 seconds to take the update. If it does not receive the update within 180 seconds, then it will mark the particular route as not reachable.

- **RIP Flush timer : 240 sec**

The RIP flush timer is 240 second which is almost equal to 4 min means that if the router does not receive the update within 240 seconds then the neighbor route will remove that particular route from the routing table which is a very slow process as 4 minutes is a long time to wait.

Advantages of RIP

**The following are the advantages of a RIP protocol:**

- It is easy to configure
- It has less complexity
- The CPU utilization is less.

**OSPF- Open Shortest Path First**

Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).

**OSPF terms –**

1. **Router I'd –** It is the highest active IP address present on the router. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.
2. **Router priority –** It is a 8 bit value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.
3. **Designated Router (DR) –** It is elected to minimize the number of adjacency formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other routers shares their DBD. In a broadcast network, router requests for an update to DR and DR will respond to that request with an update.
4. **Backup Designated Router (BDR) –** BDR is backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.

**DR and BDR election –** DR and BDR election takes place in broadcast network or multi-access network. Here are the criteria for the election:

1. Router having the highest router priority will be declared as DR.
2. If there is a tie in router priority then highest router I'd will be considered. First, the highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.

**OSPF states –** The device operating OSPF goes through certain states. These states are:

1. **Down –** In this state, no hello packet have been received on the interface.
   **Note –** The Down state doesn't mean that the interface is physically down. Here, it means that OSPF adjacency process has not started yet.
2. **INIT –** In this state, hello packet have been received from the other router.
3. **2WAY –** In the 2WAY state, both the routers have received the hello packets from other routers. Bidirectional connectivity has been established.
   **Note –** In between the 2WAY state and Exstart state, the DR and BDR election takes place.
4. **Exstart –** In this state, NULL DBD are exchanged.In this state, master and slave election take place. The router having the higher router I'd becomes the master while

other becomes the slave. This election decides Which router will send it's DBD first (routers who have formed neighbourship will take part in this election).

5. **Exchange –** In this state, the actual DBDs are exchanged.
6. **Loading –** In this sate, LSR, LSU and LSA (Link State Acknowledgement) are exchanged.
   **Important –** When a router receives DBD from other router, it compares it's own DBD with the other router DBD. If the received DBD is more updated than its own DBD then the router will send LSR to the other router stating what links are needed. The other router replies with the LSU containing the updates that are needed. In return to this, the router replies with the Link State Acknowledgement.
7. **Full –** In this state, synchronization of all the information takes place. OSPF routing can begin only after the Full state.

**Border Gateway Protocol (BGP)**

It is used to Exchange routing information for the internet and is the protocol used between ISP which are different ASes.
The protocol can connect together any internetwork of autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run BGP and that is router connect to at least one other AS's BGP router. BGP's main function is to exchange network reach-ability information with other BGP systems. Border Gateway Protocol constructs an autonomous systems' graph based on the information exchanged between BGP routers.

**Characteristics of Border Gateway Protocol (BGP):**

- **Inter-Autonomous System Configuration:** The main role of BGP is to provide communication between two autonomous systems.
- BGP supports Next-Hop Paradigm.
- Coordination among multiple BGP speakers within the AS (Autonomous System).
- **Path Information:** BGP advertisement also include path information, along with the reachable destination and next destination pair.
- **Policy Support:** BGP can implement policies that can be configured by the administrator. For ex:- a router running BGP can be configured to distinguish between the routes that are known within the AS and that which are known from outside the AS.
- Runs Over TCP.
- BGP conserve network Bandwidth.
- BGP supports CIDR.
- BGP also supports Security.

**Functionality of Border Gateway Protocol (BGP):**
BGP peers performs 3 functions, which are given below.

1. The first function consist of initial peer acquisition and authentication. both the peers established a TCP connection and perform message exchange that guarantees both sides have agreed to communicate.
2. The second function mainly focus on sending of negative or positive reach-ability information.
3. The third function verifies that the peers and the network connection between them are functioning correctly.

**BGP Route Information Management Functions:**

- **Route Storage:**
  Each BGP stores information about how to reach other networks.

- **Route Update:**
  In this task, Special techniques are used to determine when and how to use the information received from peers to properly update the routes.
- **Route Selection:**
  Each BGP uses the information in its route databases to select good routes to each network on the internet network.
- **Route advertisement:**
  Each BGP speaker regularly tells its peer what is knows about various networks and methods to reach them.

**Broadcasting and Multicasting**

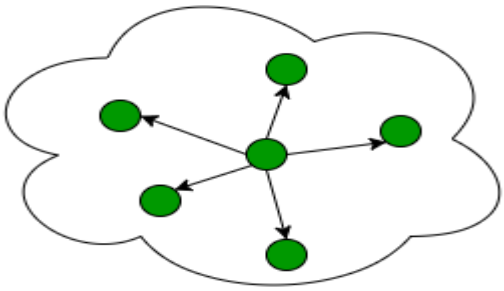
- The cast term here signifies some data(stream of packets) is being transmitted to the recipient(s) from client(s) side over the communication channel that helps them to communicate.

**BROADCASTING**

- Broadcasting in computer network is a group communication, where a sender sends data to receivers simultaneo
- Broadcasting transfer techniques can be classified into two types :
- Limited Broadcasting
- Direct Broadcasting

**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 transfer to all the recipients from a single client (sender) over the network**.**

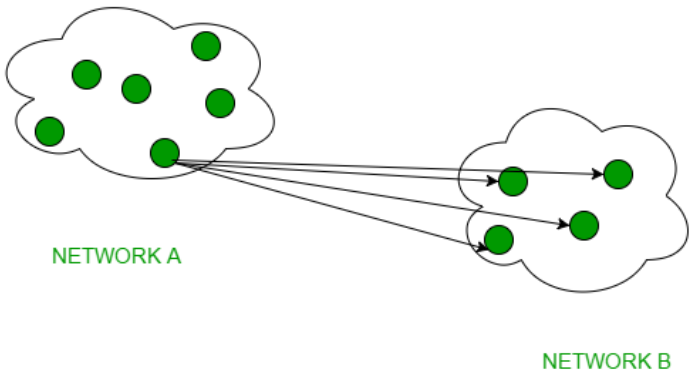


NETWORK CLUSTER

**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.**




**Advantages of Broadcasting**

- Broadcast helps to attain economies of scale when a common data stream needs to be delivered to all, by minimizing the communication and processing overhead. It ensures better utilization of resources and faster delivery in comparison to several unicast communication.

**Disadvantages of Broadcasting**

- Broadcasting cannot accommodate a very large amount of devices. Also it does not allow personalisation of the messages according to the individual preferences of the devices.

**MULTICASTING**

- 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.

**DVMRP- Distance Vector Multicast Routing Protocol**

The distance vector multicast routing protocol is multicast routing protocol that takes the routing decision based upon the source address of the packet.

This algorithm constructs the routing tree for a network.

• Whenever a router receives a packet, it forwards it to some of its ports based on the source address of packet.

• The rest of the routing tree is made by downstream routers.

• In this way, routing tree is created from destination to source.

• The protocol must achieve the following tasks:

1. It must prevent the formation of loops in the network.

2. It must prevent the formation of duplicate packets.

3. It must ensure that the path travelled by a packet is the shortest from its source to the router.

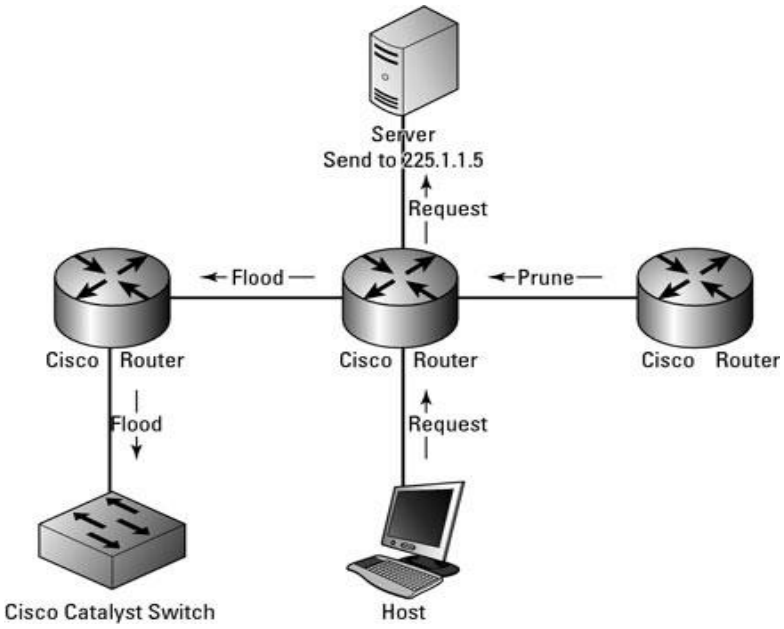
4. It should provide dynamic membership.

- The first multicast routing method for the Internet was the Distance Vector Multicast Routing Protocol (DVMRP) by Steve Deering in 1993.
- DVMRP is based on Reverse Path BroadcastingThe Reverse Path Broadcasting constructs a broadcast tree for every node in the network
- We obviously do NOT want to send to ALL nodes

**PIM- Protocol-Independent Multicast**

- Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet.
- It is termed *protocol-independent* because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols.
- PIM is not dependent on a specific unicast routing protocol; it can make use of any unicast routing protocol in use on the network. PIM does not build its own routing tables. PIM uses the unicast routing table for reverse path forwarding.

- There are four variants of PIM:
- PIM Sparse Mode (PIM-SM) explicitly builds unidirectional shared trees rooted at a *rendezvous point* (RP) per group, and optionally creates shortest-path trees per source. PIM-SM generally scales fairly well for wide-area usage.
- PIM Dense Mode (PIM-DM) uses dense multicast routing. It implicitly builds shortest-path trees by flooding multicast traffic domain wide, and then pruning back branches of the tree where no receivers are present. PIM-DM is straightforward to implement but generally has poor scaling properties. The first multicast routing protocol, DVMRP used dense-mode multicast routing.
- Bidirectional PIM (Bidir-PIM) explicitly builds shared bi-directional trees. It never builds a shortest path tree, so may have longer end-to-end delays than PIM-SM, but scales well because it needs no source-specific state.
- PIM Source-Specific Multicast (PIM-SSM) builds trees that are rooted in just one source, offering a more secure and scalable model for a limited number of applications (mostly broadcasting of content). In SSM, an IP datagram is transmitted by a source S to an SSM destination address G, and receivers can receive this datagram by subscribing to channel (S,G).
- Dense and Sparse modes are two important modes in PIM.



## UNIT IV TRANSPORT LAYER

Process to Process Communication, User Datagram Protocol (UDP), Transmission Control Protocol (TCP), SCTP Congestion Control; QoS Improving Techniques (Traffic Shaping, Admission Control And Resource Reservation).

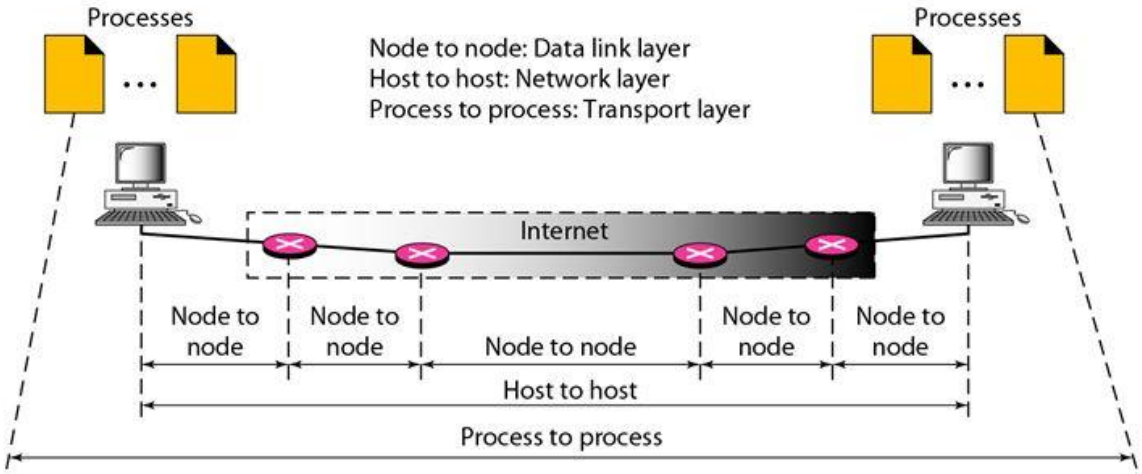
## PROCESS TO PROCESS COMMUNICATION

The Internet model has three protocols at the transport layer: UDP, TCP, and SCTP.

The data link layer is responsible for delivery of frames between two neighboring nodes over a link. This is called node-to-node delivery. The network layer is responsible for delivery of datagrams between two hosts. This is called host-to-host delivery. Communication on the Internet is not defined as the exchange of data between two nodes or between two hosts. Real communication takes place between two processes. So that we need process-to-process delivery.

However, at any moment, several processes may be running on the source host and several on the destination host. To complete the delivery, we need a mechanism to deliver data from one of these processes running on the source host to the corresponding process running on the destination host.

The transport layer is responsible for process-to-process delivery-the delivery of a packet, part of a message, from one process to another. The following figure shows these three types of deliveries and their domains.




### Client/Server Paradigm:

There are several ways to achieve process-to-process communication; the most common one is through the client/server paradigm. A process on the local host, called a client, needs services from a process usually on the remote host, called a server.

Both processes (client and server) have the same name. For example, to get the day and time from a remote machine, we need a Daytime client process running on the local host and a Daytime server process running on a remote machine.

A remote computer can run several server programs at the same time, just as local computers can run one or more client programs at the same time. For communication, we must define the following:

1. Local host
2. Local process
3. Remote host
4. Remote process

**Addressing**

Whenever we need to deliver something to one specific destination among many, we need an address.

At the data link layer, we need a MAC address to choose one node among several nodes if the connection is not point-to-point. A frame in the data link layer needs a destination MAC address for delivery and a source address for the next node's reply.

At the network layer, we need an IP address to choose one host among millions. A datagram in the network layer needs a destination IP address for delivery and a source IP address for the destination's reply.

At the transport layer, we need a transport layer address, called a port number, to choose among multiple processes running on the destination host. The destination port number is needed for delivery; the source port number is needed for the reply.

In the Internet model, the port numbers are 16-bit integers between 0 and 65,535. The client program defines itself with a port number, chosen randomly by the transport layer software running on the client host. This is the ephemeral port number.

The server process must also define itself with a port number. This port number, however, cannot be chosen randomly. If the computer at the server site runs a server process and assigns a random number as the port number, the process at the client site that wants to access that server and use its services will not know the port number.

Every client process knows the well-known port number of the corresponding server process. For example, while the Daytime client process, discussed above, can use an ephemeral (temporary) port number 52,000 to identify itself, the Daytime server process must use the well-known (permanent) port number 13.

It should be clear by now that the IP addresses and port numbers play different roles in selecting the final destination of data. The destination IP address defines the host among the different hosts in the world. After the host has been selected, the port number defines one of the processes on this particular host.

**IANA Ranges:**

The lANA (Internet Assigned Number Authority) has divided the port numbers into three ranges: well known, registered, and dynamic (or private).

• Well-known ports: The ports ranging from 0 to 1023 are assigned and controlled by lANA. These are the well-known ports.

• Registered ports: The ports ranging from 1024 to 49,151 are not assigned or controlled by lANA. They can only be registered with lANA to prevent duplication.

• Dynamic ports: The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used by any process. These are the ephemeral ports.

***Socket Addresses:***

Process-to-process delivery needs two identifiers, IP address and the port number, at each end to make a connection. The combination of an IP address and a port number is called a socket address. The client socket address defines the client process uniquely just as the server socket address defines the server process uniquely which is represented in the following figure.


**Multiplexing and Demultiplexing:**

The addressing mechanism allows multiplexing and demultiplexing by the transport layer.

**Multiplexing:**

At the sender site, there may be several processes that need to send packets. However, there is only one transport layer protocol at any time. This is a many-to-one relationship and requires multiplexing. The protocol accepts messages from different processes, differentiated by their assigned port numbers. After adding the header, the transport layer passes the packet to the network layer.

**Demultiplexing:**

At the receiver site, the relationship is one-to-many and requires demultiplexing. The transport layer receives datagrams from the network layer. After error checking and dropping of the header, the transport layer delivers each message to the appropriate process based on the port number.

**Connectionless Versus Connection-Oriented Service**

A transport layer protocol can either be connectionless or connection-oriented.

**Connectionless Service:**
In a connectionless service, the packets are sent from one party to another with no need for connection establishment or connection release. The packets are not numbered; they may be delayed or lost or may arrive out of sequence. There is no acknowledgment either. UDP, is connectionless.

**Connection-Oriented Service:**

In a connection-oriented service, a connection is first established between the sender and the receiver. Data are transferred. At the end, the connection is released. The TCP and SCTP are connection-oriented protocols.

**Reliable Versus Unreliable:**

The transport layer service can be reliable or unreliable. If the application layer program needs reliability, we use a reliable transport layer protocol by implementing flow and error control at the transport layer.

If the application program does not need reliability because it uses its own flow and error control mechanism or it needs fast service or the nature of the service does not demand flow and error control (real-time applications), then an unreliable protocol can be used. In the Internet, UDP is connectionless and unreliable; TCP and SCTP are connection oriented and reliable.

UDP- **User Datagram Protocol**

**User Datagram Protocol (UDP)** is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is **unreliable and connectionless protocol.** So, there is no need to establish connection prior to data transfer.

Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of Internet services; provides assured delivery, reliability and much more but all these services cost us with additional overhead and latency.

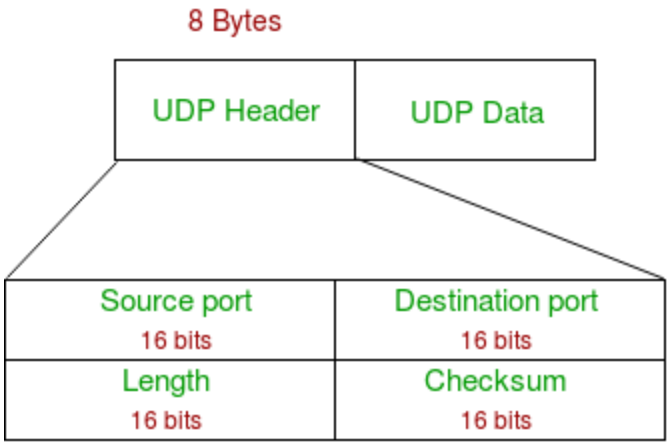
Here, UDP comes into picture. For the realtime services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets.

There is no error checking in UDP, so it also save bandwidth. User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

**UDP Header –**

UDP header is **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. First 8 Bytes contains all necessary header information and remaining part consist of data. UDP port number fields are each 16 bits long, therefore range for port numbers defined

from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or process.




1. **Source Port :** Source Port is 2 Byte long field used to identify port number of source.

2. **Destination Port :** It is 2 Byte long field, used to identify the port of destined packet.

3. **Length :** Length is the length of UDP including header and the data. It is 16-bits field.

4. **Checksum :** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

**Notes –** Unlike TCP, Checksum calculation is not mandatory in UDP. No Error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting.

**Applications of UDP:**

- Used for simple request response communication when size of data is less and hence there is lesser concern about flow and error control.
- It is suitable protocol for multicasting as UDP supports packet switching.
- UDP is used for some routing update protocols like RIP(Routing Information Protocol).
- Normally used for real time applications which can not tolerate uneven delays between sections of a received message.
- Following implementations uses UDP as a transport layer protocol:
  - NTP (Network Time Protocol)
  - DNS (Domain Name Service)
  - BOOTP, DHCP.
  - NNP (Network News Protocol)
  - Quote of the day protocol
  - TFTP, RTSP, RIP.

- Application layer can do some of the tasks through UDP-
  - Trace Route
  - Record Route
  - Time stamp
- UDP takes datagram from Network Layer, attach its header and send it to the user. So, it works fast.
- Actually UDP is null protocol if you remove checksum field.
  1. Reduce the requirement of computer resources.
  2. When using the Multicast or Broadcast to transfer.
  3. The transmission of Real-time packets, mainly in multimedia applications.

TCP

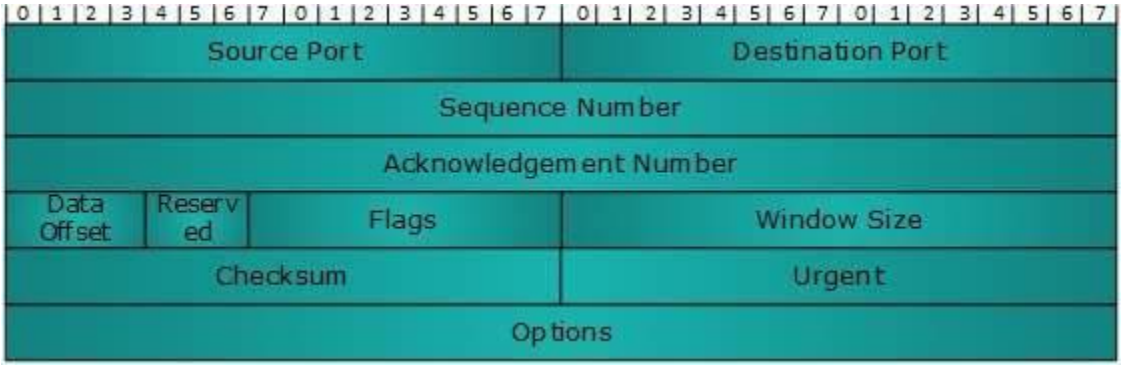
The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.

Features

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

Header

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.




- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**
    - **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
    - **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
    - **ECE** -It has two meanings:
        - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
        - If SYN bit is set to 1, ECE means that the device is ECT capable.
    - **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
    - **ACK** - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
    - **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
    - **RST** - Reset flag has the following features:
        - It is used to refuse an incoming connection.
        - It is used to reject a segment.

        - It is used to restart a connection.
    - **SYN** - This flag is used to set up a connection between hosts.
    - **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.
- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.
- **Options** - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

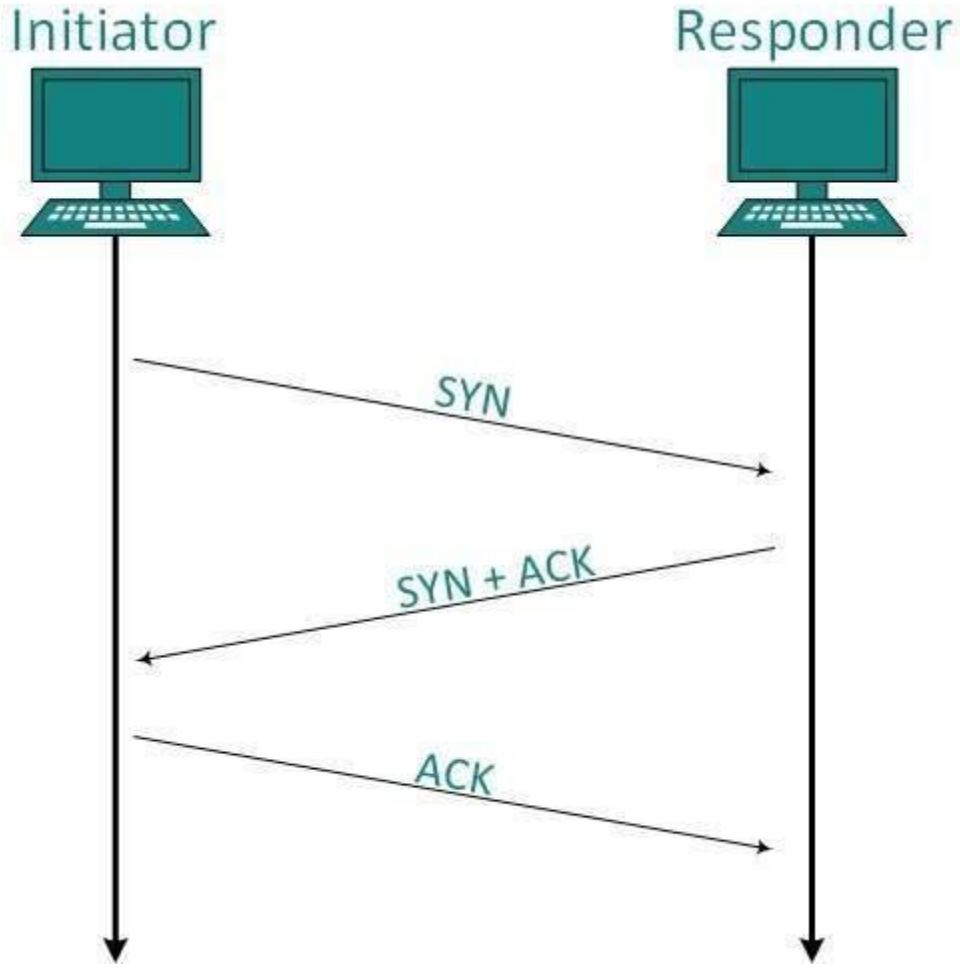
Addressing

TCP communication between two remote hosts is done by means of port numbers (TSAPs). Ports numbers can range from 0 – 65535 which are divided as:

- System Ports (0 – 1023)
- User Ports ( 1024 – 49151)
- Private/Dynamic Ports (49152 – 65535)

Connection Management

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.




## Establishment

Client initiates the connection and sends the segment with a Sequence number. Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number. Client after receiving ACK of its segment sends an acknowledgement of Server's response.

## Release

Either of server and client can send TCP segment with FIN flag set to 1. When the receiving end responds it back by ACKnowledging FIN, that direction of TCP communication is closed and connection is released.

## Bandwidth Management

TCP uses the concept of window size to accommodate the need of Bandwidth management. Window size tells the sender at the remote end, the number of data byte segments the receiver at this end can receive. TCP uses slow start phase by using window size 1 and increases the window size exponentially after each successful communication.

For example, the client uses windows size 2 and sends 2 bytes of data. When the acknowledgement of this segment received the windows size is doubled to 4 and next sent the segment sent will be 4 data bytes long. When the acknowledgement of 4-byte data segment is received, the client sets windows size to 8 and so on.

If an acknowledgement is missed, i.e. data lost in transit network or it received NACK, then the window size is reduced to half and slow start phase starts again.

### Error Control &and Flow Control

TCP uses port numbers to know what application process it needs to handover the data segment. Along with that, it uses sequence numbers to synchronize itself with the remote host. All data segments are sent and received with sequence numbers. The Sender knows which last data segment was received by the Receiver when it gets ACK. The Receiver knows about the last segment sent by the Sender by referring to the sequence number of recently received packet.

If the sequence number of a segment recently received does not match with the sequence number the receiver was expecting, then it is discarded and NACK is sent back. If two segments arrive with the same sequence number, the TCP timestamp value is compared to make a decision.

### Multiplexing

The technique to combine two or more data streams in one session is called Multiplexing. When a TCP client initializes a connection with Server, it always refers to a well-defined port number which indicates the application process. The client itself uses a randomly generated port number from private port number pools.

Using TCP Multiplexing, a client can communicate with a number of different application process in a single session. For example, a client requests a web page which in turn contains different types of data (HTTP, SMTP, FTP etc.) the TCP session timeout is increased and the session is kept open for longer time so that the three-way handshake overhead can be avoided.

This enables the client system to receive multiple connection over single virtual connection. These virtual connections are not good for Servers if the timeout is too long.

### Congestion Control

When large amount of data is fed to system which is not capable of handling it, congestion occurs. TCP controls congestion by means of Window mechanism. TCP sets a window size telling the other end how much data segment to send. TCP may use three algorithms for congestion control:

- Additive increase, Multiplicative Decrease
- Slow Start
- Timeout React

### Timer Management

TCP uses different types of timer to control and management various tasks:

#### Keep-alive timer:

- This timer is used to check the integrity and validity of a connection.

- When keep-alive time expires, the host sends a probe to check if the connection still exists.

### Retransmission timer:

- This timer maintains stateful session of data sent.
- If the acknowledgement of sent data does not receive within the Retransmission time, the data segment is sent again.

### Persist timer:

- TCP session can be paused by either host by sending Window Size 0.
- To resume the session a host needs to send Window Size with some larger value.
- If this segment never reaches the other end, both ends may wait for each other for infinite time.
- When the Persist timer expires, the host re-sends its window size to let the other end know.
- Persist Timer helps avoid deadlocks in communication.

### Timed-Wait:

- After releasing a connection, either of the hosts waits for a Timed-Wait time to terminate the connection completely.
- This is in order to make sure that the other end has received the acknowledgement of its connection termination request.
- Timed-out can be a maximum of 240 seconds (4 minutes).

## Crash Recovery

TCP is very reliable protocol. It provides sequence number to each of byte sent in segment. It provides the feedback mechanism i.e. when a host receives a packet, it is bound to ACK that packet having the next sequence number expected (if it is not the last segment).

When a TCP Server crashes mid-way communication and re-starts its process it sends TPDU broadcast to all its hosts. The hosts can then send the last data segment which was never unacknowledged and carry onwards.

## SCTP

- It is a connection- oriented protocol in computer networks which provides a full-duplex association i.e., transmitting multiple streams of data between two end points at the same time that have established a connection in network. It is sometimes referred to as next generation TCP or TCPng, SCTP makes it easier to support telephonic conversation on Internet. A telephonic conversation requires transmitting

of voice along with other data at the same time on both ends, SCTP protocol makes it easier to establish reliable connection.

- SCTP is also intended to make it easier to establish connection over wireless network and managing transmission of multimedia data. SCTP is a standard protocol (RFC 2960) and is developed by Internet Engineering Task Force (IETF).

**Characteristics of SCTP**

- **Unicast with Multiple properties –** It is a point-to-point protocol which can use different paths to reach end host.
- **Reliable Transmission –** It uses SACK and checksums to detect damaged, corrupted, discarded, duplicate and reordered data. It is similar to TCP but SCTP is more efficient when it comes to reordering of data.
- **Message oriented –** Each message can be framed and we can keep order of datastream and tabs on structure. For this, In TCP, we need a different layer for abstraction.

**Multi-homing –**
It can establish multiple connection paths between two end points and does not need to rely on IP layer for resilience

**Advantages of SCTP**

- It is a full- duplex connection i.e. users can send and receive data simultaneously.
- It allows half- closed connections.
- The message's boundaries are maintained and application doesn't have to split messages.
- It has properties of both TCP and UDP protocol.
- It doesn't rely on IP layer for resilience of paths.

**Disadvantages of SCTP**

- One of key challenges is that it requires changes in transport stack on node.
- Applications need to be modified to use SCTP instead of TCP/UDP.
- Applications need to be modified to handle multiple simultaneous streams.

SCTP CONGESTION CONTROL

- Congestion control tries avoiding overload situations in network components like routers.

- Congestion in network components can lead to packet loss which is handled by the error control function of SCTP .
- The goal of congestion control is to avoid packet loss in the first place.

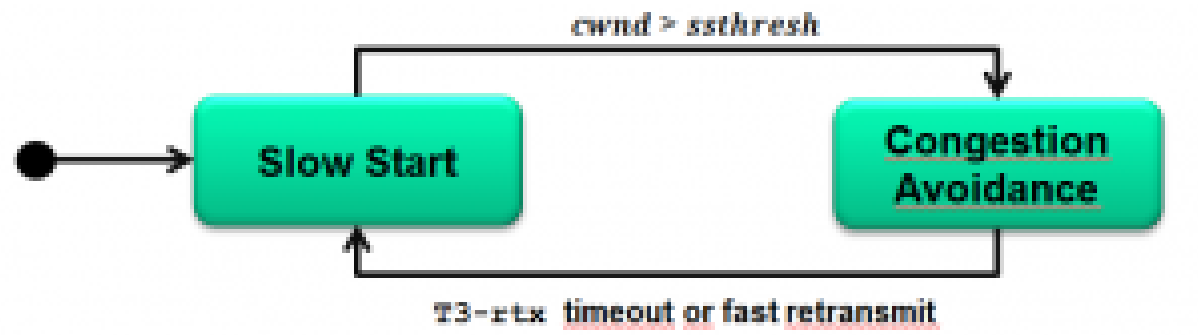
SCTP congestion control key facts

•SCTP congestion control is based on RFC2581 with some minor modifications.

•Congestion control is applied to the entire association, not individual streams.

•SCTP maintains a separate cwnd(Congestion Window) parameter for each peer destination address in multi-homed scenarios.

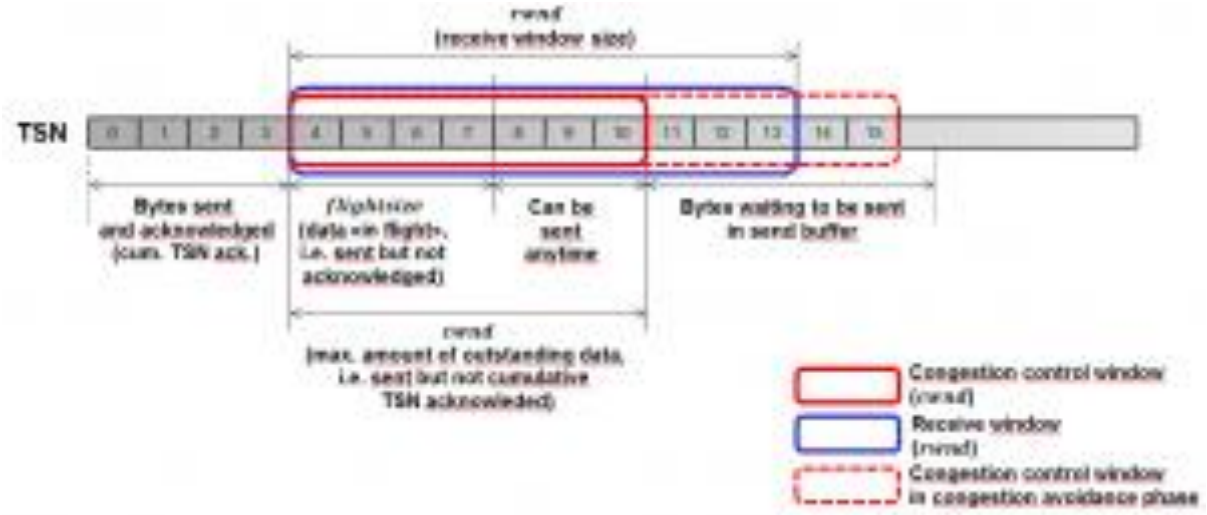
•As defined in RFC2581, the transmission rate starts slowly at the beginning (slow start phase), based on feedback provided by received SACK(Selective acknowledgement) chunks. After the slow start phase, SCTP enters the congestion avoidance phase. In case of congestion in the network, SCTP immediately reverts back to the slow start phase




SCTP congestion control window cwnd

- cwnd and rwnd (or a_rwnd = advertised receiver window size) define 2 windows where the smaller of the 2 determines the maximum amount of data that can be sent.
- After the slow start phase, cwnd is large so that rwnd becomes the dominant window size.

**Congestion control Window**




---

**Slow start and congestion avoidance phases**

- The general mechanism applied in SCTP congestion control (as per RFC2581) is to slowly increase the congestion window size cwnd, but to rapidly collapse the window when there are signs of congestion.
- Packet loss is deemed a sign of congestion. Note, however, that this is not always true (e.g. on wireless links there may be packet loss due to radio signal interferences).
- Congestion control is applied to the entire association, not individual streams. Nevertheless, cwnd is maintained per destination transport address (multihomed scenarios).

**Quality-of-Service (QoS)**

Quality-of-Service (QoS) refers to traffic control mechanisms that seek to either differentiate performance based on application or network-operator requirements or provide predictable or guaranteed performance to applications, sessions or traffic aggregates.

Basic phenomenon for QoS means in terms of packet delay and losses of various kinds.

NEED FOR QOS

- Video and audio conferencing require bounded delay and loss rate.
- Video and audio streaming requires bounded packet loss rate, it may not be so sensitive to delay.
- Time-critical applications (real-time control) in which bounded delay is considered to be an important factor.

- Valuable applications should be provided better services than less valuable applications.

## QOS SPECIFICATION

QoS requirements can be specified as:

- Delay
- Delay Variation(Jitter)
- Throughput
- Error Rate

## QOS SOLUTIONS

There are two types of QoS Solutions:

- **Stateless Solutions –**
  Routers maintain no fine grained state about traffic, one positive factor of it is that it is scalable and robust. But it has weak services as there is no guarantee about kind of delay or performance in a particular application which we have to encounter.

- **Stateful Solutions –**
  Routers maintain per flow state as flow is very important in providing the Quality-of-Service i.e. providing powerful services such as guaranteed services and high resource utilization, provides protection and is much less scalable and robust.

- QoS (Quality of Service) refers to a broad collection of networking technologies and techniques. The goal of QoS is to provide guarantees on the ability of a network to deliver predictable results.
- Elements of network performance within the scope of QoS often include availability (uptime), bandwidth (throughput), latency (delay), and error rate.

**Techniques to Improve QoS**

- Some techniques that can be used to improve the quality of service. The four common methods:
  i)Scheduling
  ii)Traffic shaping
  iii)Admission control
  iv) Resource reservation.

**a. Scheduling**

Packets from different flows arrive at a switch or router for processing. A good scheduling technique treats the different flows in a fair and appropriate manner. Several scheduling techniques are designed to improve the quality of service. We discuss three of them here: FIFO queuing, priority queuing, and weighted fair queuing.

### i. FIFO Queuing

In first-in, first-out (FIFO) queuing, packets wait in a buffer (queue) until the node (router or switch) is ready to process them. If the average arrival rate is higher than the average processing rate, the queue will fill up and new packets will be discarded. A FIFO queue is familiar to those who have had to wait for a bus at a bus stop.

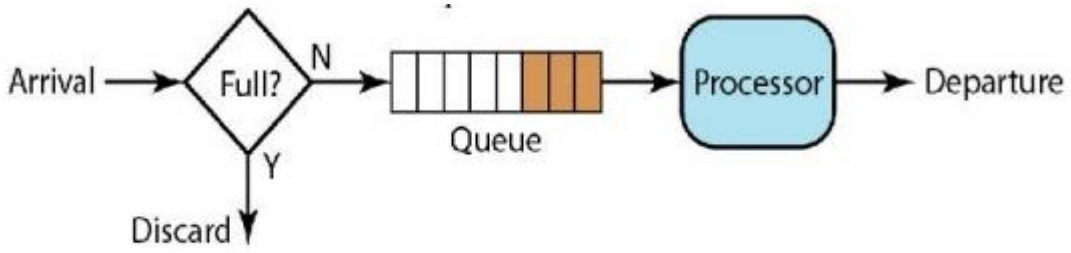



**Figure 4.31 FIFO queue**

### ii. Priority Queuing

In priority queuing, packets are first assigned to a priority class. Each priority class has its own queue. The packets in the highest-priority queue are processed first. Packets in the lowest- priority queue are processed last. Note that the system does not stop serving a queue until it is empty. Figure 4.32 shows priority queuing with two priority levels (for simplicity).

A priority queue can provide better QoS than the FIFO queue because higher priority traffic, such as multimedia, can reach the destination with less delay. However, there is a potential drawback. If there is a continuous flow in a high-priority queue, the packets in the lower-priority queues will never have a chance to be processed. This is a condition called starvation

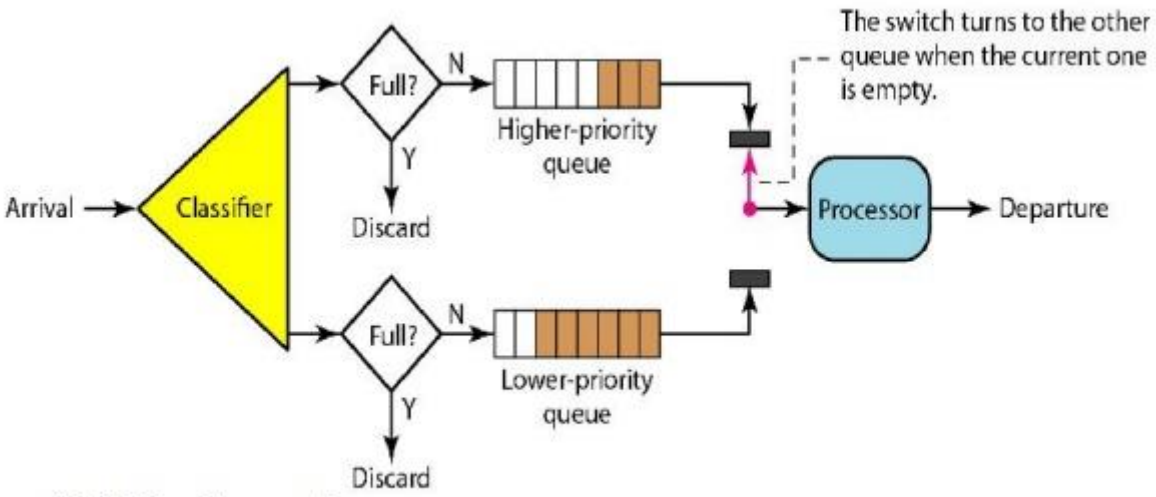



**Figure 4.32 Priority queuing**

### iii. Weighted Fair Queuing

A better scheduling method is weighted fair queuing. In this technique, the packets are still assigned to different classes and admitted to different queues. The queues, however, are weighted based on the priority of the queues; higher priority means a higher weight. The system processes packets in each queue in a round-robin fashion with the number of packets selected from each queue based on the corresponding weight. For example, if the weights are 3, 2, and 1, three packets are processed from the first queue, two from the second queue, and one from the third queue. If the system does not impose priority on the classes, all weights can be equal. In this way, we have fair queuing with priority. Figure 4.33 shows the technique with three classes.

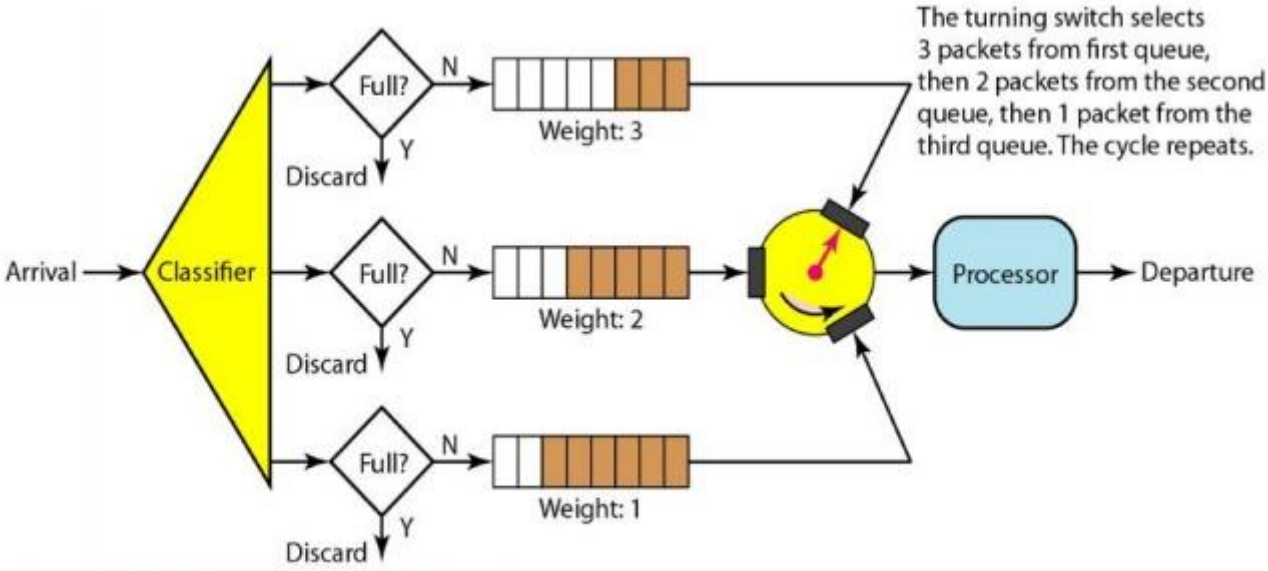



**Figure 4.33 Weighted Fair Queuing**

## b. Traffic Shaping

Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network. Two techniques can shape traffic: leaky bucket and token bucket

### i. Leaky Bucket

If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket. The rate at which the water leaks does not depend on the rate at which the water is input to the bucket unless the bucket is empty. The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate. Figure 4.34 shows a leaky bucket and its effects.

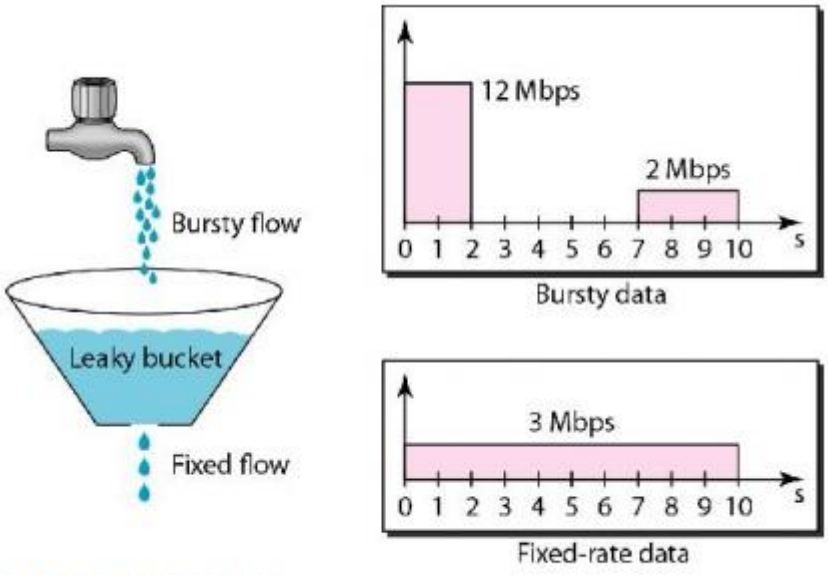



**Figure 4.34 Leaky Bucket**

In the figure, we assume that the network has committed a bandwidth of 3 Mbps for a host. The use of the leaky bucket shapes the input traffic to make it conform to this commitment. In Figure 4.34 the host sends a burst of data at a rate of 12 Mbps for 2 s, for a total of 24 Mbits of data. The host is silent for 5 s and then sends data at a rate of 2 Mbps for 3 s, for a total of 6 Mbits of data. In all, the host has sent 30 Mbits of data in lOs. The leaky bucket smooth's the traffic by sending out data at a rate of 3 Mbps during the same 10 s.

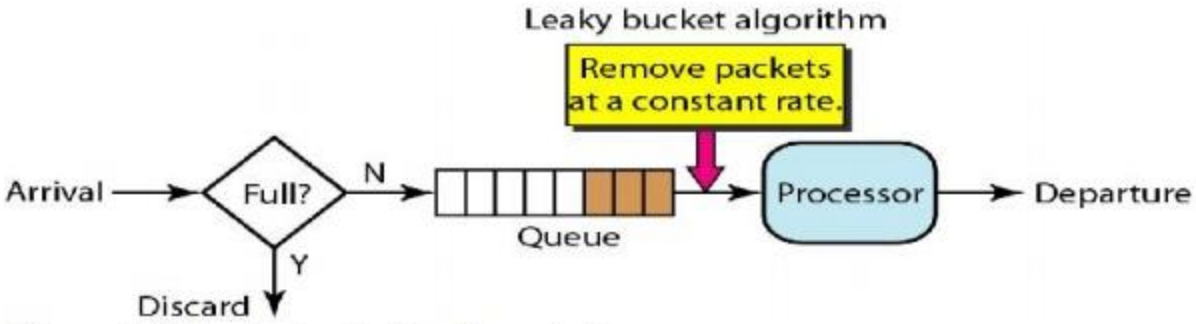



**Figure 4.35 Leaky bucket implementation**

A simple leaky bucket implementation is shown in Figure 4.35. A FIFO queue holds the packets. If the traffic consists of fixed-size packets (e.g., cells in ATM networks), the process removes a fixed number of packets from the queue at each tick of the clock. If the traffic consists of variable-length packets, the fixed output rate must be based on the number of bytes or bits.

The following is an algorithm for variable-length packets:

· Initialize a counter to n at the tick of the clock.

· If n is greater than the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.

· Reset the counter and go to step 1.

**A leaky bucket algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if the bucket is full.**

**ii. Token Bucket**

The leaky bucket is very restrictive. It does not credit an idle host. For example, if a host is not sending for a while, its bucket becomes empty. Now if the host has bursty data, the leaky bucket allows only an average rate. The time when the host was idle is not taken into account. On the other hand, the token bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens. For each tick of the clock, the system sends n tokens to the bucket. The system removes one token for every cell (or byte) of data sent. For example, if n is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens.

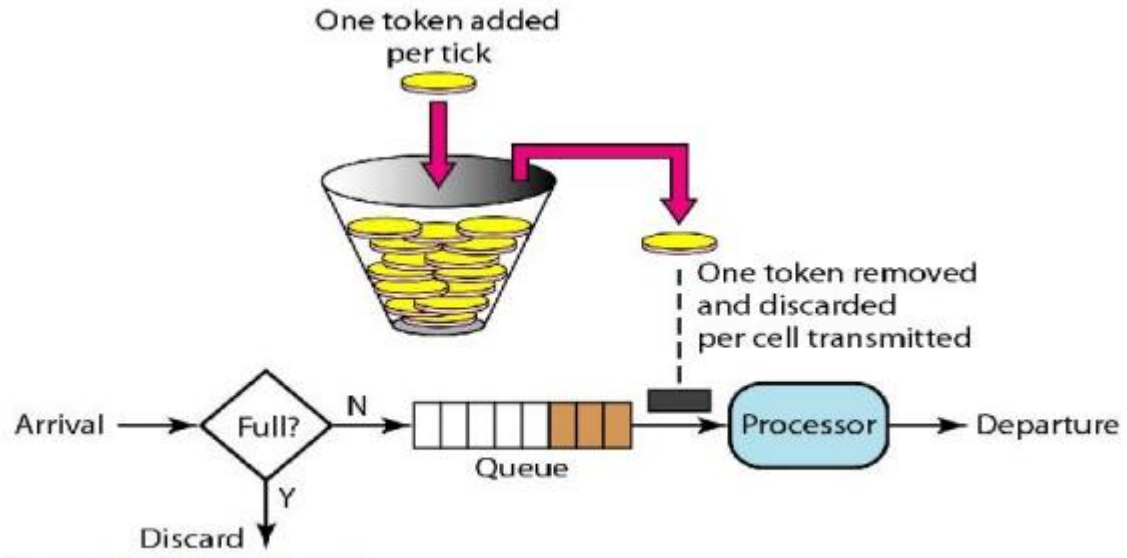



**Figure 4.36 Token bucket**

The token bucket can easily be implemented with a counter. The token is initialized to zero. Each time a token is added, the counter is incremented by 1. Each time a unit of data is sent, the counter is decremented by 1. When the counter is zero, the host cannot send data.

**The token bucket allows bursty traffic at a regulated maximum rate.**

***Combining Token Bucket and Leaky Bucket***

The two techniques can be combined to credit an idle host and at the same time regulate the traffic. The leaky bucket is applied after the token bucket; the rate of the leaky bucket needs to be higher than the rate of tokens dropped in the bucket.

**c. Resource Reservation**

A flow of data needs resources such as a buffer, bandwidth, CPU time, and so on. The quality of service is improved if these resources are reserved beforehand. We discuss in this section one QoS model called Integrated Services, which depends heavily on resource reservation to improve the quality of service.

- RSVP is a transport layer protocol that is used to reserve resources in a computer network to get different quality of services (QoS) while accessing Internet applications. It operates over Internet protocol (IP) and initiates resource reservations from the receiver's end.

**Features**

- RSVP is a receiver oriented signalling protocol. The receiver initiates and maintains resource reservation.
- It is used both for unicasting (sending data from one source to one destination) and multicasting (sending data simultaneously to a group of destination computers).
- RSVP supports dynamic automatic adaptation to changes in network.
- It provides a number of reservation styles. It also provides support for addition of future styles.

**RSVP Messages**

There are two types of RSVP messages −

- **Path Messages (path):** A path message is sent by the sender to all receivers by multicasting storing the path state at each node in its path. It stores the necessary information so that the receivers can make the reservation.
- **Reservation messages (resv):** The resv message is sent by the receiver to the sender along the reverse path of the path message. It identifies the resources that is requires by the data flow.

d. Admission Control

Admission control refers to the mechanism used by a router, or a switch, to accept or reject a flow based on predefined parameters called flow specifications. Before a router accepts a flow for processing, it checks the flow specifications to see if its capacity (in terms of bandwidth, buffer size, CPU speed, etc.) and its previous commitments to other flows can handle the new flow.

## UNIT V

## APPLICATION LAYER

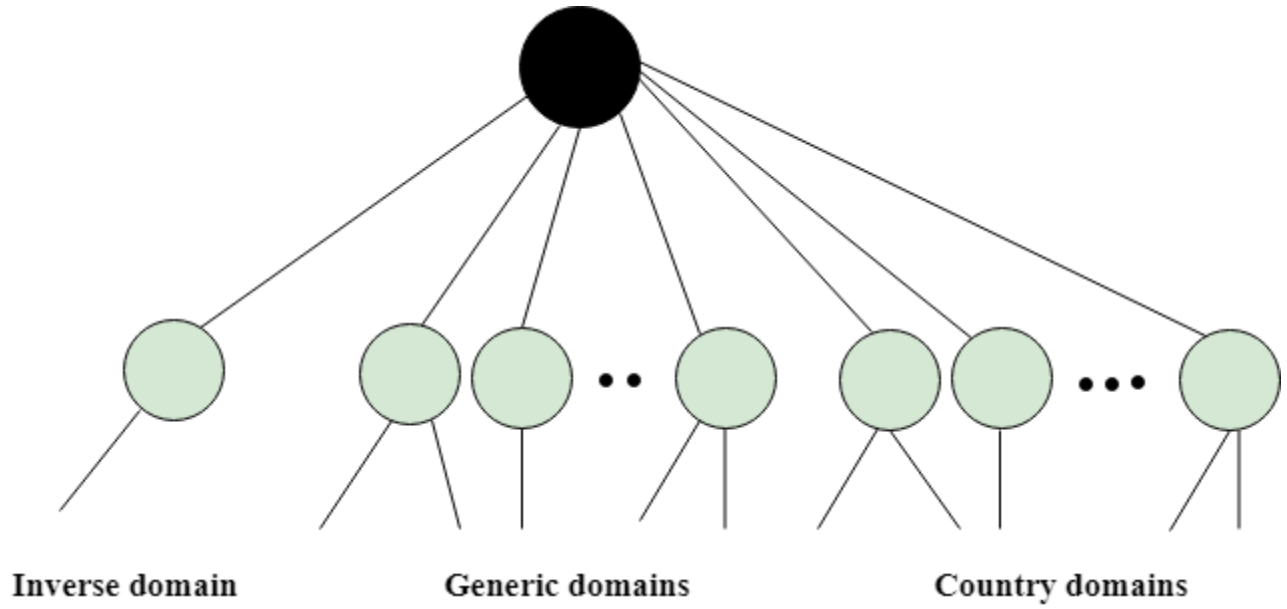
Domain Name Space (DNS), DDNS, TELNET, EMAIL, File Transfer Protocol (FTP), WWW, HTTP, SNMP, Bluetooth, Firewalls, Basic concepts of Cryptography.

### Domain Name Space (DNS)

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

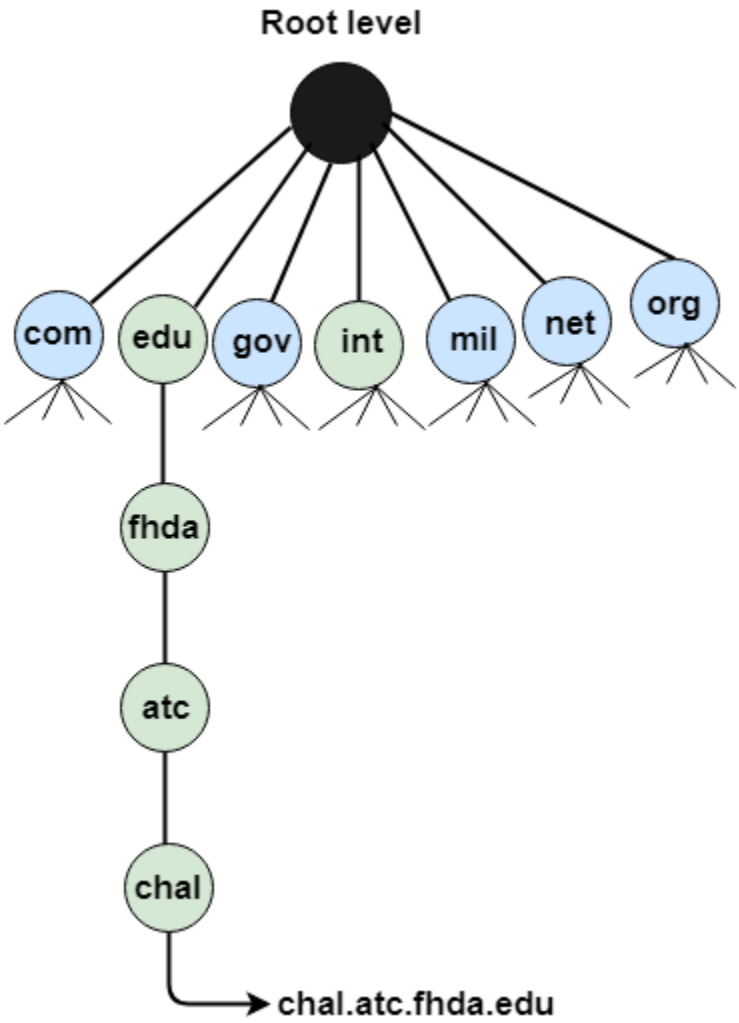
DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.




Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

| Label | Description |
|---|---|
| aero | Airlines and aerospace companies |
| biz | Businesses or firms |
| com | Commercial Organizations |
| coop | Cooperative business Organizations |
| edu | Educational institutions |
| gov | Government institutions |
| info | Information service providers |
| int | International Organizations |
| mil | Military groups |
| museum | Museum & other nonprofit organizations |
| name | Personal names |
| net | Network Support centers |
| org | Nonprofit Organizations |
| pro | Professional individual Organizations |




Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain

The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.

- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

**Dynamic Domain Name System (DDNS**

- When DNS (Domain Name System) was designed, nobody expected that there would be so many address changes such as adding a new host, removing a host, or changing an IP address. When there is a change, the change must be made to the DNS master file which needs a lot of manual updating and it must be updated dynamically.

**Dynamic Domain Name System (DDNS) :**

It is a method of automatically updating a name server in the Domain Name Server (DNS), often in real-time, with the active DDNS configuration of its configured hostnames, addresses, or other information. In DDNS, when a binding between a name and an address is determined, the information is sent, usually by DHCP (Dynamic Host Configuration Protocol) to a primary DNS server.

- The primary server updates the zone. The secondary servers are notified either actively or passively. Inactive notification, the primary server sends a message to secondary servers, whereas, in the passive notification, the secondary servers periodically check for any changes. In either case, after being notified about the change, the secondary requests information about the entire zone (zone transfer).
- DDNS can use an authentication mechanism to provide security and prevent unauthorized changes in DNS records.

**TELNET**

**TELNET** stands for **TE**rmina**L NET**work. It is a type of protocol that enables one computer to connect to local computer. It is a used as a standard **TCP/IP protocol** for virtual terminal service which is given by **ISO**. Computer which starts connection known as the **local computer**. Computer which is being connected to i.e. which accepts the connection known as **remote computer**. When the connection is established between local and remote computer. During telnet operation whatever that is performing on the remote computer will be displayed by local computer. Telnet operates on client/server principle. Local computer uses telnet client program and the remote computers uses telnet server program.

**TELNET Commands :**

Commands of the telnet are identified by a prefix character, Interpret As Command (IAC) which is having code 255. IAC is followed by command and option codes. Basic format of the command is as shown in the following figure :


**Figure –** Telnet command format

Following are some of the important **TELNET commands** :

| CHARACTER | DECIMAL | BINARY | MEANING |
|---|---|---|---|
| WILL | 251 | 11111011 | 1. Offering to enable.<br>2. Accepting a request to enable. |
| WON'T | 252 | 11111100 | 1. Rejecting a request to enable.<br>2. Offering to disable.<br>3. Accepting a request to disable. |
| DO | 253 | 11111101` | 1. Approving a request to enable.<br>2. Requesting to enable. |
| DON'T | 254 | 11111110 | 1. Disapproving a request to enable.<br>2. Approving an offer to disable.<br>3. Requesting to disable. |

Following are some **common options** used with the telnet :

| CODE | OPTION | MEANING |
|---|---|---|
| 0 | Binary | It interpret as 8-bit binary transmission. |
| 1 | Echo | It will echo the data that received on one side to the other side. |
| 3 | Suppress go ahead | It will suppress go ahead signal after data. |
| 5 | Status | It will request for the status of TELNET. |
| 6 | Timing mark | It define the timing marks. |
| 8 | Line width | It specifies the line width. |
| 9 | Page size | It specifies the number of lines in a page. |
| 24 | Terminal type | It set the terminal type. |
| 32 | Terminal speed | It set the terminal speed. |
| 34 | Line mode | It will change to the line mode. |

**Modes of Operation :**
Most telnet implementation operates in one of the following **three modes :**

Default mode

Character mode

Line mode

**Default Mode :**

- If there is no other modes are invoked then this mode is used.
- Echoing is performed in this mode by client.
- In this mode, user types a character and client enchoes the character on the screen but it does not send it until whole line is completed.

**Character Mode :**

- Each character typed in this mode is sent by client to server.
- Server in this type of mode is normally enchoes character back to be displayed on the client's screen.

**Line Mode :**

- Line editing like echoing, character erasing etc is done from the client side.
- Client will send the whole line to the server.

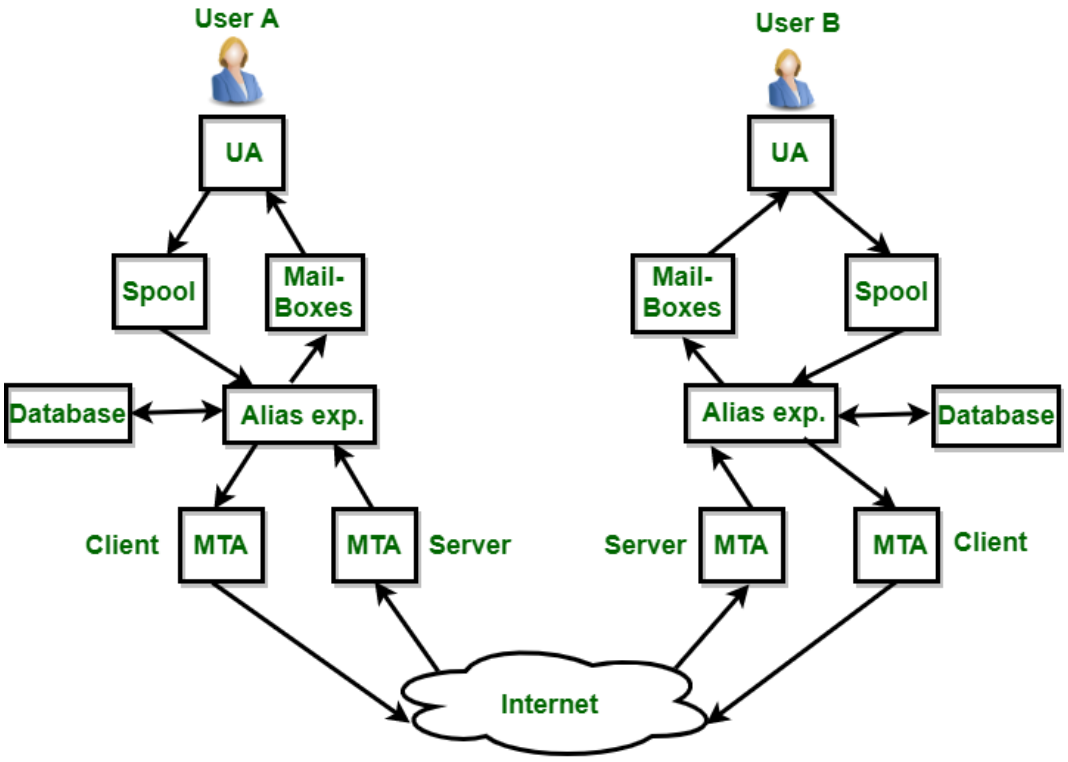
**EMAIL**

**Electronic Mail** (e-mail) is one of most widely used services of Internet. This service allows an Internet user to send a **message in formatted manner (mail)** to the other Internet user in any part of world. Message in mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called **sender** and person who receives mail is called **recipient**. It is just like postal mail service.

**Components of E-Mail System :**
The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

1. **User Agent (UA) :**
   The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.

2. **Message Transfer Agent (MTA) :**
   MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfer mail to mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done by Simple Mail Transfer Protocol.




3. **Mailbox :**
   It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox . Access to mailbox is only to owner of mailbox.

4. **Spool file :**
   This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an **alias**, to represent several different e-mail addresses. It is known as **mailing list**, Whenever user have to sent a message, system checks recipients's name against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

**Services provided by E-mail system :**

- **Composition –**
  The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.
- **Transfer –**
  Transfer means sending procedure of mail i.e. from the sender to recipient.
- **Reporting –**
  Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.
- **Displaying –**
  It refers to present mail in form that is understand by the user.

- **Disposition –**
  This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

**File Transfer Protocol (FTP)**

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

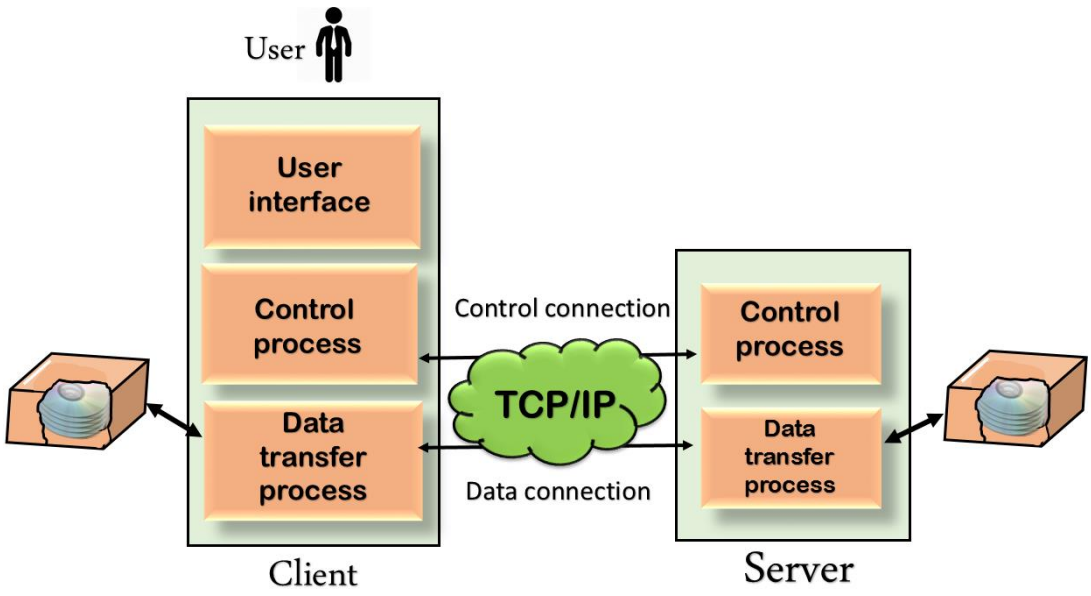
**Objectives of FTP**

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

**Why FTP?**

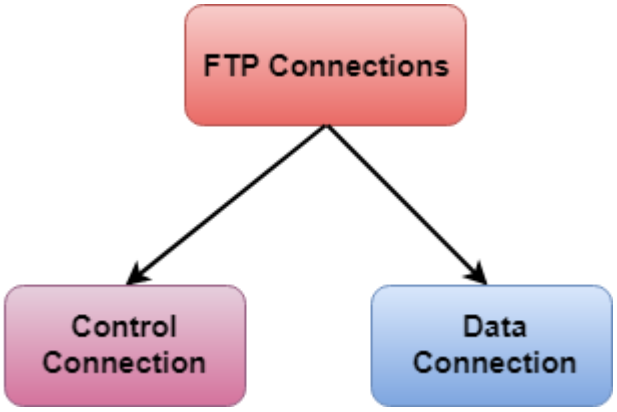
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

**Mechanism of FTP**



The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

**There are two types of connections in FTP:**




- **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

**FTP Clients**

- FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
- It allows a user to connect to a remote host and upload or download the files.
- It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
- The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

**Advantages of FTP:**

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.

- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

**Disadvantages of FTP:**

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

**WWW-WORLD WIDE WEB**

The **World Wide Web** abbreviated as WWW and commonly known as the web. The WWW was initiated by CERN (European library for Nuclear Research) in 1989.

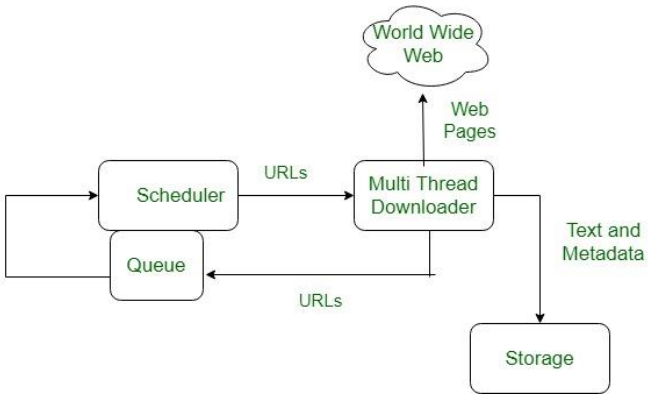
**History:**

It is a project created, by Timothy Berner's Lee in 1989, for researchers to work together effectively at CERN. is an organisation, named World Wide Web Consortium (W3C), was developed for further development in web. This organisation is directed by Tim Berner's Lee, aka father of web.

**System Architecture:**

From user's point of view, the web consists of a vast, worldwide connection of documents or web pages. Each page may contain links to other pages anywhere in the world. The pages can be retrieved and viewed by using browsers of which internet explorer, Netscape Navigator, Google, Chrome, etc are the popular ones. The browser fetches the page requested interprets the text and formatting commands on it, and displays the page, properly formatted, on the screen.

The basic model of how the web works is shown in figure below. Here the browser is displaying a web page on the client machine. When the user clicks on a line of text that is linked to a page on the abd.com server, the browser follows the hyperlink by sending a message to the abd.com server asking it for the page.




Here the browser displaying web page om the client machine when the user clicks on a line of text that is linked to a page on abd.com, the vbrowser follows the hyperlink by sending a message to abd.com server asking it for the page.

**Working of WWW:**
The World Wide Web is based on several different technologies : Web browsers, Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP).
An Web browser is used to access webpages. Web browsers can be defined as programs which display text, data, pictures, animation and video on the Internet. Hyperlinked resources on the World Wide Web can be accessed using software interface provided by Web browsers. Initially Web browsers were used only for surfing the Web but now they have become more universal. Web browsers can be used for several tasks including conducting searches, mailing, transferring files, and much more. Some of the commonly used browsers are Internet Explorer, Opera Mini, Google Chrome.

**Features of WWW:**
- HyperText Information System
- Cross-Platform
- Distributed
- Open Standards and Open Source
- Uses Web Browsers to provide a single interface for many services
- Dynamic, Interactive and Evolving.
- "Web 2.0"

**Components of Web**
There are 3 components of web:
1. **Uniform Resource Locator (URL):** serves as system for resources on web.
2. **HyperText Transfer Protocol (HTTP):** specifies communication of browser and server.
3. **Hyper Text Markup Language (HTML):** defines structure, organisation and content of webpage.

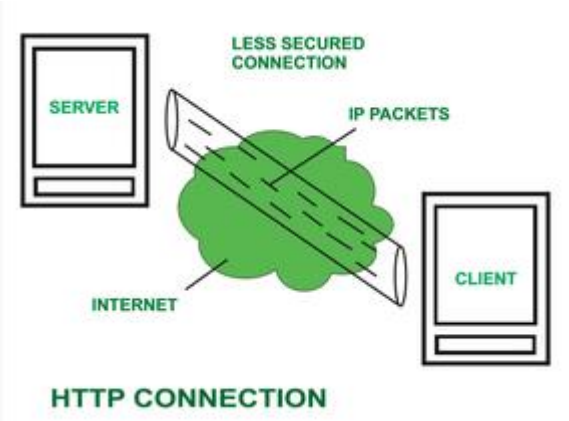
**HTTP- HyperText Transfer Protocol**

**HTTP** stands for HyperText Transfer Protocol. It is invented by **Tim Berner**. HyperText is the type of text which is specially coded with the help of some standard coding language called as HyperText Markup Language (HTML). **HTTP/2** is latest version of HTTP, which was published on May 2015.

The protocols that are used to transfer hypertext between two computers is known as HyperText Transfer Protocol.

HTTP provides standard between a web browser and web server to establish communication. It is set of rules for transferring data from one computer to another. Data such as text, images, and other multimedia files are shared on the World Wide Web. Whenever a web user opens their web browser, user will indirectly uses HTTP. It is an application protocol which is used for distributed, collaborative, hypermedia information systems.

**How it works ?**
First of all, whenever we want to open any website then first we open web browser after that we will type URL of that website (e.g., www.facebook.com ). This URL is now sent to Domain Name Server (DNS). Then DNS first check records for this URL in their database, then DNS will return IP address to web browser corresponding to this URL. Now browser is able to sent request to actual server.
After server sends data to client, connection will be closed. If we want something else from server we should have to re-establish connection between client and server.




**History ::**
Tim Berners Lee and his team at CERN gets credit for inventing original HTTP and associated technologies.

1. **HTTP version 0.9 –**
   This was first version of HTTP which was introduced in 1991.
2. **HTTP version 1.0 –**
   In 1996, RFC 1945 (Request For Comments) was introduced in HTTP version 1.0.
3. **HTTP version 1.1 –**
   In January 1997, RFC 2068 was introduced in HTTP version 1.1. Improvements and updates to HTTP version 1.1 standard were released under RFC 2616 in June 1999.

4. **HTTP version 2.0 –**
   The HTTP version 2.0 specification was published as RFC 7540 on May 14, 2015.
5. **HTTP version 3.0 –**
   HTTP version 3.0 is based on previous RFC draft. It is renamed as HyperText Transfer Protocol QUIC which is a transport layer network protocol developed by Google.

**Characteristics of HTTP :**
HTTP is IP based communication protocol which is used to deliver data from server to client or vice-versa.

1. Server processes a request, which is raised by client and also server and client knows each other only during current request and response period.
2. Any type of content can be exchanged as long as server and client are compatible with it.
3. Once data is exchanged then servers and client are no more connected with each other.
4. It is a request and response protocol based on client and server requirements.
5. It is connection less protocol because after connection is closed, server does not remember anything about client and client does not remember anything about server.
6. It is stateless protocol because both client and server does not expecting anything from each other but they are still able to communicate.

**Advantages :**

- Memory usage and CPU usage are low because of less simultaneous connections.
- Since there are few TCP connections hence network congestion are less.
- Since handshaking is done at initial connection stage, then latency is reduced because there is no further need of handshaking for subsequent requests.
- The error can be reports without closing connection.
- HTTP allows HTTP pipe-lining of request or response.

**Disadvantages :**

- HTTP requires high power to establish communication and transfer data.
- HTTP is less secure, because it does not uses any encryption method like https use TLS to encrypt normal http requests and response.
- HTTP is not optimized for cellular phone and it is too gabby.
- HTTP does not offer genuine exchange of data because it is less secure.
- Client does not close connection until it receives complete data from server and hence server needs to wait for data completion and cannot be available for other clients during this time.

**SNMP- Simple Network Management Protocol**

If an organization has 1000 of devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.

**Simple Network Management Protocol (SNMP) –**
SNMP is an application layer protocol which uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults and sometimes even used to configure remote devices.

**SNMP components –**
There are 3 components of SNMP:

1. **SNMP Manager –**
   It is a centralised system used to monitor network.It is also known as Network Management Station (NMS)
2. **SNMP agent –**
   It is a software management software module installed on a managed device. Managed devices can be network devices like PC, router, switches, servers etc.
3. **Management Information Base –**
   MIB consists of information of resources that are to be managed. These information is organised hierarchically. It consists of objects instances which are essentially variables.

**SNMP messages –**
Different variables are:

1. **GetRequest –** SNMP manager sends this message to request data from SNMP agent. It is simply used to retrieve data from SNMP agent. In response to this, SNMP agent responds with requested value through response message.
2. **GetNextRequest –** This message can be sent to discover what data is available on a SNMP agent. The SNMP manager can request for data continuously until no more data is left. In this way, SNMP manager can take knowledge of all the available data on SNMP agent.
3. **GetBulkRequest –** This message is used to retrieve large data at once by the SNMP manager from SNMP agent. It is introduced in SNMPv2c.
4. **SetRequest –** It is used by SNMP manager to set the value of an object instance on the SNMP agent.
5. **Response –** It is a message send from agent upon a request from manager. When sent in response to Get messages, it will contain the data requested. When sent in response to Set message, it will contain the newly set value as confirmation that the value has been set.
6. **Trap –** These are the message send by the agent without being requested by the manager. It is sent when a fault has occurred.
7. **InformRequest –** It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to set trap continuously until it receives an Inform message. It is same as trap but adds an acknowledgement that trap doesn't provide.

**SNMP security levels –**
It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are 3 security levels namely:

1. **noAuthNoPriv –**
   This (no authentication, no privacy) security level uses community string for authentication and no encryption for privacy.
2. **authNopriv –** This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.
3. **authPriv –** This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses DES-56 algorithm.

**SNMP versions –**
There are 3 versions of SNMP:

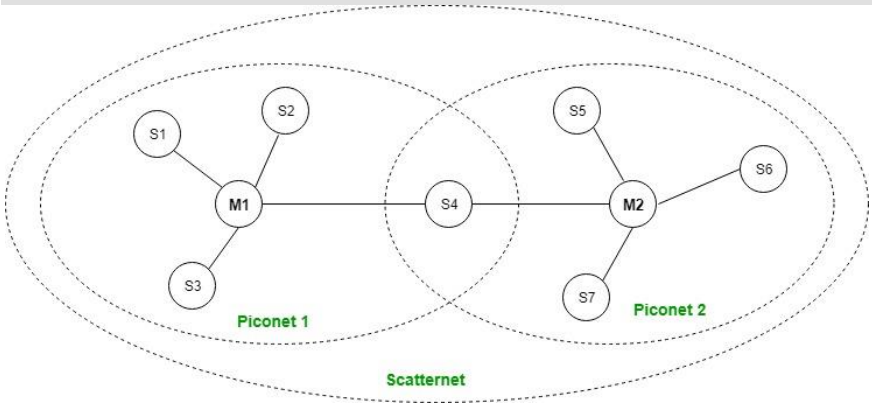
1. **SNMPv1 –** It uses community strings for authentication and use UDP only.
2. **SNMPv2c –** It uses community strings for authentication. It uses UDP but can be configured to use TCP.
3. **SNMPv3 –** It uses Hash based MAC with MD5 or SHA for authentication and DES-56 for privacy.This version uses TCP. Therefore, conclusion is the higher the version of SNMP, more secure it will be.

**Bluetooth**

It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz. Maximum devices that can be connected at the same time are 7. Bluetooth ranges upto 10 meters. It provides data rates upto 1 Mbps or 3 Mbps depending upon the version. The spreading technique which it uses is FHSS (Frequency hopping spread spectrum). A bluetooth network is called **piconet** and a collection of interconnected piconets is called **scatternet**.

**Bluetooth Architecture:**
The architecture of bluetooth defines two types of networks:

1. Piconet
2. Scatternet



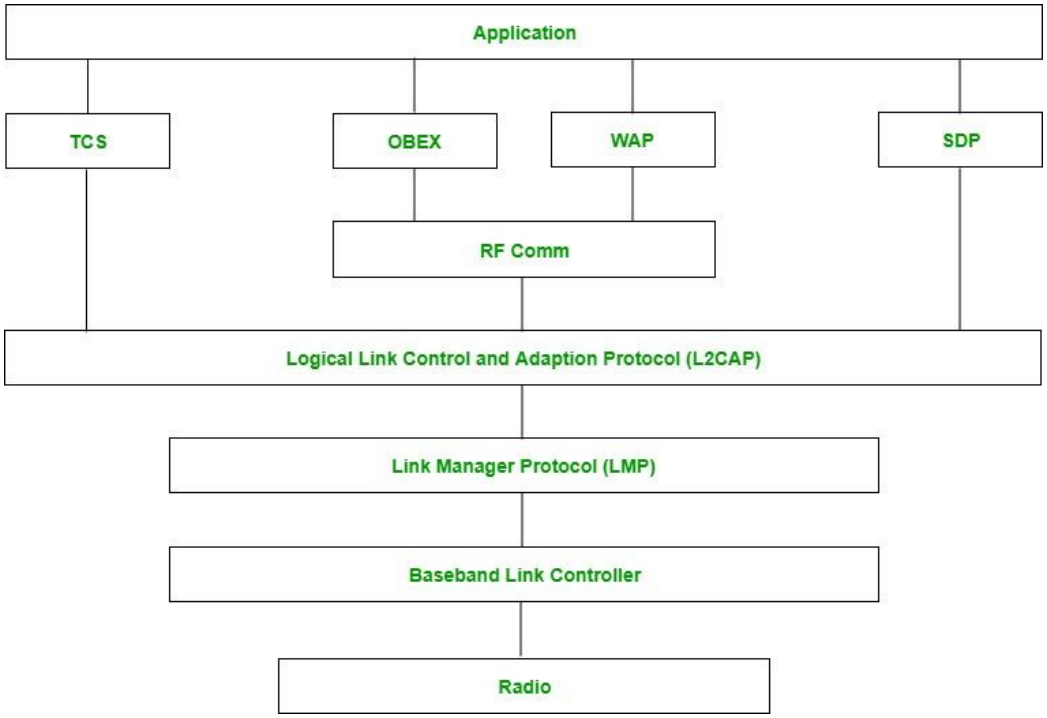

**Piconet:**

Piconet is a type of bluetooth network that contains **one primary node** called master node and **seven active secondary nodes** called slave nodes. Thus, we can say that there are total of 8 active nodes which are present at a distance of 10 metres. The communication between the primary and secondary node can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also have **255 parked nodes**, these are secondary nodes and cannot take participation in communication unless it get converted to the active state.

**Scatternet:**
It is formed by using **various piconets**. A slave that is present in one piconet can be act as master or we can say primary in other piconet. This kind of node can receive message from master in one piconet and deliver the message to its slave into the other piconet where it is

acting as a slave. This type of node is refer as bridge node. A station cannot be master in two piconets.

**Bluetooth protocol stack:**




1. **Radio (RF) layer:**
   It performs modulation/demodulation of the data into RF signals. It defines the physical characteristics of bluetooth transceiver. It defines two types of physical link: connection-less and connection-oriented.

2. **Baseband Link layer:**
   It performs the connection establishment within a piconet.

3. **Link Manager protocol layer:**
   It performs the management of the already established links. It also includes authentication and encryption processes.

4. **Logical Link Control and Adaption protocol layer:**
   It is also known as the heart of the bluetooth protocol stack. It allows the communication between upper and lower layers of the bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs the segmentation and multiplexing.

5. **SDP layer:**
   It is short for Service Discovery Protocol. It allows to discover the services available on another bluetooth enabled device.

6. **RF comm layer:**
   It is short for Radio Frontend Component. It provides serial interface with WAP and OBEX.

7. **OBEX:**
   It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices.

8. **WAP:**
   It is short for Wireless Access Protocol. It is used for internet access.

9. **TCS:**
   It is short for Telephony Control Protocol. It provides telephony service.

10. **Application layer:**
    It enables the user to interact with the application.

**Advantages:**

- Low cost.
- Easy to use.
- It can also penetrate through walls.
- It creates an adhoc connection immediately without any wires.
- It is used for voice and data transfer.

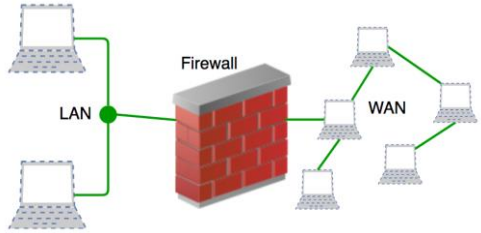
**Disadvantages:**

- It can be hacked and hence, less secure.
- It has slow data transfer rate: 3 Mbps.
- It has small range: 10 meters.

**Firewalls**

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

**Accept :** allow the traffic
**Reject :** block the traffic but reply with an "unreachable error"
**Drop :** block the traffic with no reply
A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.




**History and Need for Firewall**

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address.
But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.

Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

**How Firewall Works**

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.

From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

**Default policy:** It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop).
Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to *accept*, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as *drop* (or reject) is always a good practice.

**Generation of Firewall**
Firewalls can be categorized based on its generation.

1. **First Generation- Packet Filtering Firewall :** Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers).
   Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers.

   Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be Filtered

according to following rules:

| | Source IP | Dest. IP | Source Port | Dest. Port | Action |
|---|---|---|---|---|---|
| 1 | 192.168.21.0 | -- | -- | -- | deny |
| 2 | -- | -- | -- | 23 | deny |
| 3 | -- | 192.168.21.3 | -- | -- | deny |
| 4 | -- | 192.168.21.0 | -- | >1023 | Allow |

Sample Packet Filter Firewall Rule

1. Incoming packets from network 192.168.21.0 are blocked.
2. Incoming packets destined for internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.

2. **Second Generation- Stateful Inspection Firewall :** Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.
3. **Third Generation- Application Layer Firewall :** Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.
   In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules.
   *Note: Application layer firewalls can also be used as Network Address Translator(NAT).*
4. **Next Generation Firewalls (NGFW) :** Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

**Types of Firewall**

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls:** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls:** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Both types of firewall have their own advantages.

## Basic concepts of Cryptography

Whenever we come across the term cryptography, the first thing and probably the only thing that comes to our mind is private communication through encryption. There is more to cryptography than just encryption. In this article, we will try to learn the basics of cryptography.

## The Basic Principles

### 1. Encryption

In a simplest form, encryption is to convert the data in some unreadable form. This helps in protecting the privacy while sending the data from sender to receiver. On the receiver side, the data can be decrypted and can be brought back to its original form. The reverse of encryption is called as decryption. The concept of encryption and decryption requires some extra information for encrypting and decrypting the data. This information is known as key. There may be cases when same key can be used for both encryption and decryption while in certain cases, encryption and decryption may require different keys.

### 2. Authentication

This is another important principle of cryptography. In a layman's term, authentication ensures that the message was originated from the originator claimed in the message. Now, one may think how to make it possible? Suppose, Alice sends a message to Bob and now Bob wants proof that the message has been indeed sent by Alice. This can be made possible if Alice performs some action on message that Bob knows only Alice can do. Well, this forms the basic fundamental of Authentication.

### 3. Integrity

Now, one problem that a communication system can face is the loss of integrity of messages being sent from sender to receiver. This means that Cryptography should ensure that the messages that are received by the receiver are not altered anywhere on the communication path. This can be achieved by using the concept of cryptographic hash.

### 4. Non Repudiation

What happens if Alice sends a message to Bob but denies that she has actually sent the message? Cases like these may happen and cryptography should prevent the originator or sender to act this way. One popular way to achieve this is through the use of digital signatures.

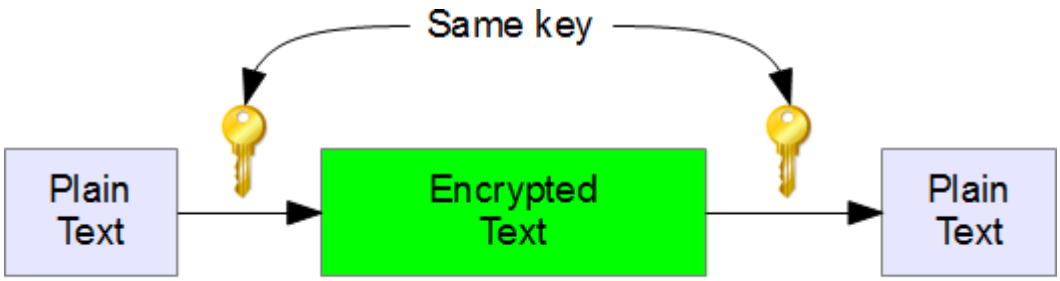
## Types of Cryptography

There are three types of cryptography techniques :

- Secret key Cryptography
- Public key cryptography
- Hash Functions

1. Secret Key Cryptography

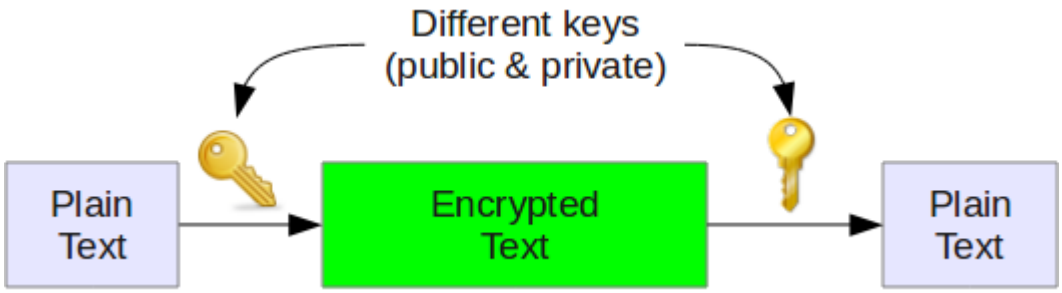
This type of cryptography technique uses just a single key. The sender applies a key to encrypt a message while the receiver applies the same key to decrypt the message. Since only single key is used so we say that this is a symmetric encryption.




The biggest problem with this technique is the distribution of key as this algorithm makes use of single key for encryption or decryption.

2. Public Key Cryptography

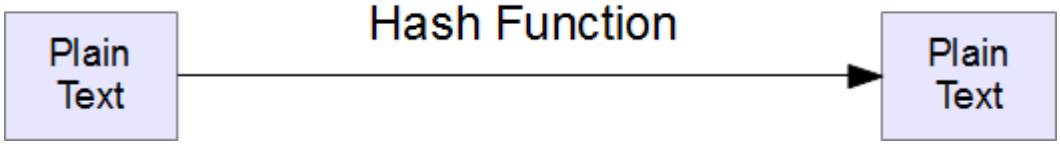
This type of cryptography technique involves two key crypto system in which a secure communication can take place between receiver and sender over insecure communication channel. Since a pair of keys is applied here so this technique is also known as asymmetric encryption.




In this method, each party has a private key and a public key. The private is secret and is not revealed while the public key is shared with all those whom you want to communicate with. If Alice wants to send a message to bob, then Alice will encrypt it with Bob's public key and Bob can decrypt the message with its private key.

This is what we use when we setup public key authentication in openssh to login from one server to another server in the backend without having to enter the password.

3. Hash Functions



This technique does not involve any key. Rather it uses a fixed length hash value that is computed on the basis of the plain text message. Hash functions are used to check the integrity of the message to ensure that the message has not be altered,compromised or affected by virus.

So we see that how different types of cryptography techniques (described above) are used to implement the basic principles that we discussed earlier. In the future article of this series, we'll cover more advanced topics on Cryptography.