MAR GREGORIOS COLLEGE OF ARTS & SCIENCE

Block No.8, College Road, Mogappair West, Chennai – 37

Affiliated to the University of Madras
Approved by the Government of Tamil Nadu
An ISO 9001:2015 Certified Institution

DEPARTMENT OF COMPUTER APPLICATIONS

SUBJECT NAME: COMPUTER NETWORKS

SEMESTER: IV

PREPARED BY: PROF.K.RAJALAKSHMI/PROF.S.ANITHA/
PROF.J.SUMITHRA DEVI

OBJECTIVES:

- To understand the concept of Computer network
- To impart knowledge about networking and inter networking devices

OUTCOMES:

- Analyse different network models
- Analyse and compare a number of data link, network and transport layer
- Analysing key networking protocols and their hierarchical relationship in the conceptual model like TCP/IP and OSI

UNIT - I Introduction – Network Hardware - Software - Reference Models - OSI and TCP/IP Models - Example Networks: Internet, ATM, Ethernet and Wireless LANs - Physical Layer - Theoretical Basis for Data Communication - Guided Transmission Media.

UNIT - II Wireless Transmission - Communication Satellites - Telephone System: Structure, Local Loop, Trunks and Multiplexing and Switching. Data Link Layer: Design Issues - Error Detection and Correction.

UNIT - III Elementary Data Link Protocols - Sliding Window Protocols - Data Link Layer in the Internet - Medium Access Layer - Channel Allocation Problem - Multiple Access Protocols - Bluetooth.

UNIT - IV Network Layer - Design Issues - Routing Algorithms - Congestion Control Algorithms - IP Protocol - IP Addresses - Internet Control Protocols.

UNIT - V Transport Layer - Services - Connection Management - Addressing, Establishing and Releasing a Connection - Simple Transport Protocol - Internet Transport Protocols (ITP) - Network Security: Cryptography.

TEXT BOOK : 1. A. S. Tanenbaum, “Computer Networks”, Prentice-Hall of India 2008, 4th Edition.
REFERENCE BOOKS:

1. Stallings, “Data and Computer Communications”, Pearson Education 2012, 7 th Edition.

2. B. A. Forouzan, “Data Communications and Networking”, Tata McGraw Hill 2007, 4th Edition.

3. F. Halsall, “Data Communications, Computer Networks and Open Systems”, Pearson Education 2008. 4. D. Bertsekas and R. Gallagher, “Data Networks”, PHI 2008, 2 nd Edition.

5. Lamarca, “Communication Networks”, Tata McGraw Hill 2002.

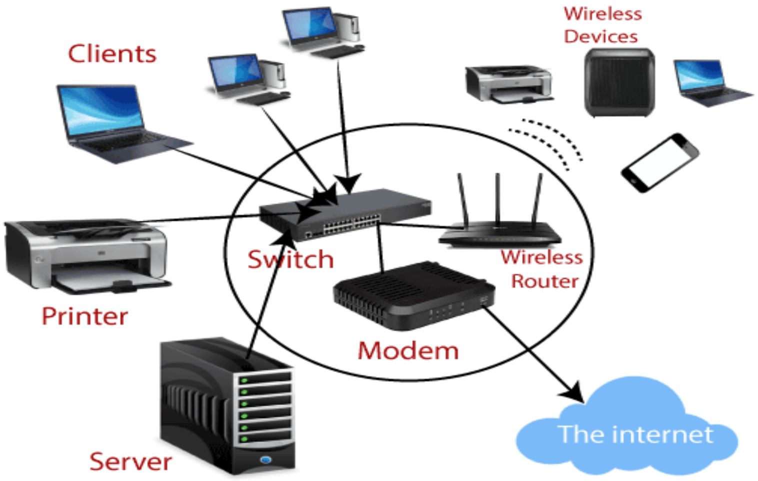
WEB REFERENCES: NPTEL & MOOC courses titled Computer Networks
https://nptel.ac.in/courses/106106091/

<u>UNIT I</u>

Introduction to Computer Networks

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. “Computer network’’ to mean a collection of autonomous computers interconnected by a single technology.

Two computers are said to be interconnected if they are able to exchange information. The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used. Networks come in many sizes, shapes and forms, as we will see later. They are usually connected together to make larger networks, with the Internet being the most well-known example of a network of networks.



Basic Diagram for Computer Networks

USES OF COMPUTER NETWORKS

1. Business Applications
   - To distribute information throughout the company (resource sharing).Sharing physical resources such as printers, and tape backup systems, is sharing information
   - client-server model. It is widely used and forms the basis of much network usage.
   - Communication medium among employees. email (electronic mail) which employees generally use for a great deal of daily communication.
   - Telephone calls between employees may be carried by the computer network.instead of by the phone company. This technology is called IP telephony or Voice over IP (VoIP) when Internet technology is used.
   - Desktop sharing lets remote workers see and interact with a graphical. Computer screen

- doing business electronically, especially with customers and suppliers. This new model is called e-commerce (electronic commerce) and it has grown rapidly in recent years.

2 .Home Applications

- peer-to-peer communication.
- person-to-person communication
- electronic commerce
- entertainment.(game playing,)

3.Mobile Users

- Text messaging or texting
- Smart phones
- GPS (Global Positioning System)
- m-commerce
- NFC (Near Field Communication)

4. Social Issues With the good comes the bad, as this new-found freedom brings with it many unsolved social, political, and ethical issues. Social networks, message boards, content sharing sites, and a host of other applications allow people to share their views with like-minded individuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise.

Applications

- Accessing Remote databases
- Accessing Remote programs
- Value added communication facility
- Marketing and sales
- Financial services
- Manufacturing
- Electronic message
- Directory services
- Information services
- Teleconferencing
- Cellular telephone
- Cable television

Types of Computer Networks

A computer network is a cluster of computers over a shared communication path that work for the purpose of sharing resources from one computer to another, provided by or located on the network nodes.

Some of the uses of computer networks are the following:

- Communicating using email, video, instant messaging, etc.

- Sharing devices such as printers, scanners, etc.
- Sharing files
- Sharing software and operating programs on remote systems
- Allowing network users to easily access and maintain information

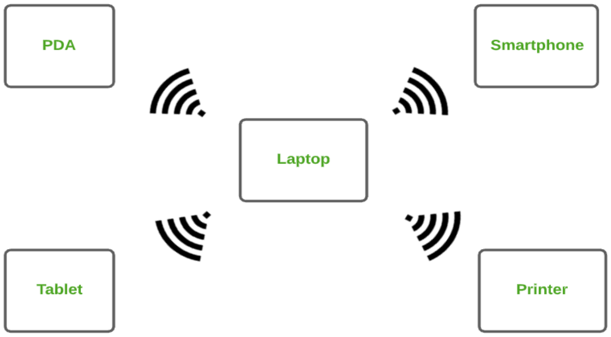
Types of Computer Networks

1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Wide Area Network (WAN)
4. Wireless Local Area Network (WLAN)
5. Metropolitan Area Network (MAN)
6. Enterprise Private Network (EPN)
7. Virtual Private Network

These are explained as following below.

1. **Personal Area Network (PAN)** :

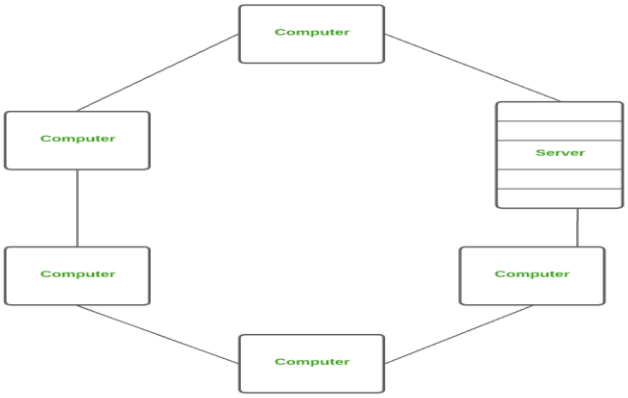
   PAN is the most basic type of computer network. This network is restrained to a single person, that is, communication between the computer devices is centred only to an individual's work space. PAN offers a network range of 10 meters from a person to the device providing communication.



2. **Local Area Network (LAN) :**

   LAN is the most frequently used network. A LAN is a computer network that connects computers together through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-fi.

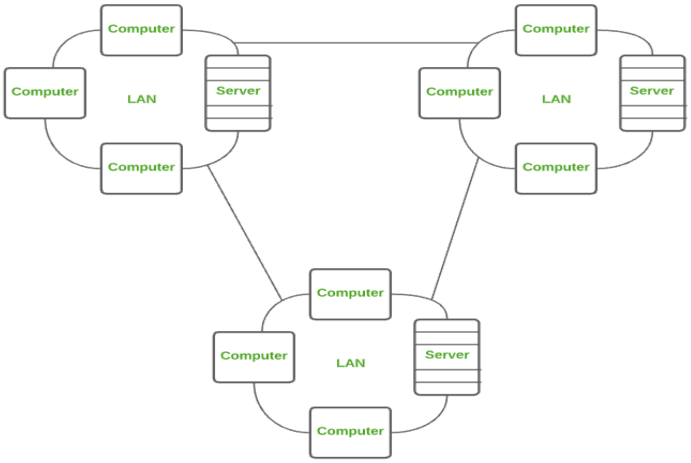
Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.



3. **Wide Area Network (WAN) :**

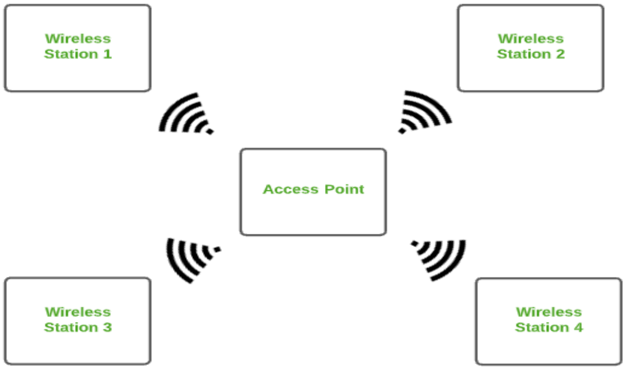
   WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other.

The most common example of WAN is the Internet.



4. Wireless Local Area Network (WLAN) :
WLAN is a type of computer network that acts as a local area network but makes use of wireless network technology like Wi-Fi. This network doesn’t allow devices communicating over physical cables like in LAN, but allows devices to communicate wirelessly.

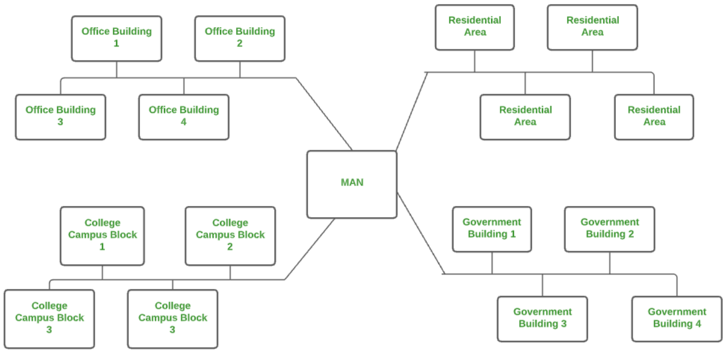
The most common example of WLAN is Wi-Fi.



4. **Metropolitan Area Network (MAN) :**

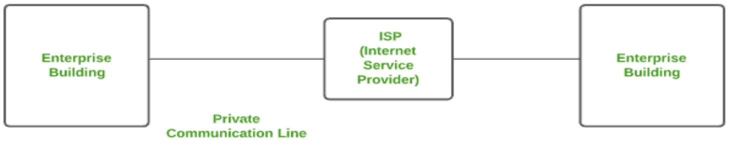
   A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town or metropolitan area.

Examples of MAN are networking in towns, cities, a single large city, large area within multiple buildings, etc.



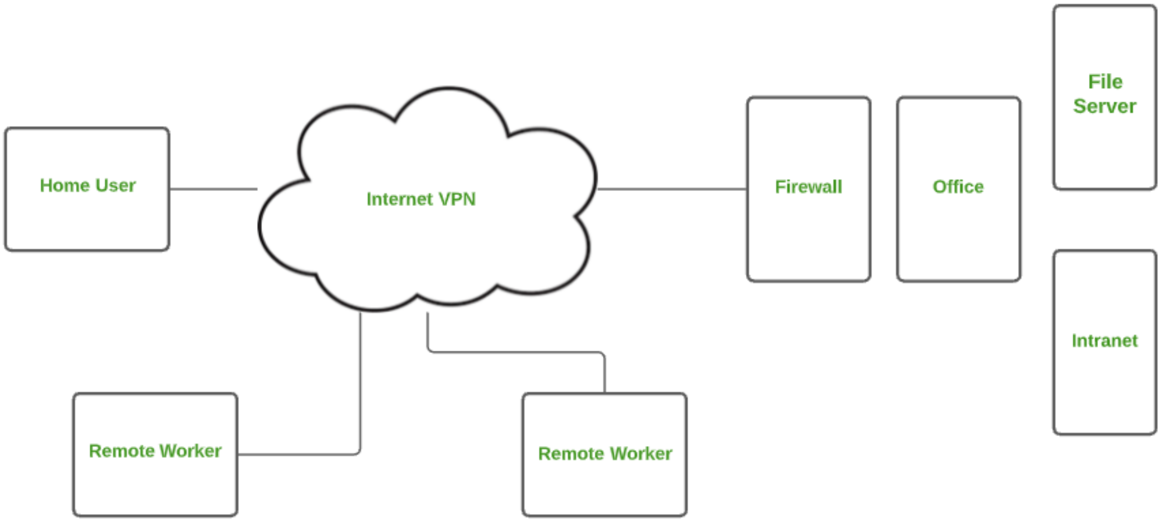
5. **Enterprise Private Network (EPN) :**

   EPN is a type of computer network mostly used by businesses that want a secure connection over various locations to share computer resources.



7.Virtual Private Network (VPN) :

A VPN is a type of computer network that extends a private network across the internet and lets the user send and receive data as if they were connected to a private network even though they are not. Through a virtual point to point connection users can access a private network remotely. VPN protects you from malicious sources by operating as a medium that gives you protected network connection.



Network Hardware

Network devices or networking hardware are the physical devices that are used for establishing connections and facilating interaction between different devices in a computer network.

Network interface card (NIC)

A network interface card (NIC) is a hardware component, typically a circuit board or chip, which is installed on a computer so it can connect to a network. Modern NICs provide functionality to computers, such as support for I/O interrupt, direct memory access (DMA) interfaces, data transmission, network traffic engineering and partitioning.

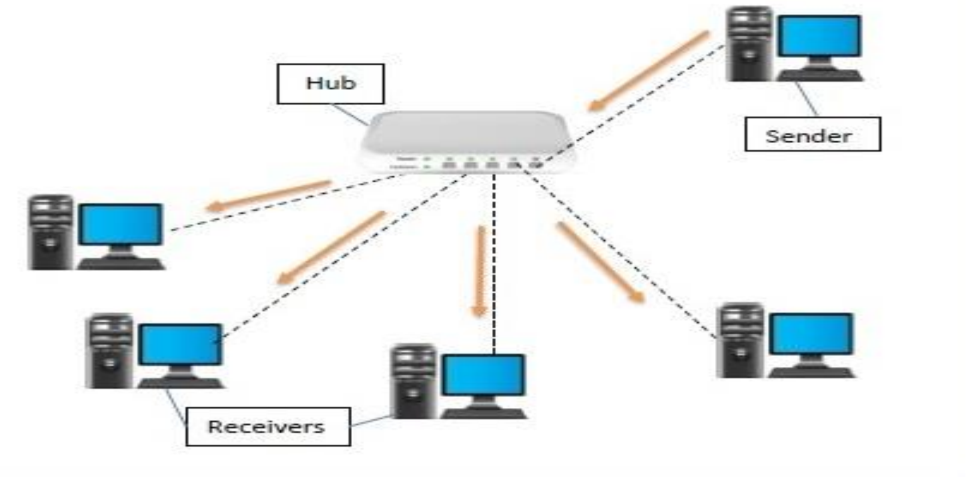
A NIC provides a computer with a dedicated, full-time connection to a network. It implements the physical layer circuitry necessary for communicating with a data link layer standard, such as Ethernet or Wi-Fi. Each card represents a device and can prepare, transmit and control the flow of data on the network.

The NIC uses the OSI model to send signals at the physical layer, transmit data packets at the network layer and operate as an interface at the TCP/IP layer.

Hubs

A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN.

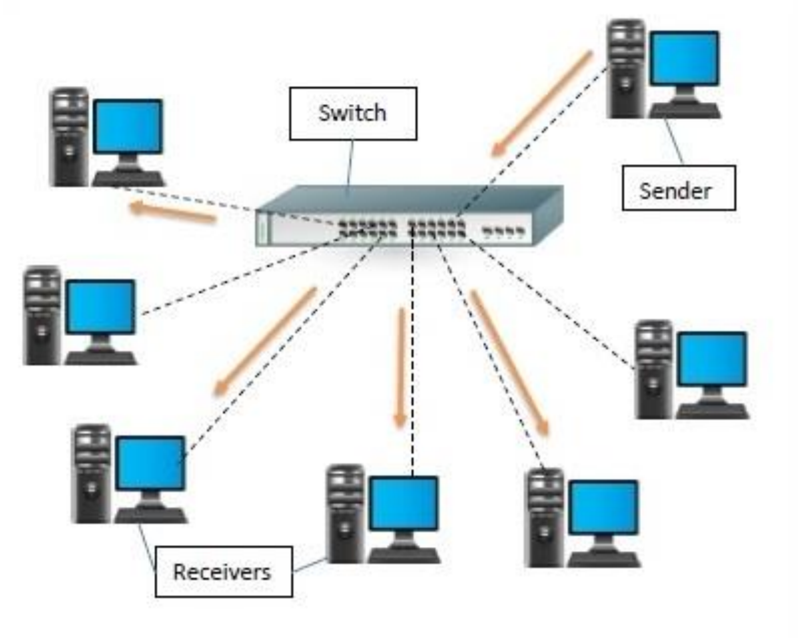
A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.



Switches

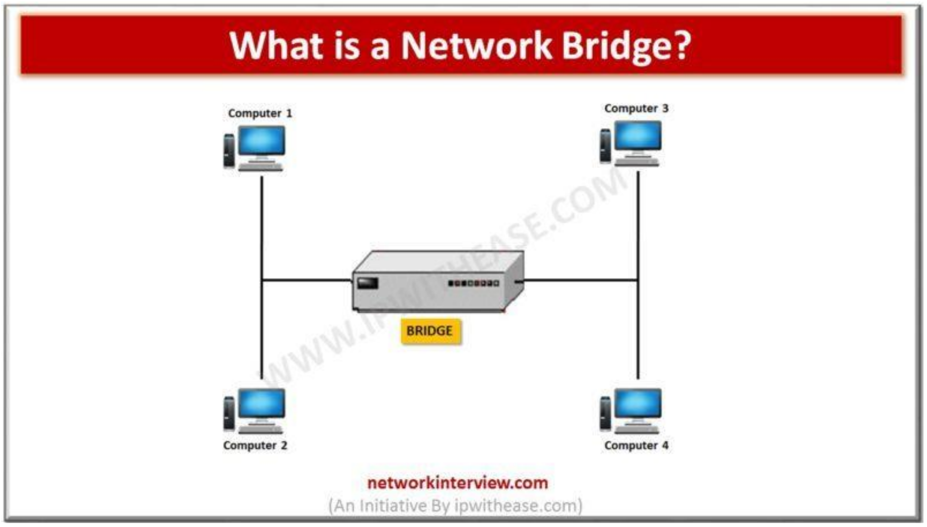
A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over the network.

Like a hub, a switch also has many ports, to which computers are plugged in. However, when a data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding device(s). Thus, it supports both unicast and multicast communications.



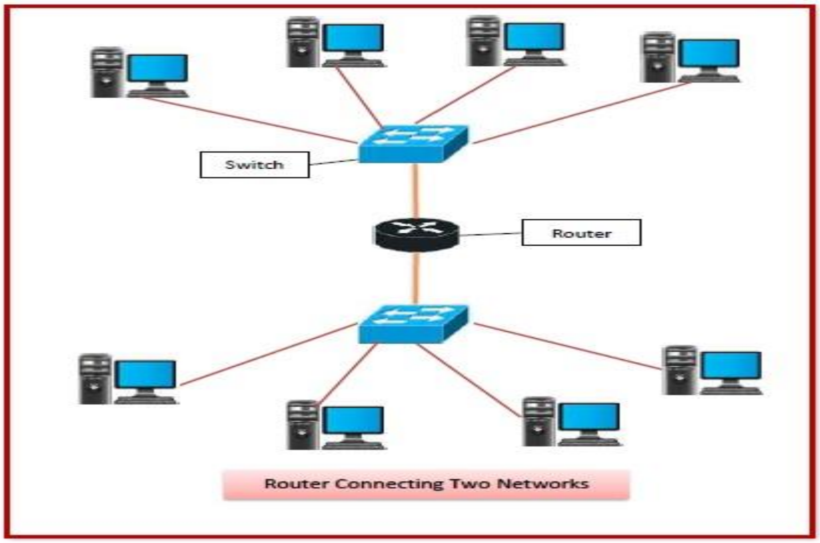
Bridges

A bridge is a computer **network hardware device** that works at the **data link layer of OSI model,** and it also helps to make interconnection in between multiple networks with using of same protocol.



Routers

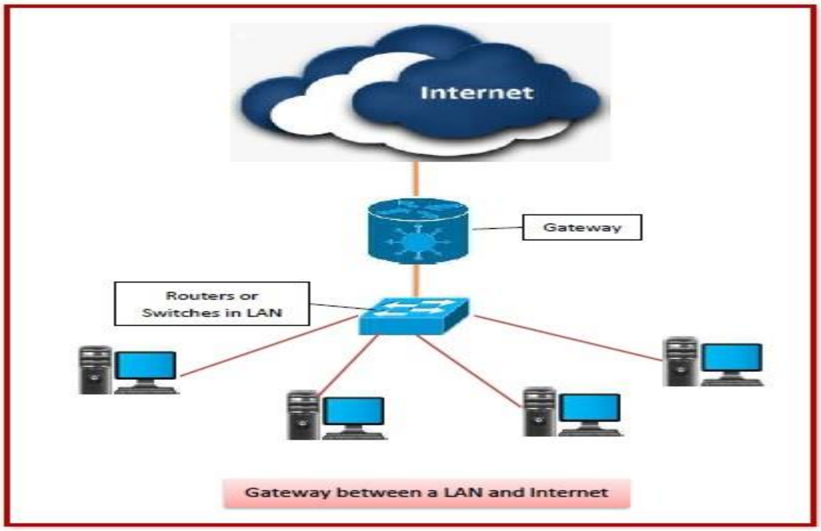
Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.



Router Connecting Two Networks

Gateways

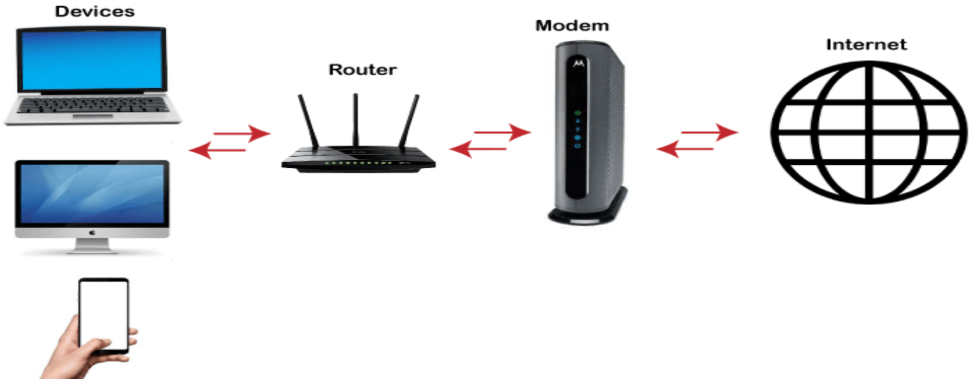
A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.



Gateway between a LAN and Internet

Modem

Modem stands for Modulation Demodulation. A modem converts the digital data signals into analogue data signals. They can be installed within the computer in a development slot applicable for it.



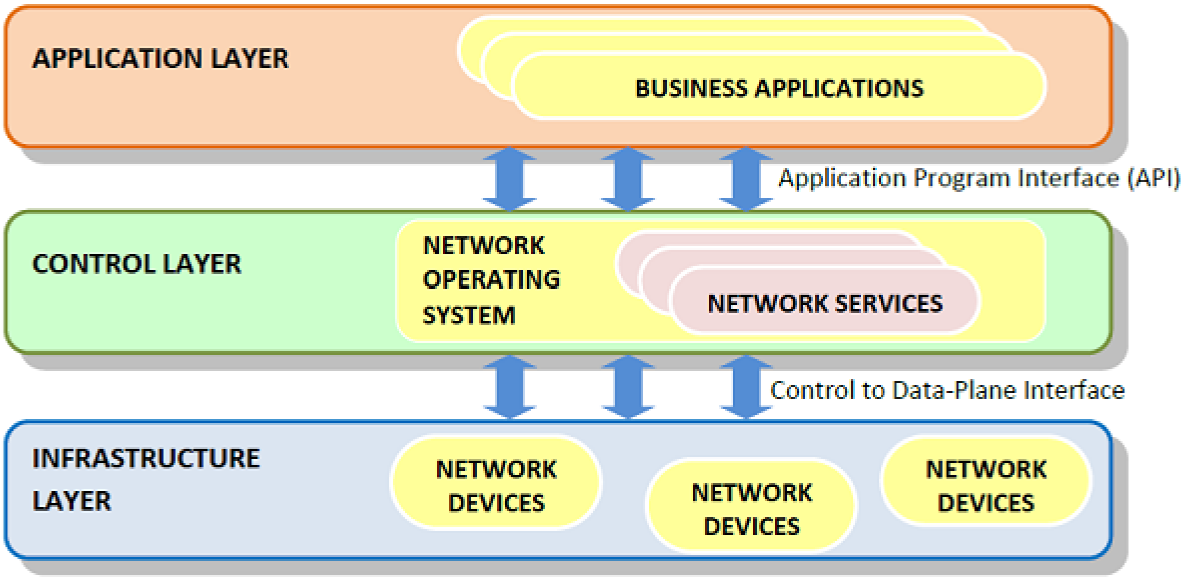
Network Software

Network software encompasses a broad range of software used for design, implementation, and operation and monitoring of computer networks. Traditional networks were hardware based with software embedded. With the advent of Software – Defined Networking (SDN), software is separated from the hardware thus making it more adaptable to the ever-changing nature of the computer network.

Functions of Network Software

- Helps to set up and install computer networks
- Enables users to have access to network resources in a seamless manner
- Allows administrations to add or remove users from the network
- Helps to define locations of data storage and allows users to access that data
- Helps administrators and security system to protect the network from data breaches, unauthorized access and attacks on a network
- Enables network virtualizations

The Software Defined Networking framework has three layers as depicted in the following diagram



- **APPLICATION LAYER** – SDN applications reside in the Application Layer. The applications convey their needs for resources and services to the control layer through APIs.
- **CONTROL LAYER** – The Network Control Software, bundled into the Network Operating System, lies in this layer. It provides an abstract view of the underlying network infrastructure. It receives the requirements of the SDN applications and relays them to the network components.
- **INFRASTRUCTURE LAYER** – Also called the Data Plane Layer, this layer contains the actual network components. The network devices reside in this layer that shows their network capabilities through the Control to data-Plane Interface.

Reference Models in Computer Network

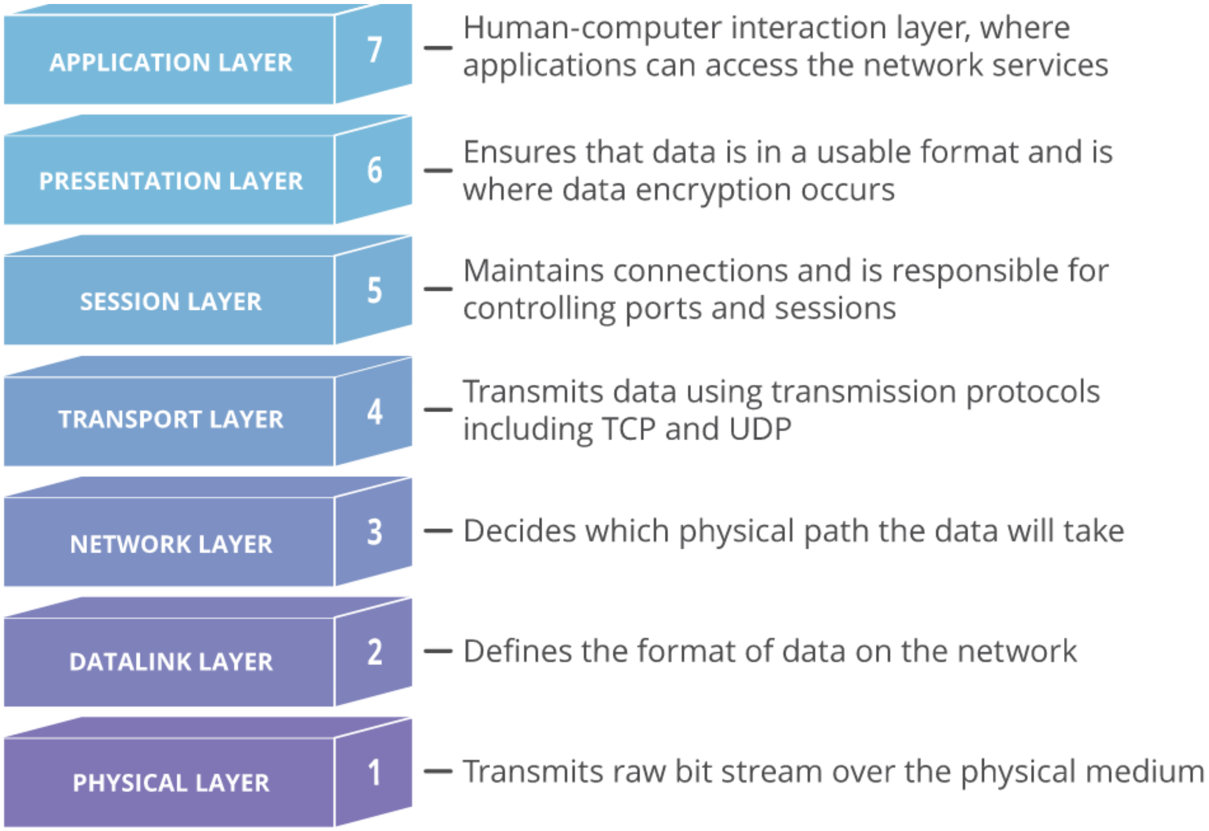
In computer networks, reference models give a conceptual framework that standardizes communication between heterogeneous networks.

The two popular reference models are –

- OSI Model
- TCP/IP Protocol Suite

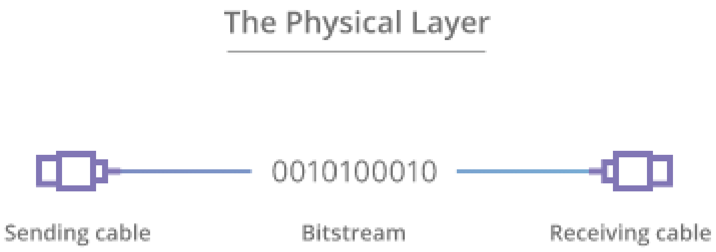
Layers of OSI Model

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


APPLICATION LAYER
7
— Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER
6
— Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER
5
— Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
4
— Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER
3
— Decides which physical path the data will take
DATALINK LAYER
2
— Defines the format of data on the network
PHYSICAL LAYER
1
— Transmits raw bit stream over the physical medium

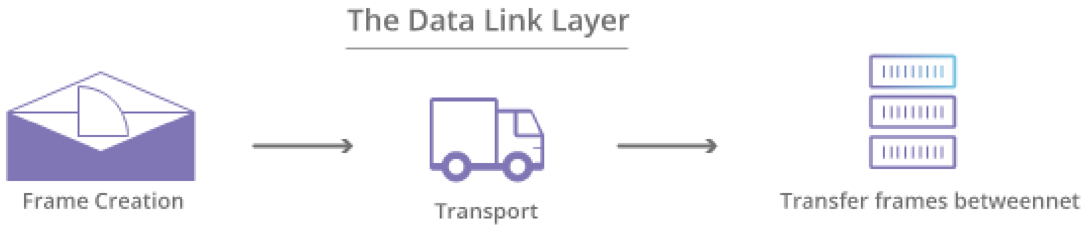
1. The physical layer

This layer includes the physical equipment involved in the data transfer, such as the cables and switches. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.



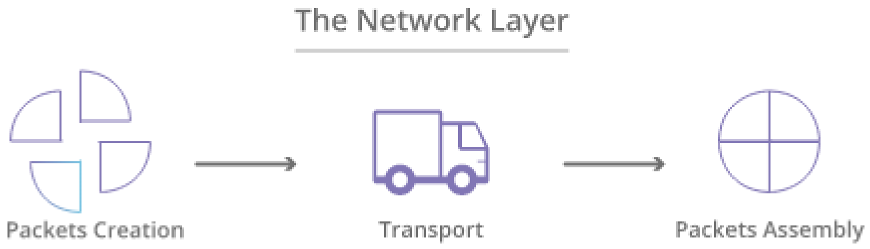
2. The data link layer

The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the SAME network. The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication (The transport layer only does flow control and error control for inter-network communications).



3. The network layer

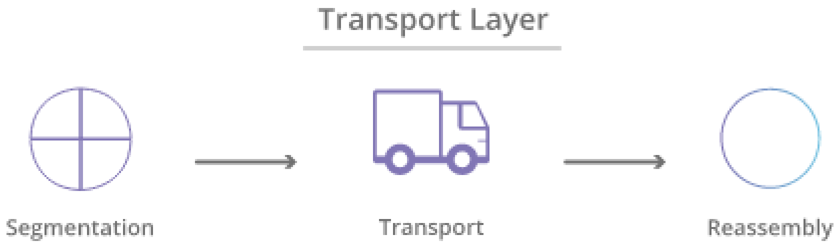
The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembling these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination; this is known as routing.



4. The transport layer

Layer 4 is responsible for end-to-end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.

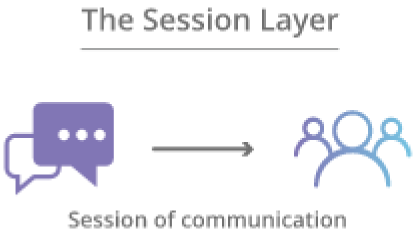
The transport layer is also responsible for flow control and error control. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection doesn't overwhelm a receiver with a slow connection. The transport layer performs error control on the receiving end by ensuring that the data received is complete, and requesting a retransmission if it isn't.



5. The session layer

This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.

The session layer also synchronizes data transfer with checkpoints. For example, if a 100 megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.



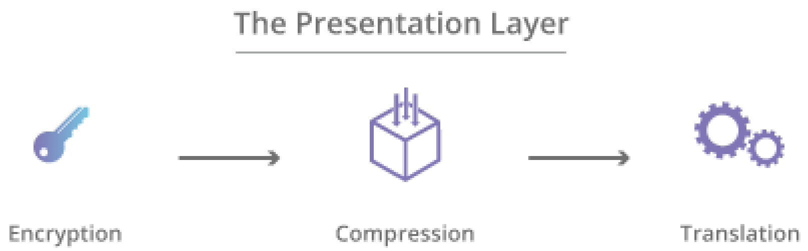
6. The presentation layer

This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for translation, encryption, and compression of data.

Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand.

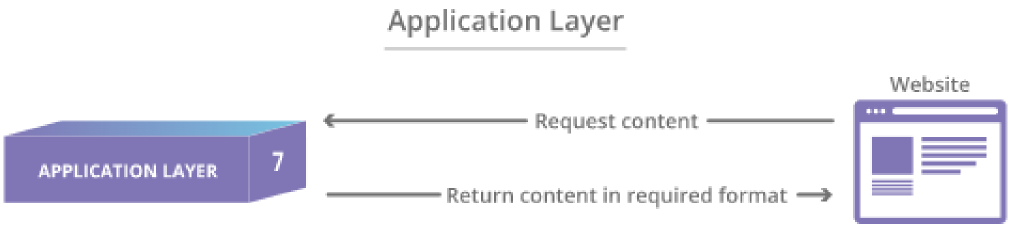
If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender’s end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.

Finally the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.



7. The application layer

This is the only layer that directly interacts with data from the user. Software applications like web browsers and email clients rely on the application layer to initiate communications. But it should be made clear that client software applications are not part of the application layer; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user. Application layer protocols include HTTP as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

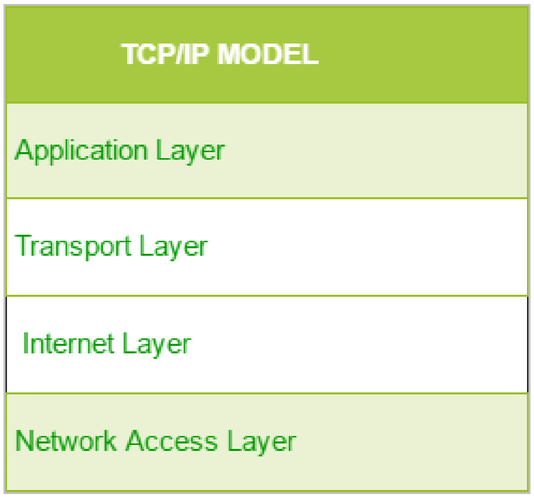


TCP/IP

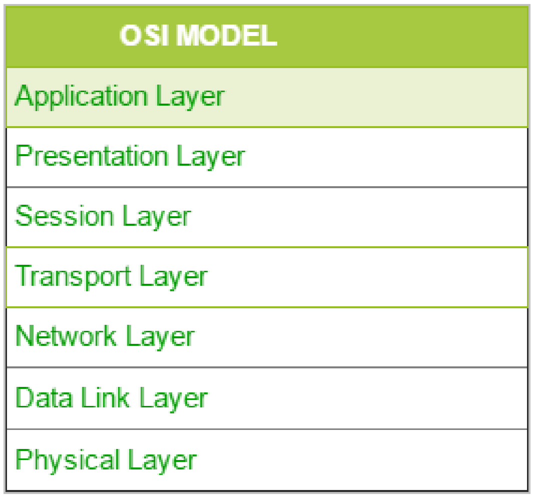
The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department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



TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer



OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

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.
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.

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.

Examples of Network:-

Internet

The Internet is a **global network** of billions of computers and other electronic devices. With the Internet, it's possible to access almost any information, communicate with anyone else in the world, and do much more.

You can do all of this by connecting a computer to the Internet, which is also called **going online.** When someone says a computer is online, it's just another way of saying it's connected to the Internet.

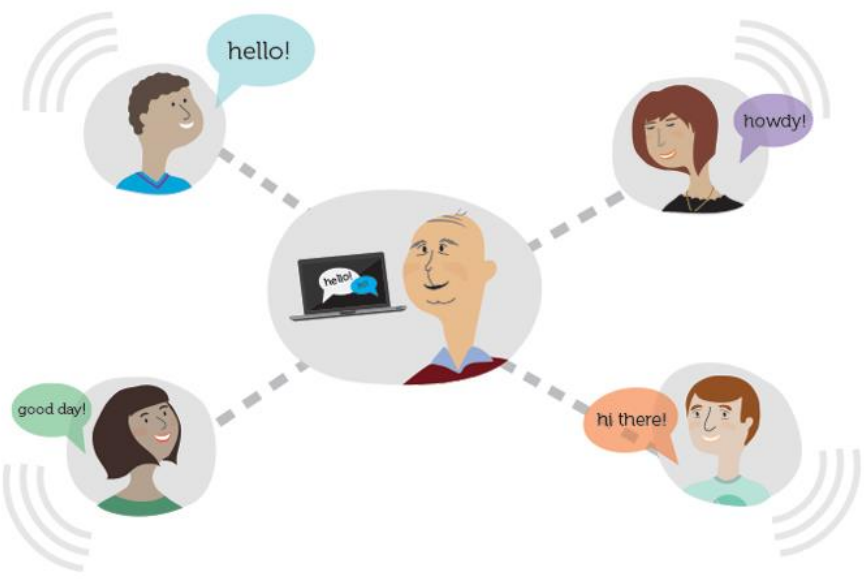
How does the Internet work?

It's important to realize that the Internet is a global network of **physical cables**, which can include copper telephone wires, TV cables, and fiber optic cables. Even wireless connections like Wi-Fi and 3G/4G rely on these physical cables to access the Internet.

When you visit a website, your computer sends a request over these wires to a **server**. A server is where websites are stored, and it works a lot like your computer's hard drive. Once the request arrives, the server retrieves the website and sends the correct data back to your computer. What's amazing is that this all happens in just a few seconds!

Other things you can do on the Internet

One of the best features of the Internet is the ability to communicate almost instantly with anyone in the world. **Email** is one of the oldest and most universal ways to communicate and share information on the Internet, and billions of people use it. **Social media** allows people to connect in a variety of ways and build communities online.



There are many other things you can do on the Internet. There are thousands of ways to keep up with news or **shop for anything** online. You can pay your bills, **manage your bank accounts**, meet new people, **watch TV**, or learn new skills. You can learn or do almost anything online.

What is an IP address?

IP address stands for internet protocol address. Every PC/Local machine is having an IP address and that IP address is provided by the Internet Service Providers (ISP's). These are some sets of rules which govern the flow of data whenever a device is connected to the Internet. It differentiates computers, websites, and routers. Just like human identification cards like Aadhar cards, Pan cards, or any other unique identification documents. Every laptop and desktop has its own unique IP address for identification. It's an important part of internet technology. An IP address is displayed as a set of four-digit like 192.154.3.29. Here each number on the set ranges from 0 to 255. Hence, the total IP address range from 0.0.0.0 to 255.255.255.255.

World Wide Web(WWW)

The worldwide web is a collection of all the web pages, web documents that you can see on the Internet by searching their URLs (Uniform Resource Locator) on the Internet. For example, www.geeksforgeeks.org is a URL of the GFG website and all the content of this site like webpages and all the web documents are stored on the worldwide web. Or in other words, the world wide web is an information retrieval service of the web.

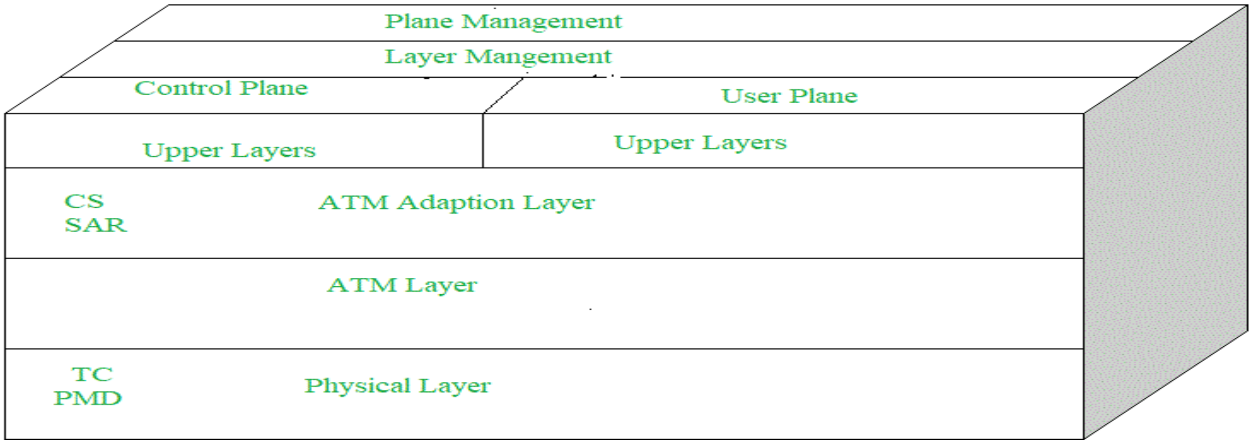
Asynchronous Transfer Mode (ATM)

It is an International Telecommunication Union- Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video, or voice which is conveyed in small fixed-size packets called cells. Cells are transmitted asynchronously and the network is connection-oriented.

Working of ATM:

ATM standard uses two types of connections. i.e., Virtual path connections (VPCs) which consist of Virtual channel connections (VCCs) bundled together which is a basic unit carrying a single stream of cells from user to user. A virtual path can be created end-to-end across an ATM network, as it does not rout the cells to a particular virtual circuit. In case of major failure, all cells belonging to a particular virtual path are routed the same way through the ATM network, thus helping in faster recovery.

Switches connected to subscribers use both VPIs and VCIs to switch the cells which are Virtual Path and Virtual Connection switches that can have different virtual channel connections between them, serving the purpose of creating a *virtual trunk* between the switches which can be handled as a single entity. Its basic operation is straightforward by looking up the connection value in the local translation table determining the outgoing port of the connection and the new VPI/VCI value of connection on that link.



ATM Applications:

1. **ATM WANs –**
   It can be used as a WAN to send cells over long distances, a router serving as an end-point between ATM network and other networks, which has two stacks of the protocol.

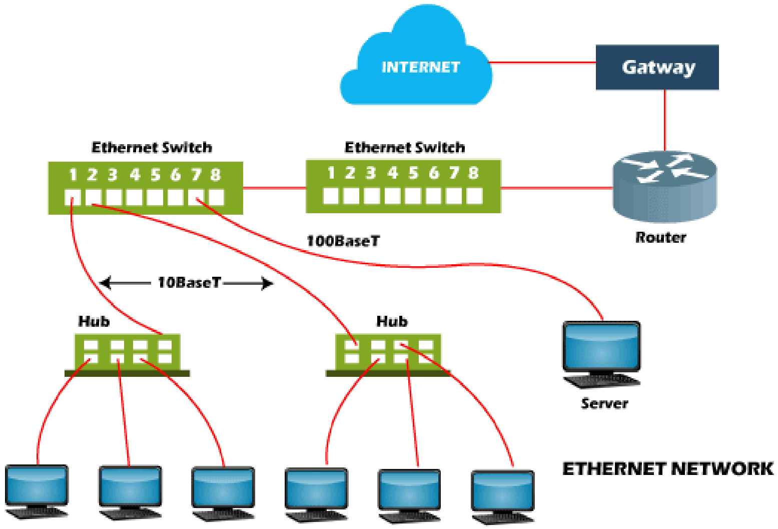
2. **Multimedia virtual private networks and managed services –**
   It helps in managing ATM, LAN, voice, and video services and is capable of full-service virtual private networking, which includes integrated access to multimedia.
3. **Frame relay backbone –**
   Frame relay services are used as a networking infrastructure for a range of data services and enabling frame-relay ATM service to Internetworking services.

4. **Residential broadband networks –**
   ATM is by choice provides the networking infrastructure for the establishment of residential broadband services in the search of highly scalable solutions.

5. **Carrier infrastructure for telephone and private line networks –**
   To make more effective use of SONET/SDH fiber infrastructures by building the ATM infrastructure for carrying the telephonic and private-line traffic.

What is Ethernet?

Ethernet is a type of communication protocol that is created at Xerox PARC in 1973 by Robert Metcalfe and others, which connects computers on a network over a wired connection. It is a widely used LAN protocol, which is also known as Alto Aloha Network. It connects computers within the local area network and wide area network. Numerous devices like printers and laptops can be connected by LAN and WAN within buildings, homes, and even small neighborhoods.



It offers a simple user interface that helps to connect various devices easily, such as switches, routers, and computers. A local area network (LAN) can be created with the help of a single router and a few Ethernet cables, which enable communication between all linked devices. This is because an Ethernet port is included in your laptop in which one end of a cable is plugged in and connect the other to a router. Ethernet ports are slightly wider, and they look similar to telephone jacks. The wireless networks replaced Ethernet in many areas; however, Ethernet is still more common for wired networking. Wi-Fi reduces the need for cabling as it allows the users to connect smartphones or laptops to a network without the required cable. While comparing with Gigabit Ethernet, the faster maximum data transfer rates are provided by the

802.11ac Wi-Fi standard. Still, as compared to a wireless network, wired connections are more secure and are less prone to interference. This is the main reason to still use Ethernet by many businesses and organizations.

Wireless LAN

Wireless LAN stands for **Wireless Local Area Network**. It is also called LAWN (**Local Area Wireless Network**). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.

The IEEE 802.11 group of standards defines the technologies for wireless LANs. For path sharing, 802.11 standard uses the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance). It also uses an encryption method i.e. wired equivalent privacy algorithm.

Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.

In some instance wireless LAN technology is used to save costs and avoid laying cable, while in other cases, it is the only option for providing high-speed internet access to the public. Whatever the reason, wireless solutions are popping up everywhere.

Advantages of WLANs

- **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).
- **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.
- **Design:** Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.
- **Robustness:** Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.
- **Cost:** The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, after providing wireless access to the wireless network via an access point for the first user, adding additional users to a network will not increase the cost. And second, wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it.
- **Ease of Use:** Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

Physical Layer

Physical layer in the OSI model plays the role of interacting with actual hardware and signaling mechanism. Physical layer is the only layer of OSI network model which actually deals with the physical connectivity of two different stations. This layer defines the hardware equipment, cabling, wiring, frequencies, pulses used to represent binary signals etc.

Physical layer provides its services to Data-link layer. Data-link layer hands over frames to physical layer. Physical layer converts them to electrical pulses, which represent binary data.The binary data is then sent over the wired or wireless media.

Signals

When data is sent over physical medium, it needs to be first converted into electromagnetic signals. Data itself can be analog such as human voice, or digital such as file on the disk.Both analog and digital data can be represented in digital or analog signals.

- **Digital Signals**

  Digital signals are discrete in nature and represent sequence of voltage pulses. Digital signals are used within the circuitry of a computer system.

- **Analog Signals**

  Analog signals are in continuous wave form in nature and represented by continuous electromagnetic waves.

Theoretical Basis for Data Communication

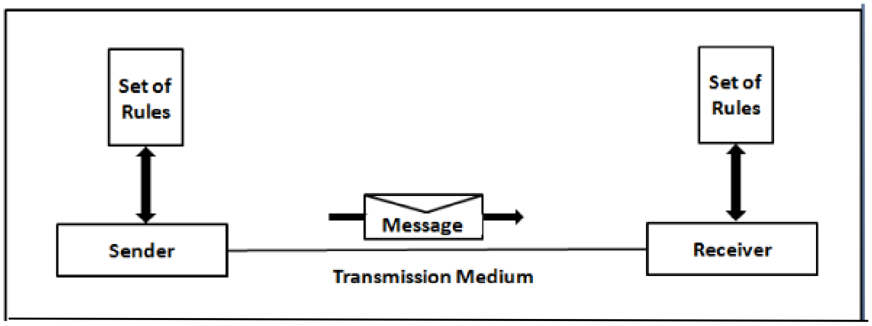
Data Communication is a process of exchanging data or information. In case of computer networks this exchange is done betweentwo devices over a transmission medium.
This process involves a communication system which is made up of hardware and software. The hardware part involves the sender and receiver devices and the intermediate devices through which the data passes. The software part involves certain rules which specify what is to be communicated, how it is to be communicated and when. It is also called as a Protocol.
The following sections describes the fundamental characteristics that are important for the effective working of data communication process and is followed by the components that make up a data communications system.

Characteristics of Data Communication
The effectiveness of any data communications system depends upon the following four fundamental characteristics:

1.Delivery: The data should be delivered to the correct destination and correct user.
2. Accuracy: The communication system should deliver the data accurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data.
3. Timeliness: Audio and Video data has to be delivered in a timely manner without any delay; such a data delivery is called real time transmission of data.
4. Jitter: It is the variation in the packet arrival time. Uneven Jitter may affect the timeliness of data being transmitted

Components of Data Communication

A Data Communication system has five components as shown in the diagram below:



1. Message
Message is the information to be communicated by the sender to the receiver.
2. Sender
The sender is any device that is capable of sending the data (message).
3. Receiver
The receiver is a device that the sender wants to communicate the data (message).
4. Transmission Medium
It is the path by which the message travels from sender to receiver.
It can be wired or wireless and many subtypes in both.

5. Protocol
It is an agreed upon set or rules used by the sender and receiver to communicate data.
A protocol is a set of rules that governs data communication.
A Protocol is a necessity in data communications without which the communicating entities are like two persons trying to talk to each other in a different language without know the other language

Transmission Media

The media over which the information between two computer systems is sent, called transmission media. Transmission media comes in two forms.

- **Guided Media**

  All communication wires/cables are guided media, such as UTP, coaxial cables, and fiber Optics. In this media, the sender and receiver are directly connected and the information is send (guided) through it.

- **Unguided Media**

  Wireless or open air space is said to be unguided media, because there is no connectivity between the sender and receiver. Information is spread over the air, and anyone including the actual recipient may collect the information.

Guided Media

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

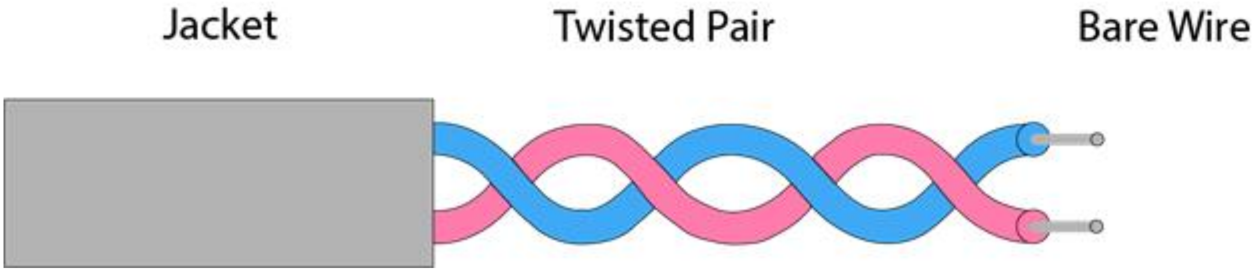
Types Of Guided media:

Twisted pair:

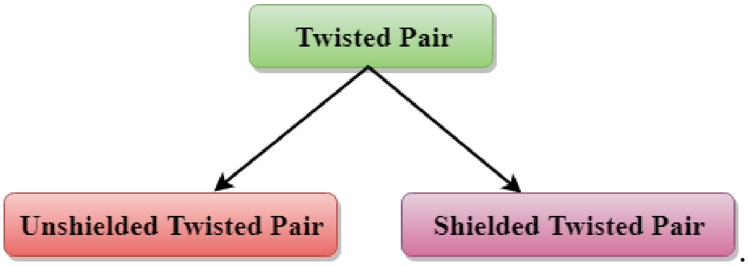
Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Types of Twisted pair:



Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support upto 4Mbps.
- **Category 3:** It can support upto 16Mbps.
- **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- **Category 5:** It can support upto 200Mbps.

Advantages Of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics Of Shielded Twisted Pair:

- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.

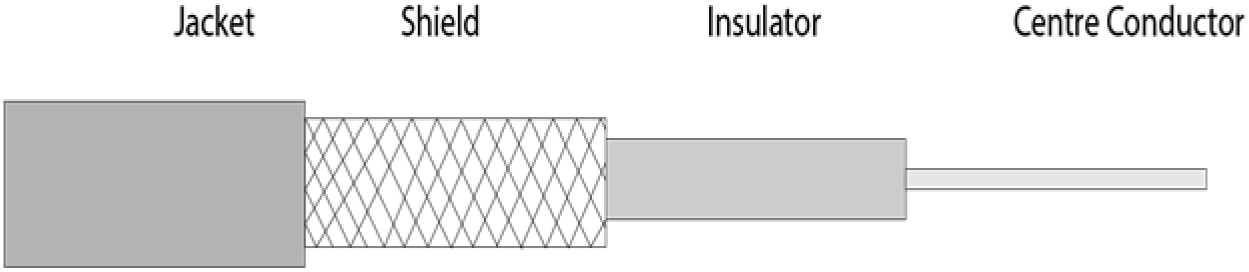
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

Coaxial Cable

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).



Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

UnGuided Transmission

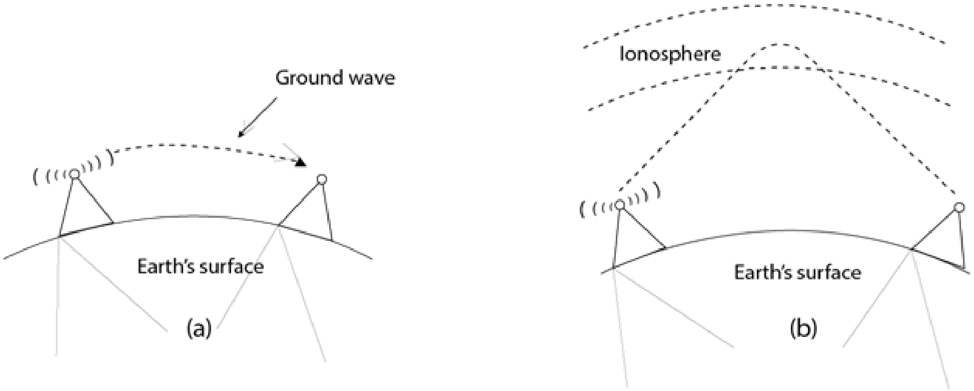
- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.

- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

Radio waves

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is **FM radio**.



Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics Of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.

- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

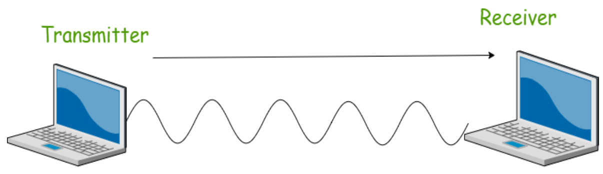
UNIT – II

Wireless Communication

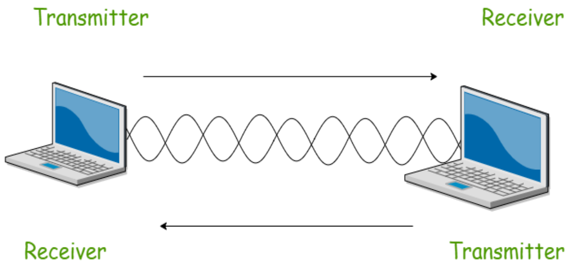
Wired network is a bounded medium. Data travel over a path that a wire or cable takes.In modern era of advanced and enormous no of devices, wired medium of communication imposes a restriction on fluent communication. There are various problems with wired networks.

Basics of Wireless Communication :

Wireless communication takes places over free space through RF (radio frequency), one device, **Transmitter** send signal to other device, **Receiver**. Two devices (transmitter and receiver) must use same frequency (or channel) to be able to communicate with each other. If a large number of wireless devices communicate at same time, radio frequency can cause interference with each other.Interference increases as no of devices increases.



Unidirectional Communication



Bidirectional Communication

Wireless devices share airtime just like wired devices connect to shared media and share common bandwidth. For effective use of media, all wireless devices operate in half duplex mode to avoid collision or interference.

Advantages

Wireless communication involves transfer of information without any physical connection between two or more points. Because of this absence of any 'physical infrastructure', wireless communication has certain advantages. This would often include collapsing distance or space.

Wireless communication has several advantages; the most important ones are discussed below −

Cost effectiveness

Wired communication entails the use of connection wires. In wireless networks, communication does not require elaborate physical infrastructure or maintenance practices. Hence the cost is reduced.

Example − Any company providing wireless communication services does not incur a lot of costs, and as a result, it is able to charge cheaply with regard to its customer fees.

Flexibility

Wireless communication enables people to communicate regardless of their location. It is not necessary to be in an office or some telephone booth in order to pass and receive messages.

Miners in the outback can rely on satellite phones to call their loved ones, and thus, help improve their general welfare by keeping them in touch with the people who mean the most to them.

Convenience

Wireless communication devices like mobile phones are quite simple and therefore allow anyone to use them, wherever they may be. There is no need to physically connect anything in order to receive or pass messages.

Example − Wireless communications services can also be seen in Internet technologies such as Wi-Fi. With no network cables hampering movement, we can now connect with almost anyone, anywhere, anytime.

Speed

Improvements can also be seen in speed. The network connectivity or the accessibility were much improved in accuracy and speed.

Example − A wireless remote can operate a system faster than a wired one. The wireless control of a machine can easily stop its working if something goes wrong, whereas direct operation can’t act so fast.

Accessibility

The wireless technology helps easy accessibility as the remote areas where ground lines can’t be properly laid, are being easily connected to the network.

Example − In rural regions, online education is now possible. Educators no longer need to travel to far-flung areas to teach their lessons. Thanks to live streaming of their educational modules.

communication satellite

A **communication satellite** is a **microwave repeater station** in a space that is used for telecommunication, radio and television signals. A communication satellite processes the data coming from one earth station and it converts the data into another form and send it to the second earth station.

How a Satellite Works

Two stations on earth want to communicate through radio broadcast but are too far away to use conventional means. The two stations can use a relay station for their communication. One earth station transmits the signal to the satellite.

Uplink frequency is the frequency at which ground station is communicating with satellite. The satellite transponder converts the signal and sends it down to the second earth station, and this is called **Downlink frequency**. The second earth station also communicates with the first one in the same way.

Advantages of Satellite

The advantages of Satellite Communications are as follows −

- The Coverage area is very high than that of terrestrial systems.
- The transmission cost is independent of the coverage area.
- Higher bandwidths are possible.

Satellite Communication Basics

The process of satellite communication begins at an **earth station**. Here an installation is designed to transmit and receive signals from a satellite in orbit around the earth. Earth stations send information to satellites in the form of high powered, high frequency (GHz range) signals.

The satellites **receive** and **retransmit** the signals back to earth where they are received by other earth stations in the coverage area of the satellite. **Satellite's footprint** is the area which receives a signal of useful strength from the satellite.

The transmission system from the earth station to the satellite through a channel is called the **uplink**. The system from the satellite to the earth station through the channel is called the **downlink**.

Earth Orbits

A satellite when launched into space, needs to be placed in certain orbit to provide a particular way for its revolution, so as to maintain accessibility and serve its purpose whether scientific, military or commercial. Such orbits which are assigned to satellites, with respect to earth are called as **Earth Orbits**. The satellites in these orbits are Earth Orbit Satellites.

The important kinds of Earth Orbits are −

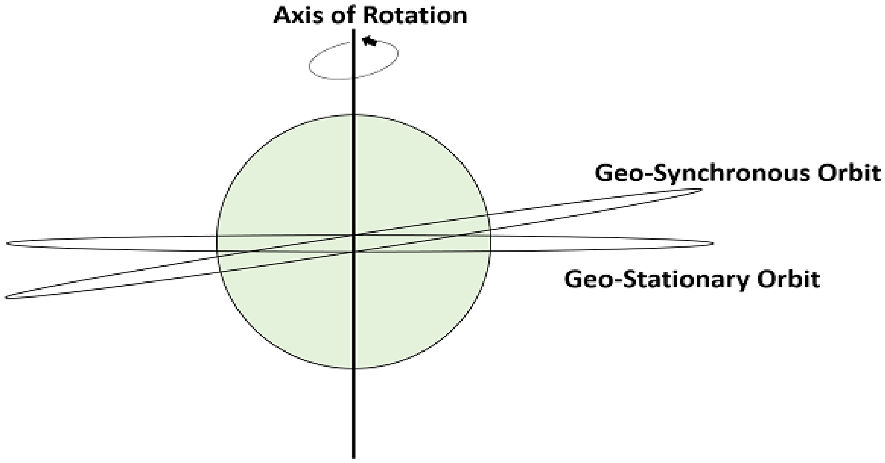
- Geo-synchronous Earth Orbit
- Geo-stationary Earth Orbit
- Medium Earth Orbit
- Low Earth Orbit

Geo-synchronous Earth Orbit (GEO) Satellites

A Geo-synchronous Earth orbit Satellite is one which is placed at an altitude of 22,300 miles above the Earth. This orbit is synchronized with a **side real day** (i.e., 23hours 56minutes). This orbit can **have inclination and eccentricity**. It may not be circular. This orbit can be tilted at the poles of the earth. But it appears stationary when observed from the Earth.

The same geo-synchronous orbit, if it is **circular** and in the plane of equator, it is called as geo-stationary orbit. These Satellites are placed at 35,900kms (same as geosynchronous) above the Earth's Equator and they keep on rotating with respect to earth's direction (west to east). These satellites are considered **stationary** with respect to earth and hence the name implies.

Geo-Stationary Earth Orbit Satellites are used for weather forecasting, satellite TV, satellite radio and other types of global communications.



The above figure shows the difference between Geo-synchronous and Geo- Stationary orbits. The Axis of rotation indicates the movement of Earth.

The main point to note here is that every Geo-Stationary orbit is a Geo-Synchronous orbit. But every Geo-Synchronous orbit is NOT a Geo-stationary orbit.

Medium Earth Orbit (MEO) Satellites

Medium earth orbit (MEO) satellite networks will orbit at distances of about 8000 miles from earth's surface. Signals transmitted from a MEO satellite travel a shorter distance. This translates to improved signal strength at the receiving end. This shows that smaller, more lightweight receiving terminals can be used at the receiving end.

Since the signal is travelling a shorter distance to and from the satellite, there is less transmission delay. **Transmission delay** can be defined as the time it takes for a signal to travel up to a satellite and back down to a receiving station.

For real-time communications, the shorter the transmission delay, the better will be the communication system. As an example, if a GEO satellite requires 0.25 seconds for a round trip, then MEO satellite requires less than 0.1 seconds to complete the same trip. MEOs operates in the frequency range of 2 GHz and above.

Low Earth Orbit (LEO) Satellites

The LEO satellites are mainly classified into three categories namely, little LEOs, big LEOs, and Mega-LEOs. LEOs will orbit at a distance of 500 to 1000 miles above the earth's surface.

This relatively short distance reduces transmission delay to only 0.05 seconds. This further reduces the need for sensitive and bulky receiving equipment. Little LEOs will operate in the 800 MHz (0.8 GHz) range. Big LEOs will operate in the 2 GHz or above range, and Mega-LEOs operates in the 20-30 GHz range.

The higher frequencies associated with **Mega-LEOs** translates into more information carrying capacity and yields to the capability of real-time, low delay video transmission scheme.

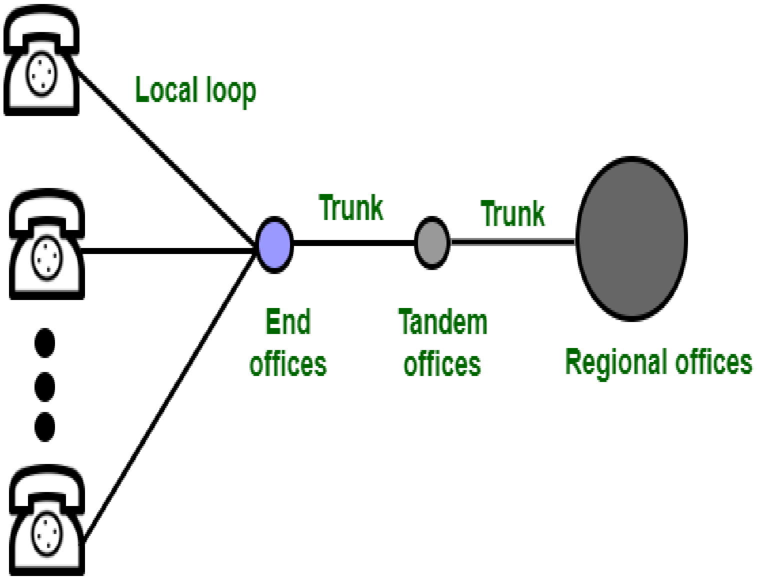
Telephone Network

Telephone Network is used to provide voice communication. Telephone Network uses Circuit Switching. Originally, the entire network was referred to as a plain old telephone system (POTS) which uses analog signals. With the advancement of technology, i.e. in the computer era, there comes a feature to carry data in addition to voice. Today’s network is both analogous and digital.

Major Components of Telephone Network: There are three major components of the telephone network:

1. Local loops
2. Trunks
3. Switching Offices

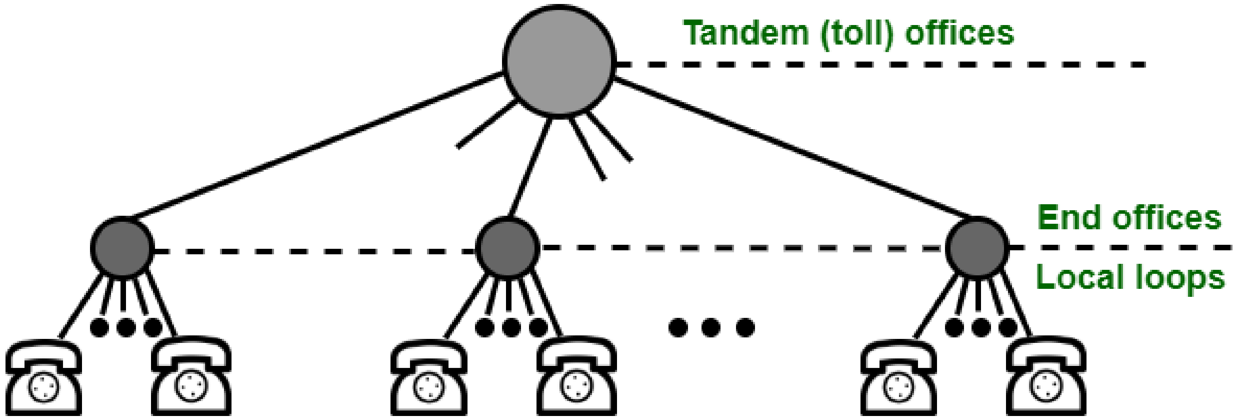
There are various levels of switching offices such as end offices, tandem offices, and regional offices. The entire telephone network is as shown in the following figure:



Local Loops: Local Loops are the twisted pair cables that are used to connect a subscriber telephone to the nearest end office or local central office. For voice purposes, its bandwidth is 4000 Hz. It is very interesting to examine the telephone number that is associated with each local loop. The office is defined by the first three digits and the local loop number is defined by the next four digits defines.

Trunks: It is a type of transmission medium used to handle the communication between offices. Through multiplexing, trunks can handle hundreds or thousands of connections. Mainly transmission is performed through optical fibers or satellite links.

Switching Offices: As there is a permanent physical link between any two subscribers. To avoid this, the telephone company uses switches that are located in switching offices. A switch is able to connect various loops or trunks and allows a connection between different subscribes.



Advantages of Telephone Network:

- It is a circuit-switched network.

- There is no transmission delay as any receiver can be selected.
- It is cheap in price because it is a widely spread network.

Disadvantages of Telephone Network:

- It requires a large time for connection.
- It has a low transmission speed.

Applications of Telephone Network:

- It helps to connect people.
- It is used by business organizations to advertise their products.
- It is also used around the world for recreational purposes.

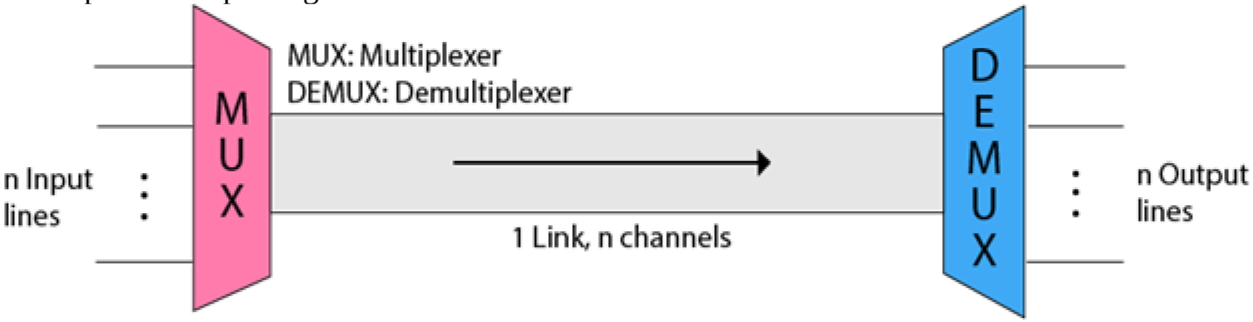
Multiplexing

Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

Demultiplexing is achieved by using a device called Demultiplexer (**DEMUX**) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.

Concept of Multiplexing



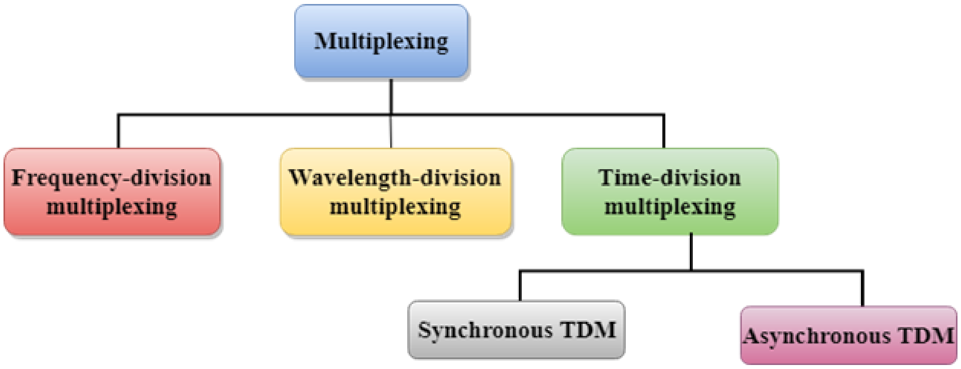
- ○ The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
- ○ The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Advantages of Multiplexing:

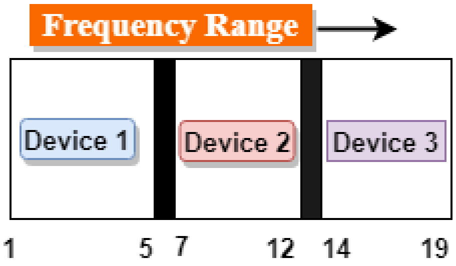
- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.

Multiplexing Techniques

Multiplexing techniques can be classified as:


Multiplexing
Frequency-division multiplexing
Wavelength-division multiplexing
Time-division multiplexing
Synchronous TDM
Asynchronous TDM

Frequency-division Multiplexing (FDM)

- It is an analog technique.
- **Frequency Division Multiplexing** is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.
- 

- In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.
- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.

- The carriers which are used for modulating the signals are known as **sub-carriers**. They are represented as f1,f2..fn.
- **FDM** is mainly used in radio broadcasts and TV networks.

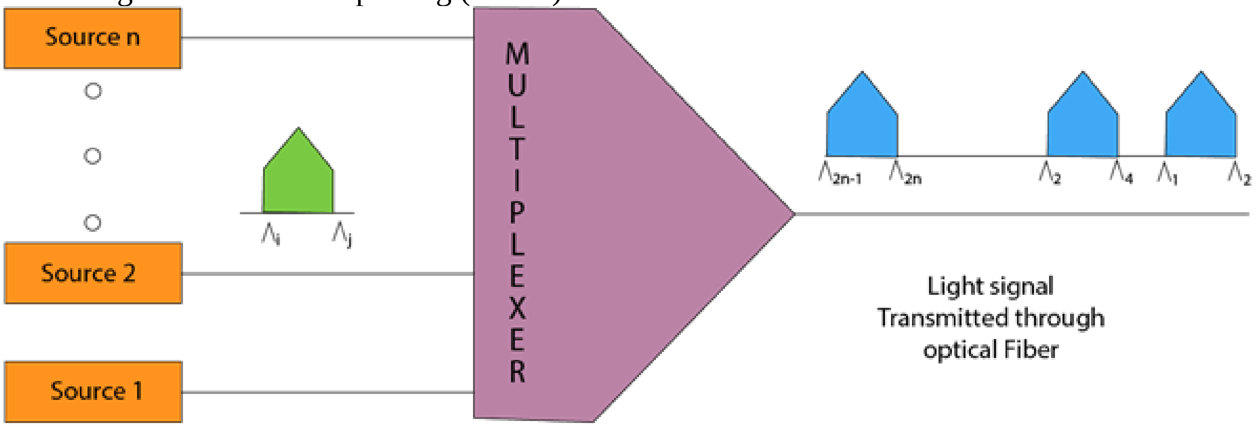
Advantages Of FDM:

- FDM is used for analog signals.
- FDM process is very simple and easy modulation.
- A Large number of signals can be sent through an FDM simultaneously.
- It does not require any synchronization between sender and receiver.

Disadvantages Of FDM:

- FDM technique is used only when low-speed channels are required.
- It suffers the problem of crosstalk.
- A Large number of modulators are required.
- It requires a high bandwidth channel.

Wavelength Division Multiplexing (WDM)



WDM Transmitter

- Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable.
- WDM is used on fibre optics to increase the capacity of a single fibre.
- It is used to utilize the high data rate capability of fibre optic cable.
- It is an analog multiplexing technique.

- Optical signals from different source are combined to form a wider band of light with the help of multiplexer.
- At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.
- Multiplexing and Demultiplexing can be achieved by using a prism.
- Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.
- Prism also performs a reverse operation, i.e., demultiplexing the signal.

Time Division Multiplexing

- It is a digital technique.
- In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.
- In **Time Division Multiplexing technique**, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.
- It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.

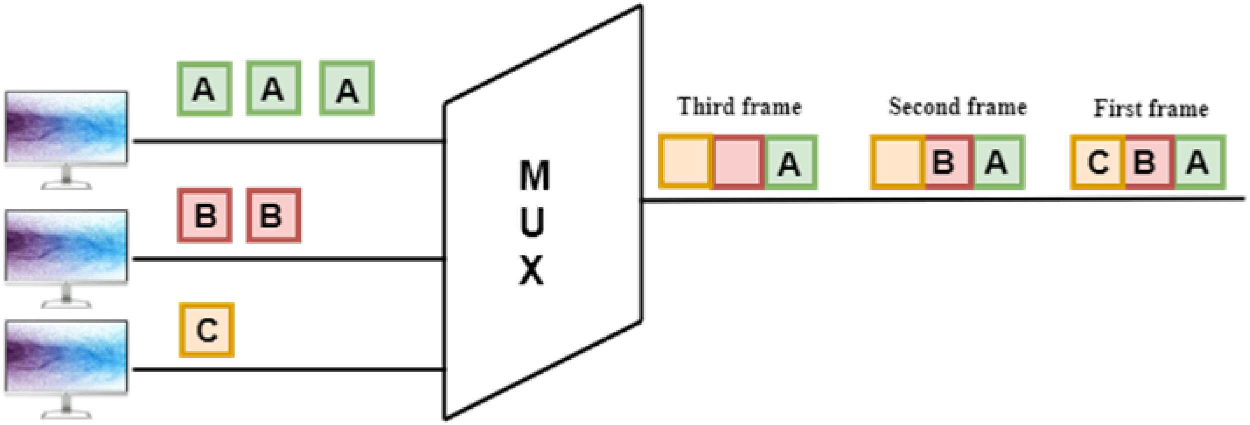
There are two types of TDM:

- Synchronous TDM
- Asynchronous TDM

Synchronous TDM

- A Synchronous TDM is a technique in which time slot is preassigned to every device.
- In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.

- If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.
- The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.
- If there are n devices, then there are n slots.



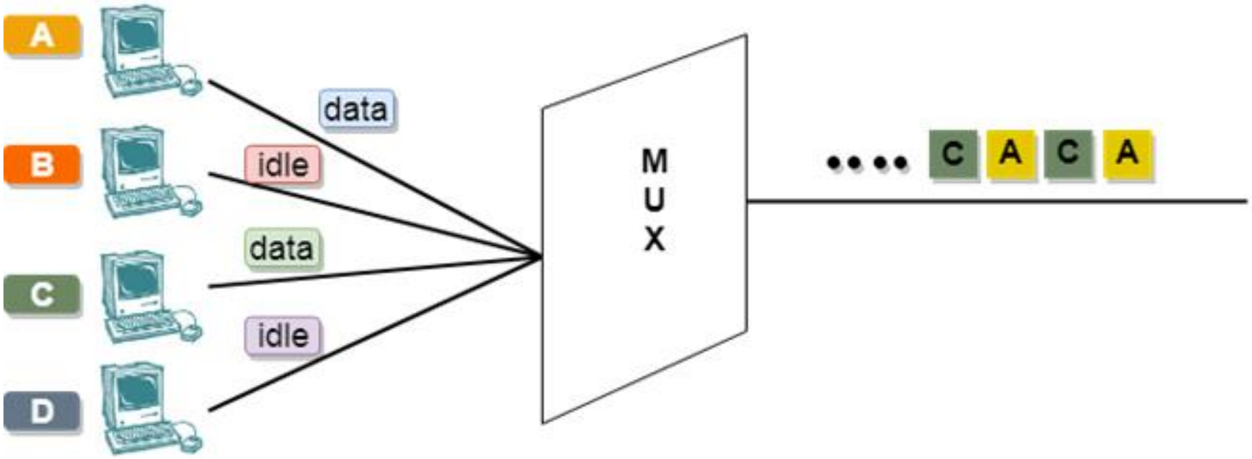
Asynchronous TDM

- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.
- An asynchronous TDM technique dynamically allocates the time slots to the devices.
- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.

ADDRESS	DATA

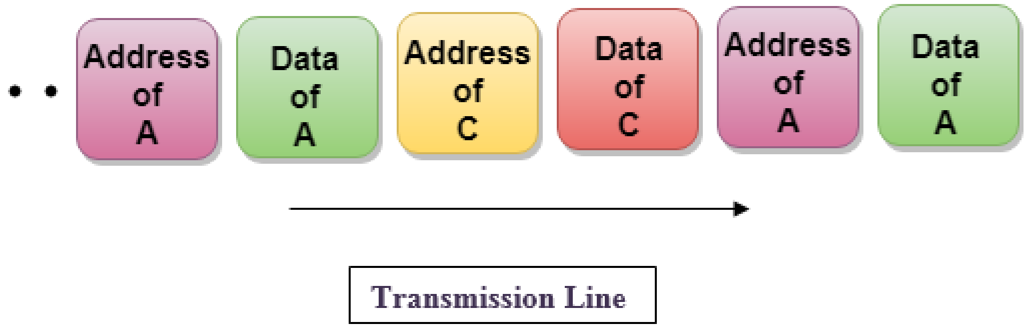
- The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.
- In Synchronous TDM, if there are n sending devices, then there are n time slots. In Asynchronous TDM, if there are n sending devices, then there are m time slots where m is less than n (**m<n**).
- The number of slots in a frame depends on the statistical analysis of the number of input lines.

Concept Of Asynchronous TDM



In the above diagram, there are 4 devices, but only two devices are sending the data, i.e., A and C. Therefore, the data of A and C are only transmitted through the transmission line.

Frame of above diagram can be represented as:



The above figure shows that the data part contains the address to determine the source of the data

Switching

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as **switching**.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.
- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.

Advantages of Switching:

- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

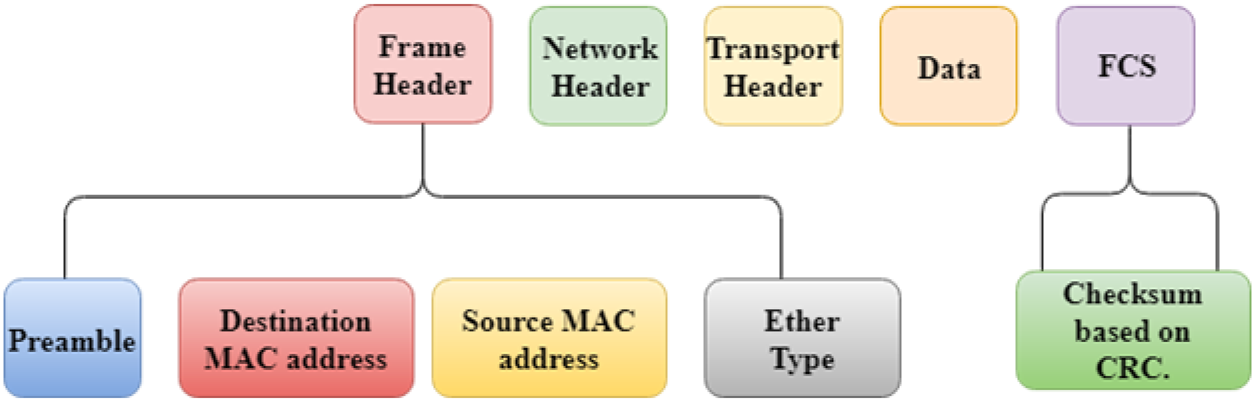
Disadvantages of Switching:

- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

Switching Modes

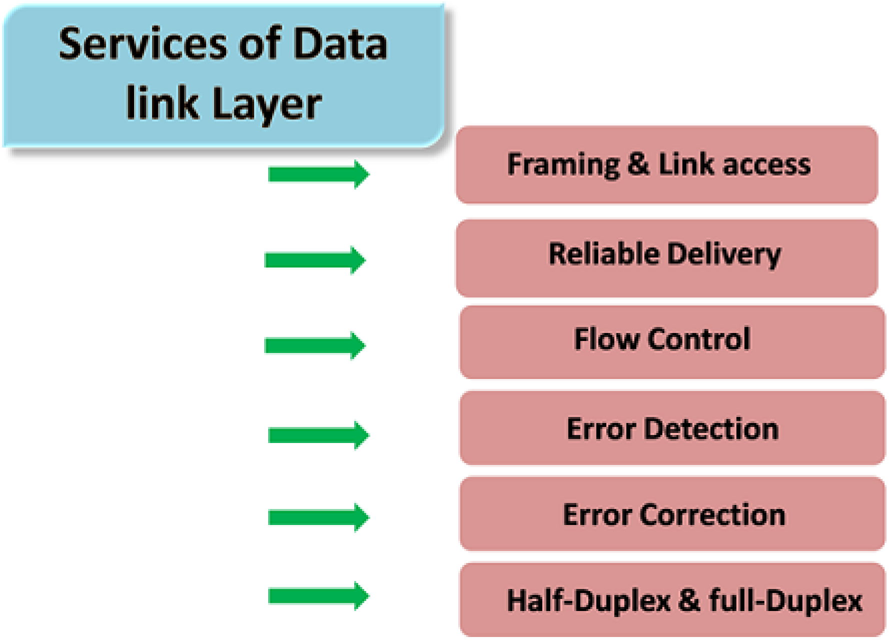
- The layer 2 switches are used for transmitting the data on the data link layer, and it also performs error checking on transmitted and received frames.

- The layer 2 switches forward the packets with the help of MAC address.
- Different modes are used for forwarding the packets known as **Switching modes**.
- In **switching mode**, Different parts of a frame are recognized. The frame consists of several parts such as preamble, destination MAC address, source MAC address, user's data, FCS.



<u>**Data Link Layer**</u>

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



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

- **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

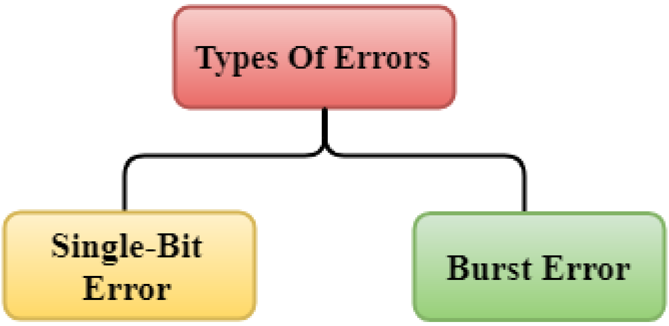
Error Detection&Correction

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

Types Of Errors

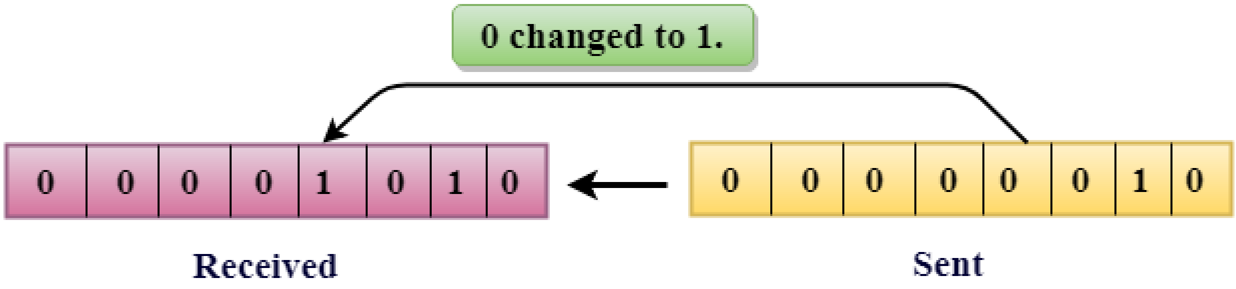
Errors can be classified into two categories:

- Single-Bit Error
- Burst Error



Single-Bit Error:

The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



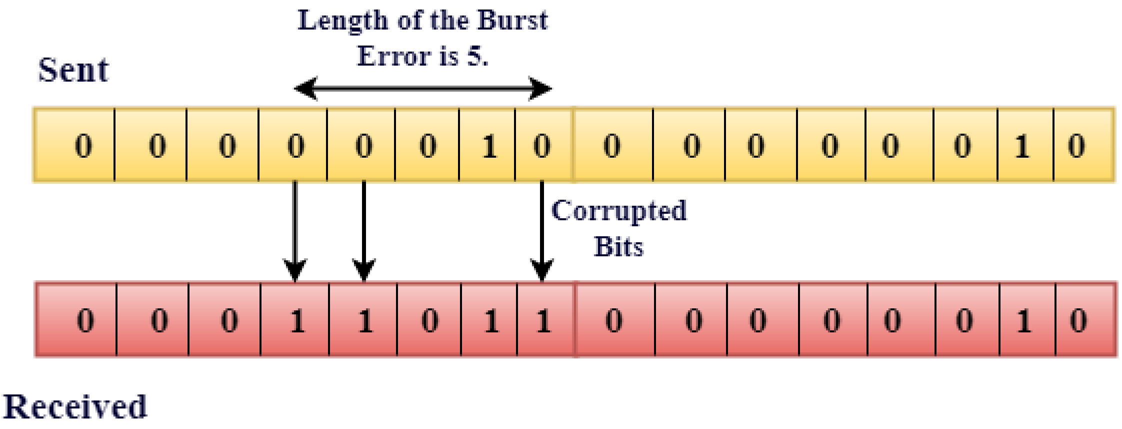
Single-Bit Error does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.

Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.

Burst Error:

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

The Burst Error is determined from the first corrupted bit to the last corrupted bit.



The duration of noise in Burst Error is more than the duration of noise in Single-Bit.

Burst Errors are most likely to occurr in Serial Data Transmission.

The number of affected bits depends on the duration of the noise and data rate.

Error Detecting Techniques:

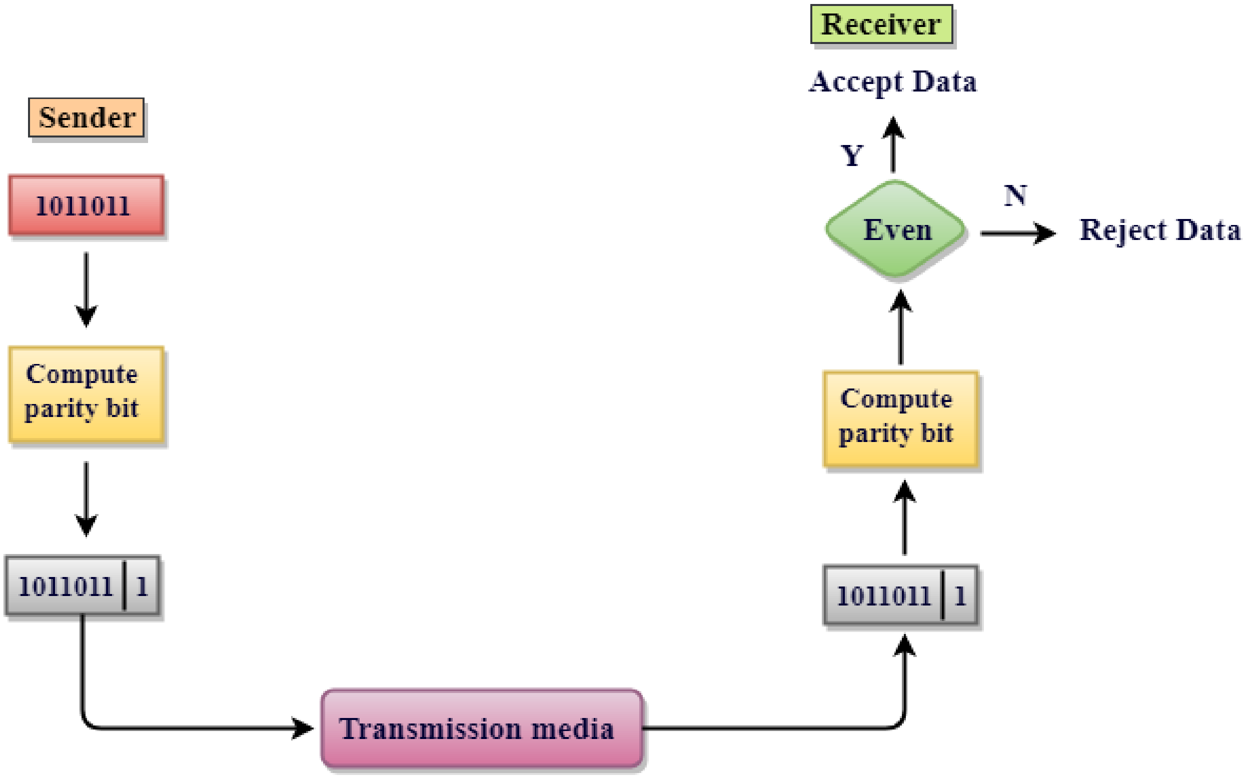
The most popular Error Detecting Techniques are:

- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

Single Parity Check

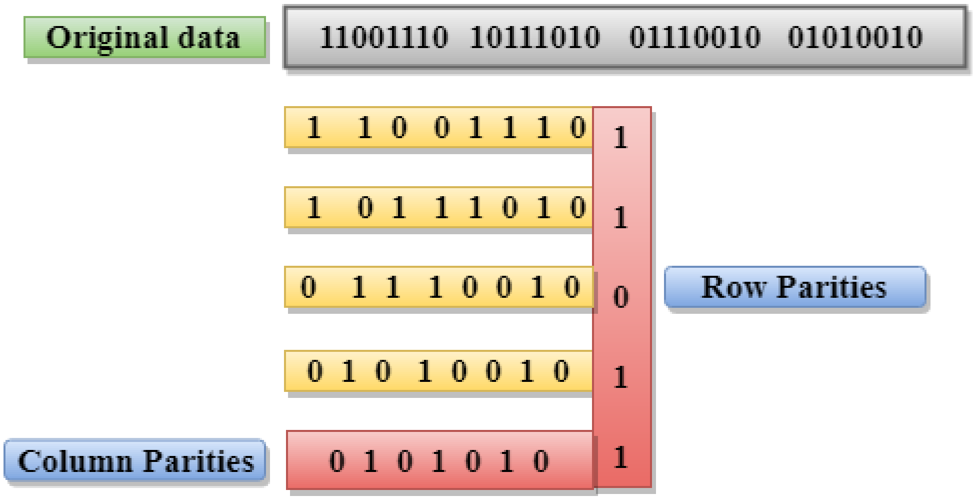
- Single Parity checking is the simple mechanism and inexpensive to detect the errors.
- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.

- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.
- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.
- This technique generates the total number of 1s even, so it is known as even-parity checking.



Two-Dimensional Parity Check

- Performance can be improved by using **Two-Dimensional Parity Check** which organizes the data in the form of a table.
- Parity check bits are computed for each row, which is equivalent to the single-parity check.
- In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block.
- At the receiving end, the parity bits are compared with the parity bits computed from the received data.



Error Correction

In the digital world, error correction can be done in two ways:

- **Backward Error Correction** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection.For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error.

For m data bits, r redundant bits are used. r bits can provide 2r combinations of information. In m+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.

UNIT III

Elementary Data Link Protocols and Sliding Window Protocols

Protocols in the data link layer are designed so that this layer can perform its basic functions: framing, error control and flow control. Framing is the process of dividing bit - streams from physical layer into data frames whose size ranges from a few hundred to a few thousand bytes. Error control mechanisms deals with transmission errors and retransmission of corrupted and lost frames. Flow control regulates speed of delivery and so that a fast sender does not drown a slow receiver.

Elementary Data Link protocols are classified into three categories, as given below −

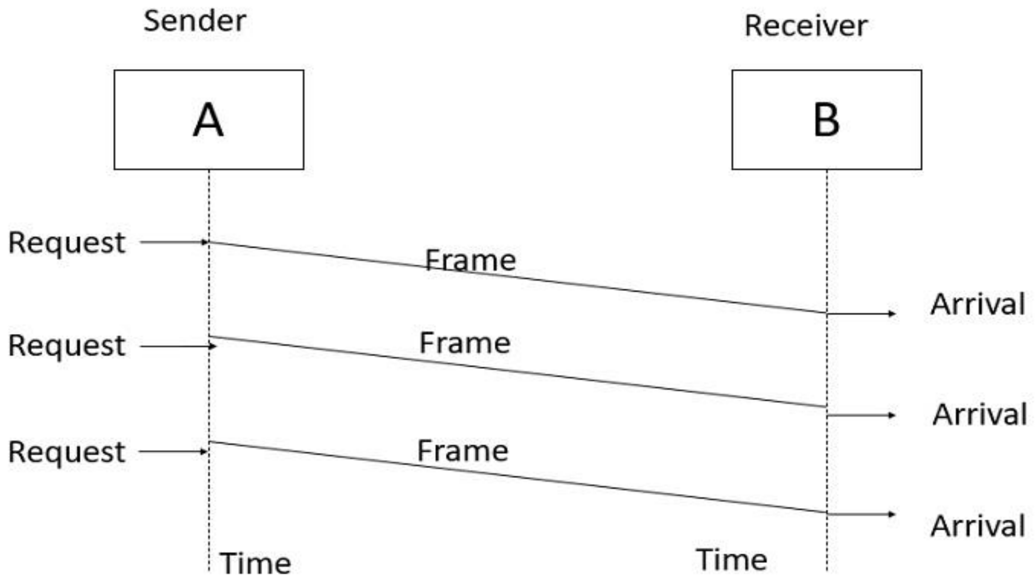
- Protocol 1 − Unrestricted simplex protocol
- Protocol 2 − Simplex stop and wait protocol
- Protocol 3 − Simplex protocol for noisy channels.

Let us discuss each protocol one by one.

Unrestricted Simplex Protocol

Data transmitting is carried out in one direction only. The transmission (Tx) and receiving (Rx) are always ready and the processing time can be ignored. In this protocol, infinite buffer space is available, and no errors are occurring that is no damage frames and no lost frames.

The Unrestricted Simplex Protocol is diagrammatically represented as follows −



Simplex Stop and Wait protocol

In this protocol we assume that data is transmitted in one direction only. No error occurs; the receiver can only process the received information at finite rate. These assumptions imply that the transmitter cannot send frames at rate faster than the receiver can process them.

The main problem here is how to prevent the sender from flooding the receiver. The general solution for this problem is to have the receiver send some sort of feedback to sender, the process is as follows −

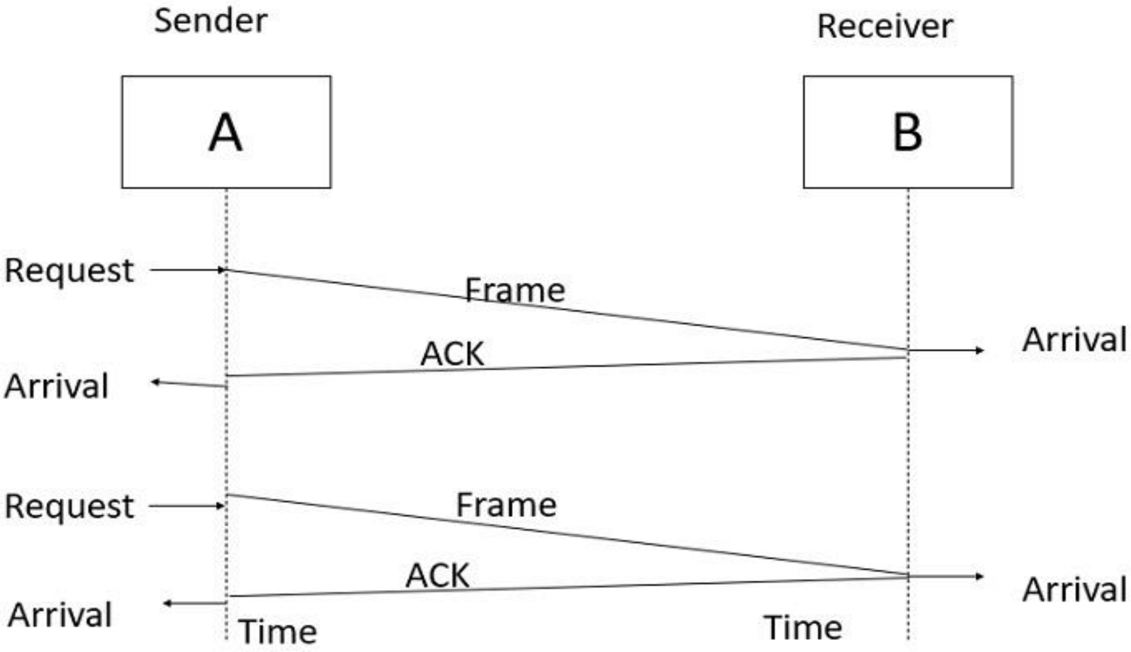
Step1 − The receiver send the acknowledgement frame back to the sender telling the sender that the last received frame has been processed and passed to the host.

Step 2 − Permission to send the next frame is granted.

Step 3 − The sender after sending the sent frame has to wait for an acknowledge frame from the receiver before sending another frame.

This protocol is called Simplex Stop and wait protocol, the sender sends one frame and waits for feedback from the receiver. When the ACK arrives, the sender sends the next frame.

The Simplex Stop and Wait Protocol is diagrammatically represented as follows −

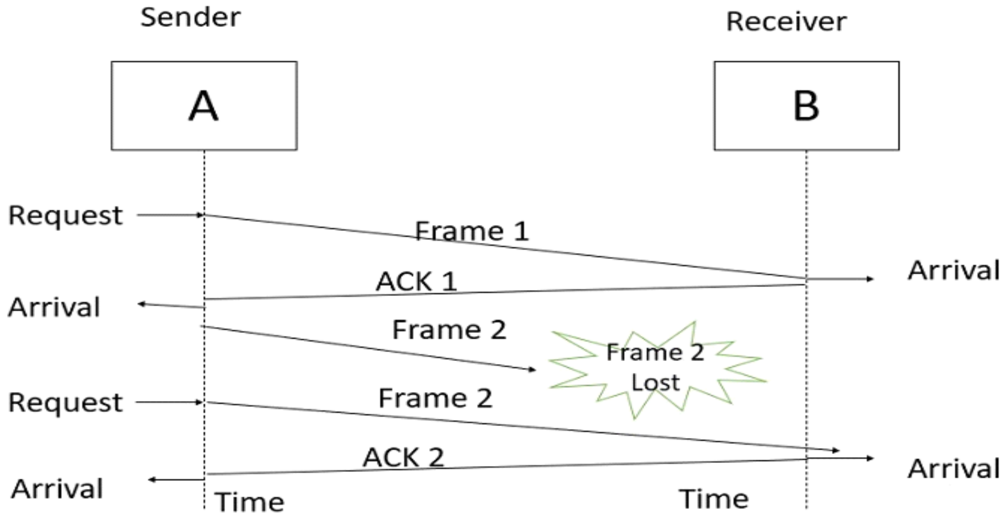


Simplex Protocol for Noisy Channel

Data transfer is only in one direction, consider separate sender and receiver, finite processing capacity and speed at the receiver, since it is a noisy channel, errors in data frames or acknowledgement frames are expected. Every frame has a unique sequence number.

After a frame has been transmitted, the timer is started for a finite time. Before the timer expires, if the acknowledgement is not received , the frame gets retransmitted, when the acknowledgement gets corrupted or sent data frames gets damaged, how long the sender should wait to transmit the next frame is infinite.

The Simplex Protocol for Noisy Channel is diagrammatically represented as follows −



Sliding Window Protocols

- Sliding window protocol is a flow control protocol.
- It allows the sender to send multiple frames before needing the acknowledgements.
- Sender slides its window on receiving the acknowledgements for the sent frames.
- This allows the sender to send more frames.
- It is called so because it involves sliding of sender's window.

Sliding Window

• Sliding window refers to an imaginary boxes that hold the frames on both sender and receiver side.

• It provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgment.

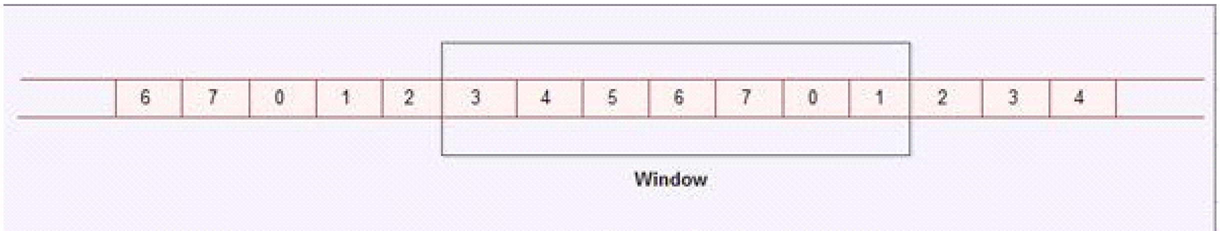
• Frames may be acknowledged by receiver at any point even when window is not full on receiver side.

• Frames may be transmitted by source even when window is not yet full on sender side.

• The windows have a specific size in which the frames are numbered modulo- n, which means they are numbered from 0 to n-l. For e.g. if n = 8, the frames are numbered 0, 1,2,3,4,5,6, 7, 0, 1,2,3,4,5,6, 7, 0, 1, ….

• The size of window is n-1. For e.g. In this case it is 7. Therefore, a maximum of n-l frames may be sent before an acknowledgment.

• When the receiver sends an ACK, it includes the number of next frame it expects to receive. For example in order to acknowledge the group of frames ending in frame 4, the receiver sends an ACK containing the number 5. When sender sees an ACK with number 5, it comes to know that all the frames up to number 4 have been received.



Sliding window

Sliding Window on Sender Side

• At the beginning of a transmission, the sender's window contains n-l frames.

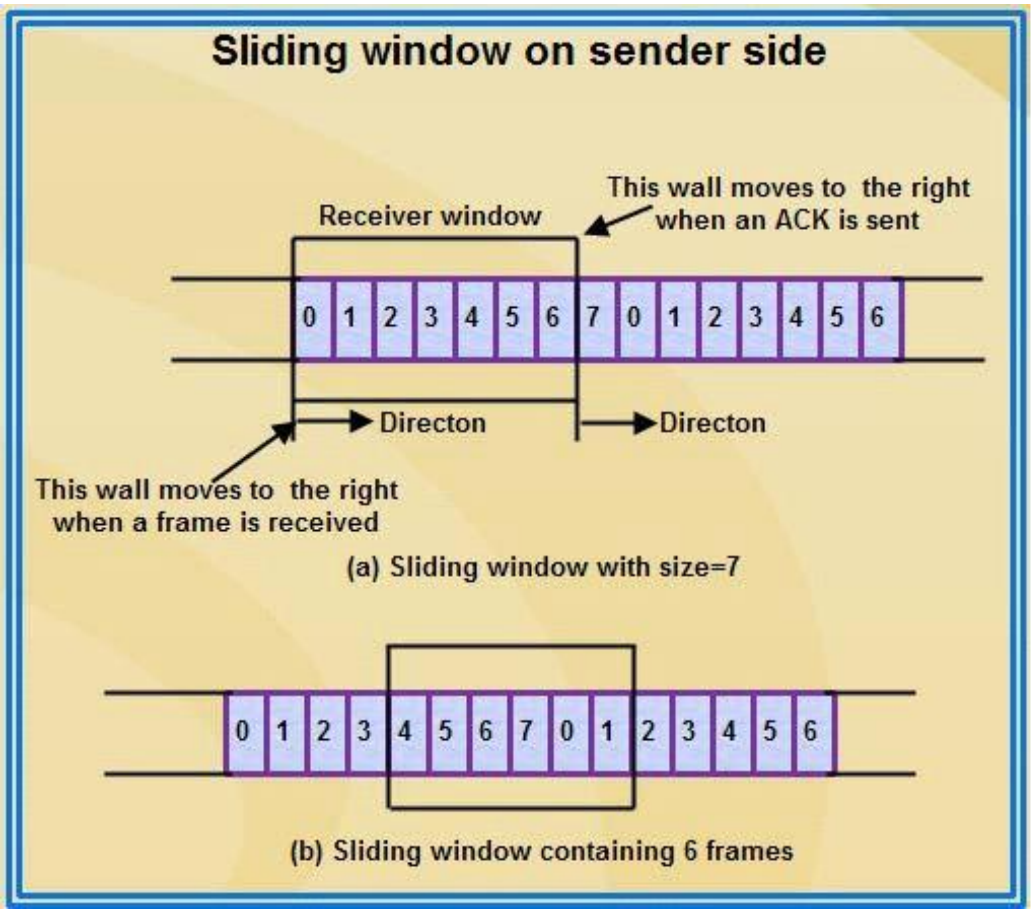
• As the frames are sent by source, the left boundary of the window moves inward, shrinking the size of window. This means if window size is w, if four frames are sent by source after the last acknowledgment, then the number of frames left in window is w-4.

• When the receiver sends an ACK, the source's window expand i.e. (right boundary moves outward) to allow in a number of new frames equal to the number of frames acknowledged by that ACK.

• For example, Let the window size is 7 (see diagram (a)), if frames 0 through 3 have been sent and no acknowledgment has been received, then the sender's window contains three frames – 4,5,6.

• Now, if an ACK numbered 3 is received by source, it means three frames (0, 1, 2) have been received by receiver and are undamaged.

• The sender's window will now expand to include the next three frames in its buffer. At this point the sender's window will contain six frames (4, 5, 6, 7, 0, 1). (See diagram (b)).


Sliding window on sender side
Receiver window
This wall moves to the right when an ACK is sent
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
Directon
Directon
This wall moves to the right when a frame is received
(a) Sliding window with size=7
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
(b) Sliding window containing 6 frames

Sliding Window on Receiver Side

• At the beginning of transmission, the receiver's window contains n-1 spaces for frame but not the frames.

• As the new frames come in, the size of window shrinks.

• Therefore the receiver window represents not the number of frames received but the number of frames that may still be received without an acknowledgment ACK must be sent.

• Given a window of size w, if three frames are received without an ACK being returned, the number of spaces in a window is w-3.

• As soon as acknowledgment is sent, window expands to include the number of frames equal to the number of frames acknowledged.

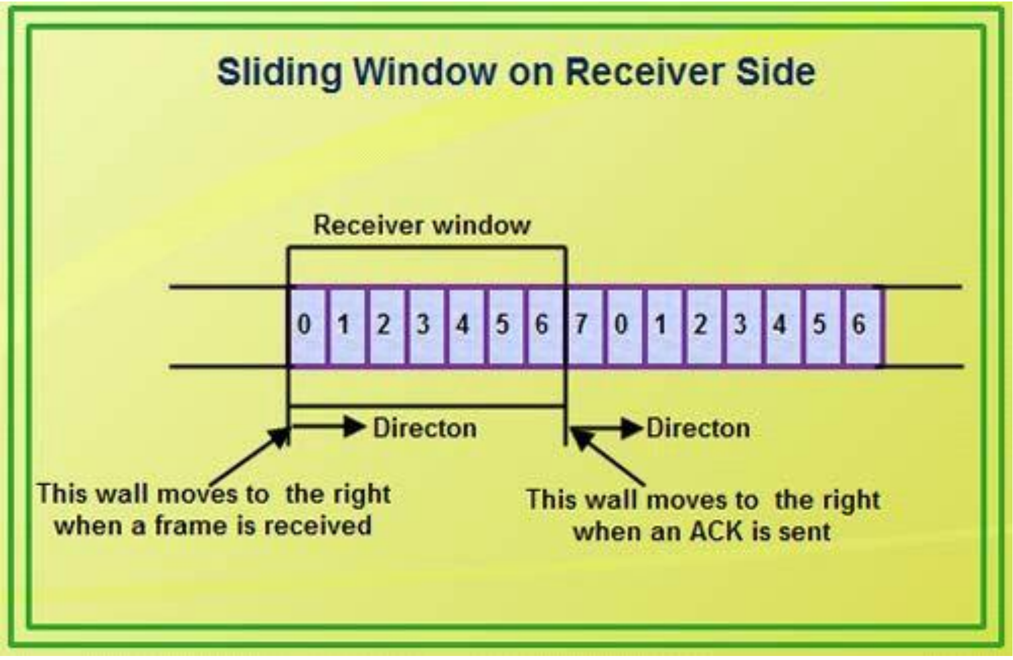
• For example, let the size of receiver's window is 7 as shown in diagram. It means window contains spaces for 7 frames.

• With the arrival of the first frame, the receiving window shrinks, moving the boundary from space 0 to 1. Now, window has shrunk by one, so the receiver may accept six more frame before it is required to send an ACK.

• If frames 0 through 3 have arrived but have DOC been acknowledged, the window will contain three frame spaces.

• As receiver sends an ACK, the window of the receiver expands to include as many new placeholders as newly acknowledged frames.

• The window expands to include a number of new frame spaces equal to the number of the most recently acknowledged frame minus the number of previously acknowledged frame. For *e.g.,* If window size is 7 and if prior ACK was for frame 2 & the current ACK is for frame 5 the window expands by three (5-2).


Sliding Window on Receiver Side
Receiver window
0
1
2
3
4
5
6
7
0
1
2
3
4
5
6
Directon
Directon
This wall moves to the right when a frame is received
This wall moves to the right when an ACK is sent

• Therefore, the sliding window of sender shrinks from left when frames of data are sending. The sliding window of the sender expands to right when acknowledgments are received.

• The sliding window of the receiver shrinks from left when frames of data are received. The sliding window of the receiver expands to the right when acknowledgement is sent.

Medium Access Layer

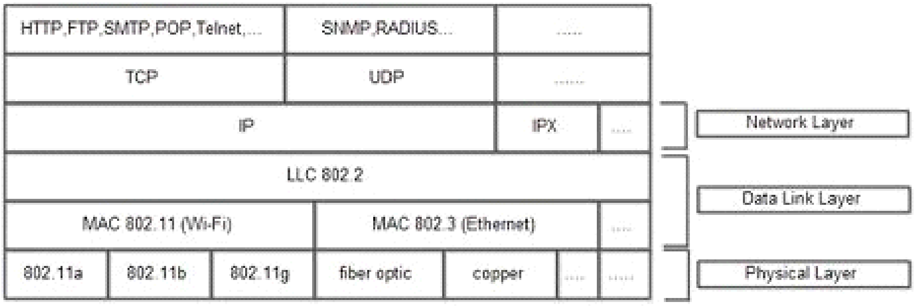
The Media Access Control (MAC) data communication Networks protocol sub-layer, also known as the Medium Access Control, is a sub-layer of the data link layer specified in the seven-layer OSI model. The medium access layer was made necessary by systems that share a common communications medium. Typically these are local area networks. The MAC layer is the “low” part of the second OSI layer, the layer of the “data link”. In fact, the IEEE divided this layer into two layers “above” is the control layer the logical connection (Logical Link Control, LLC) and “down” the control layer The medium access (MAC).

The LLC layer is standardized by the IEEE as the 802.2 since the beginning 1980 Its purpose is to allow level 3 network protocols (for eg IP) to be based on a single layer (the LLC layer) regardless underlying protocol used, including WiFi, Ethernet or Token Ring, for example. All WiFi data packets so carry a pack LLC, which contains itself packets from the upper network layers. The header of a packet LLC indicates the type of layer 3 protocol in it: most of the time, it is IP protocol, but it could be another protocol, such as IPX (Internet Packet Exchange) for example. Thanks to the

LLC layer, it is possible to have at the same time, on the same network, multiple Layer 3 protocols.

In LAN nodes uses the same communication channel for transmission. The MAC sub-layer has two primary responsibilities:

Data encapsulation, including frame assembly before transmission, and frame parsing/error detection during and after reception. Media access control, including initiation of frame transmission and recovery from transmission failure.



Network layers.

Following Protocols are used by Medium Access Layer :

ALOHA : ALOHA is a system for coordinating and arbitrating access to a shared communication channel. It was developed in the 1970s at the University of Hawaii. The original system used terrestrial radio broadcasting, but the system has been implemented in satellite communication systems. A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time.

In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

Carrier Sensed Multiple Access (CSMA) : CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear.

Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it. There are two methods for avoiding these so-called collisions, listed here :

CSMA/CD (Carrier Sense Multiple Access/Collision Detection) : CD (collision detection) defines what happens when two devices sense a clear channel, then attempt to transmit at the same time. A collision occurs, and both devices stop transmission, wait for a random amount of time, and then retransmit. This is the technique used to access the 802.3 Ethernet network channel.

This method handles collisions as they occur, but if the bus is constantly busy, collisions can occur so often that performance drops drastically. It is estimated that network traffic must be less than 40 percent of the bus capacity for the network to operate efficiently. If distances are long, time lags occur that may result in inappropriate carrier sensing, and hence collisions.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) : In CA collision avoidance), collisions are avoided because each node signals its intent to transmit before actually doing so. This method is not popular because it requires excessive overhead that reduces performance.

Ethernet : IEEE 802.3 Local Area Network (LAN) Protocols : Ethernet protocols refer to the family of local-area network (LAN)covered by the IEEE 802.3. In the Ethernet standard, there are two modes of operation: half-duplex and full-duplex modes. In the half duplex mode, data are transmitted using the popular Carrier-Sense Multiple Access/Collision Detection (CSMA/CD) protocol on a shared medium.
The main disadvantages of the half-duplex are the efficiency and distance limitation, in which the link distance is limited by the minimum MAC frame size. This restriction reduces the efficiency drastically for high-rate transmission. Therefore, the carrier extension technique is used to ensure the minimum frame-size of 512 bytes in Gigabit Ethernet to achieve a reasonable link distance. Four data rates are currently defined for operation over optical-fiber and twisted-pair cables :

10 Mbps – 10Base-T Ethernet (IEEE 802.3)
100 Mbps – Fast Ethernet (IEEE 802.3u)
1000 Mbps – Gigabit Ethernet (IEEE 802.3z)
10-Gigabit – 10 Gbps Ethernet (IEEE 802.3ae).

The **Ethernet System** consists of three basic elements :

(1) The physical medium used to carry Ethernet signals between computers,

(2) a set of medium access control rules embedded in each Ethernet interface that allow multiple computers to fairly arbitrate access to the shared Ethernet channel, and

(3) an Ethernet frame that consists of a standardized set of bits used to carry data over the system.

As with all IEEE 802 protocols, the ISO data link layer is divided into two IEEE 802 sub-layers, the Media Access Control (MAC) sub-layer and the MAC-client sub-layer. The IEEE 802.3 physical layer corresponds to the ISO physical layer.

Each Ethernet-equipped computer operates independently of all other stations on the network: there is no central controller. All stations attached to an Ethernet are connected to a shared signalling system, also called the medium. To send data a station first listens to the channel, and when the channel is idle the station transmits its data in the form of an Ethernet frame, or packet.

After each frame transmission, all stations on the network must contend equally for the next frame transmission opportunity. Access to the shared channel is determined by the medium access control (MAC) mechanism embedded in the Ethernet interface located in each station. The medium access control mechanism is based on a system called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

As each Ethernet frame is sent onto the shared signal channel, all Ethernet interfaces look at the destination address. If the destination address of the frame matches with the interface address, the frame will be read entirely and be delivered to the networking software running on that computer. All other network interfaces will stop reading the frame when they discover that the destination address does not match their own address.

IEEE 802.4 Token Bus : In token bus network station must have possession of a token before it can transmit on the network. The IEEE 802.4 Committee has defined token bus standards as broadband networks, as opposed to Ethernet's baseband transmission technique. The topology of the network can include groups of workstations connected by long trunk cables.

These workstations branch from hubs in a star configuration, so the network has both a bus and star topology. Token bus topology is well suited to groups of users that are separated by some distance. IEEE 802.4 token bus networks are constructed with 75-ohm coaxial cable using a bus topology. The broadband characteristics of the 802.4 standard support transmission over several different channels simultaneously.

The token and frames of data are passed from one station to another following the numeric sequence of the station addresses. Thus, the token follows a logical ring rather than a physical ring. The last station in numeric order passes the token back to the first station. The token does not follow the physical ordering of workstation attachment to the cable. Station 1 might be at one end of the cable and station 2 might be at the other, with station 3 in the middle.

While token bus is used in some manufacturing environments, Ethernet and token ring standards have become more prominent in the office environment.

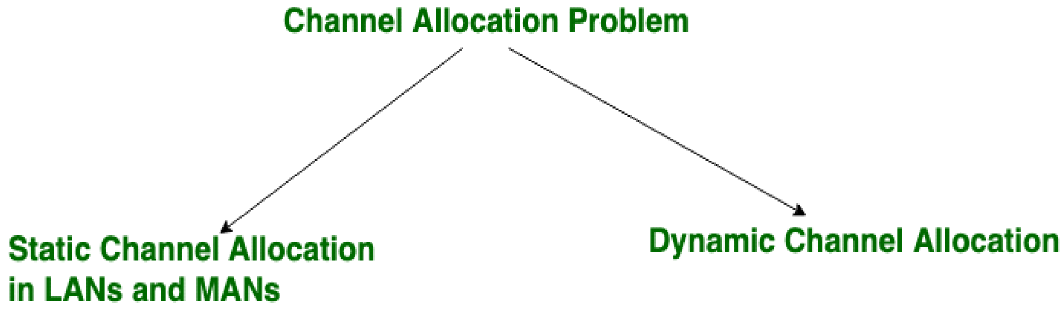
IEEE 802.5 Token Ring : Token ring is the IEEE 802.5 standard for a token-passing ring network with a star-configured physical topology. Internally, signals travel around the network from one station to the next in a ring. Physically, each station connects to a central hub called a MAU (multi-station access unit). The MAU contains a "collapsed ring," but the physical configuration is a star topology. When a station is attached, the ring is extended out to the station and then back to the MAU .

If a station goes offline, the ring is re established with a bypass at the station connector. Token ring was popular for an extended period in the late 1980s and 1990s, especially in IBM legacy system environments. IBM developed the technology and provided extensive support for connections to SNA systems. More recently, Ethernet, Fast Ethernet, and Gigabit Ethernet technologies have pushed token ring and other LAN technologies to the sidelines.

Channel Allocation Problem

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place. If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, than Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.

Channel allocation problem can be solved by two schemes: Static Channel Allocation in LANs and MANs, and Dynamic Channel Allocation.


Channel Allocation Problem
Static Channel Allocation in LANs and MANs
Dynamic Channel Allocation

1. Static Channel Allocation in LANs and MANs:
It is the classical or traditional approach of allocating a single channel among multiple competing users Frequency Division Multiplexing (FDM). if there are N users, the bandwidth is divided into N equal sized portions each user being assigned one portion. since each user has a private frequency band, there is no interface between users.
It is not efficient to divide into fixed number of chunks.

T = 1/(U*C-L)

T(FDM) = N*T(1/U(C/N)-L/N)
Where,

T = mean time delay,
C = capacity of channel,
L = arrival rate of frames,
1/U = bits/frame,
N = number of sub channels,
T(FDM) = Frequency Division Multiplexing Time

2. Dynamic Channel Allocation:
Possible assumptions include:

- **Station Model:**
  Assumes that each of N stations independently produce frames. The probability of producing a packet in the interval IDt where I is the constant arrival rate of new frames.

- **Single Channel Assumption:**
  In this allocation all stations are equivalent and can send and receive on that channel.

- **Collision Assumption:**
  If two frames overlap in time-wise, then that’s collision. Any collision is an error, and

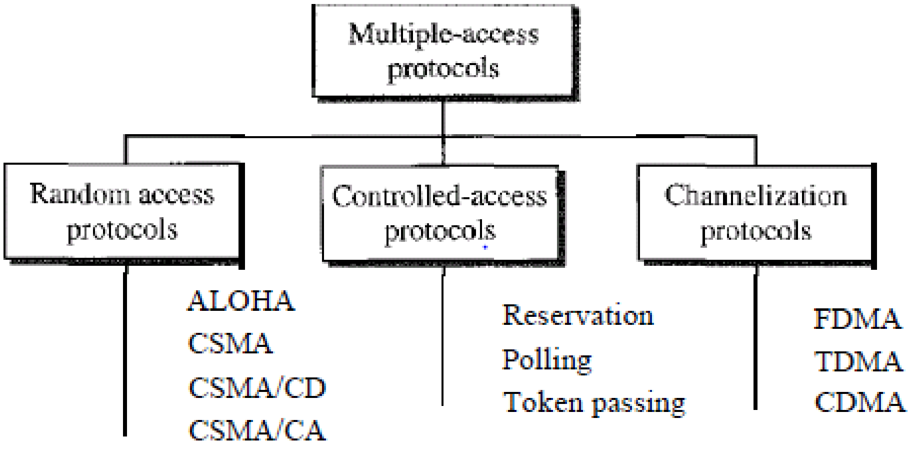
both frames must re transmitted. Collisions are only possible error.

- **Time** can be divided into Slotted or Continuous.
- **Stations** can sense a channel is busy before they try it.

Protocol Assumption:

- N independent stations.
- A station is blocked until its generated frame is transmitted.
- probability of a frame being generated in a period of length Dt is IDt where I is the arrival rate of frames.
- Only a single Channel available.
- Time can be either: Continuous or slotted.
- **Carrier Sense:** A station can sense if a channel is already busy before transmission.
- **No Carrier Sense:** Time out used to sense loss data.

Multiple Access Protocols



1. RANDOM ACCESS:

- In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.
- This decision depends on the state of the medium (idle or busy).Two features give this method its name. First, there is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called random access. Second, no rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called contention methods

ALOHA

This random access method, was developed at the University of Hawaiiin early 1970. It was designed for a radio (wireless) LAN, but it can be used on any shared medium. It is obvious that there are potential collisions in this arrangement. The medium is shared between the stations. When a station sends data, another station may attempt todo so at the same time. The data from the two stations collide and become garbled.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- The problem with CSMA is that transmitting station continues to transmit its frame even though a collision occurs.
- The channel time is unnecessarily wasted due to this. In CSMA/CD, if a station receives other transmissions when it is transmitting, then a collision can be detected as soon as it occurs and the transmission time is saved.
- As soon as a collision is detected, the transmitting stations release a jam signal.
- The jam signal will alert the other stations. The stations then are not supposed to transmit immediately after the collision has occurred. Otherwise there is possibility that the same frames would collide again.
- After some ―back off‖ delay time the stations will retry the transmission. If again the collision takes place then the back off time is increased progressively.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- In a wired network, the received signal has almost the same energy as the sent signal because either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver. This means that in a collision, the detected energy almost doubles.
- However, in a wireless network, much of the sent energy is lost in transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10% additional energy. This is not useful for effective collision detection. We need to avoid collisions on wireless networks because they cannot be detected.
- Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for this network. Collisions are avoided through the use of CSMAICA's three strategies: the interframespace, the contention window, and acknowledgments

2. CONTROLLED ACCESS

Controlled Access

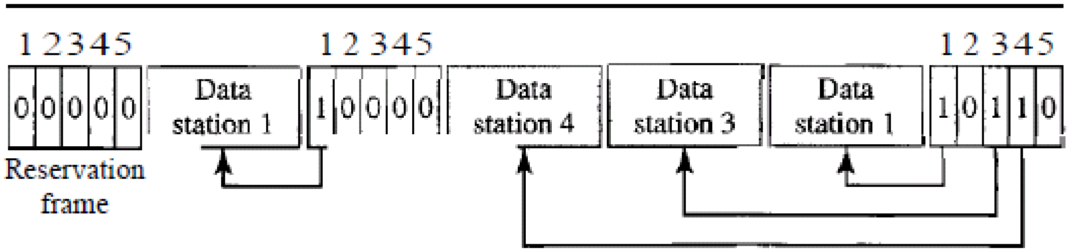
In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. We discuss three popular controlled-access methods.

Reservation

In the reservation method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval. If there are N stations in the system, there are exactly N reservation minislots in the reservation frame.

Each minislot belongs to a station. When a station needs to send a data frame, it makes a reservation in its own minislot.

The stations that have made reservations can send their data frames after the reservation frame. Figure below shows a situation with five stations and a five-minislot 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 works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.

The primary device controls the link; the secondary devices follow its instructions. It is up to the primary device to determine which device is allowed to use the channel at a given time. The primary device, therefore, is always the initiator of a session

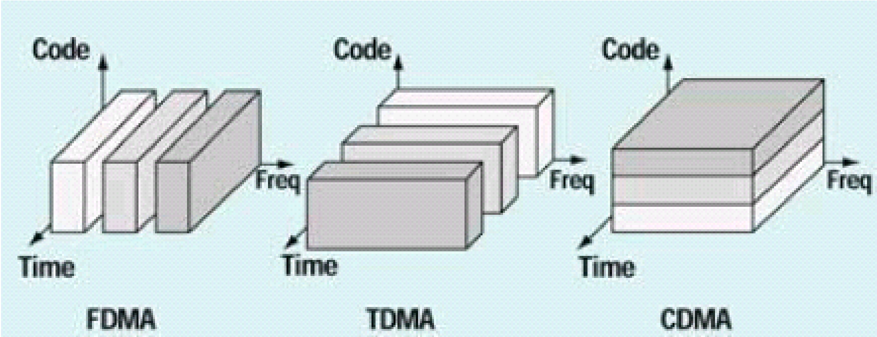
If the primary wants to receive data, it asks the secondary‘s if they have anything to send; this is called poll function. If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function.

Token Passing:

- In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a predecessor and a successor. The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring.
- The current station is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.
- Token management is needed for this access method. Stations must be limited in the time they can have possession of the token. The token must be monitored to ensure it has not been lost or destroyed.
- For example, if a station that is holding the token fails, the token will disappear from the network. Another function of token management is to assign priorities to the stations and to the types of data being transmitted. And finally, token management is needed to make low-priority stations release the token to high priority stations.

3. CHANNELIZATION

Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations. Three channelization protocols: FDMA, TDMA, and CDMA.



FDMA: In frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data. In other words, each band is reserved for a specific station, and it belongs to the station all the time. Each station also uses a bandpass filter to confine the transmitter frequencies. To prevent station interferences, the allocated bands are separated from one another by small guard bands.

TDMA: In time-division multiple access (TDMA), the stations share the bandwidth of the channel in time. Each station is allocated a time slot during which it can send data. Each station transmits its data in is assigned time slot.

CDMA:

- In CDMA each user is given a unique code sequence or signature sequence. This sequence allows the user to spread information signal across the assigned frequency band.
- At the receiver the signal is recovered by using the same code sequence. At the receiver, the signals received from various users are separated by checking the cross-correlation of the received signal with each possible user signature sequence.
- In CDMA the users access the channel in a random manner. Hence the signals transmitted by multiple users will completely overlap both in time and in frequency.
- The CDMA signals are spread in frequency. Therefore the demodulation and separation of these signals at the receiver can be achieved by using the pseudorandom code sequence. CDMA is sometimes also called as spread spectrum multiple access (SSMA).
- In CDMA as the bandwidth as well as time of the channel is being shared by the users, it is necessary to introduce the guard times and guard bands.
- CDMA does not any synchronization, but the code sequences or signature waveforms are required.

Bluetooth

• Bluetooth is, with the infrared, one of the major wireless technologies developed to achieve WPAN.

Bluetooth is a wireless LAN technology used to connect devices of different functions such as telephones, computers (laptop or desktop), notebooks, cameras, printers and so on. Bluetooth is an example of personal area network.

- Bluetooth project was started by SIG (Special Interest Group) formed by four companies IBM, Intel, Nokia and Toshiba for interconnecting computing and communicating devices using short-range, lower-power, inexpensive wireless radios.

- The project was named Bluetooth after the name of Viking king – Harald Blaat and who unified Denmark and Norway in 10th century.

- Nowadays, Bluetooth technology is used for several computer and non computer application.

1. It is used for providing communication between peripheral devices like wireless mouse or keyboard with the computer.
2. It is used by modern healthcare devices to send signals to monitors.
3. It is used by modern communicating devices like mobile phone, PDAs, palmtops etc to transfer data rapidly.
4. It is used for dial up networking. Thus allowing a notebook computer to call via a mobile phone.
5. It is used for cordless telephoning to connect a handset and its local base station.
6. It also allows hands-free voice comml1nication with headset.
7. It also enables a mobile computer to connect to a fixed LAN.
8. It can also be used for file transfer operations from one mobile phone to another.
9. Bluetooth uses omni directional radio waves that can through walls or other non-metal barriers.

Bluetooth devices have a built-in short range radio transmitter. The rate provided is 1Mbps and uses 2.4 GHz bandwidth.

Bluetooth is that when the device is with in the scope of a other devices automatically start the transfer information without the user noticing. a small network between the devices is created and the user can accessed as if there were cables.

Bluetooth Architecture

Bluetooth architecture defines two types of networks:

1. Piconet

2. Scattemet

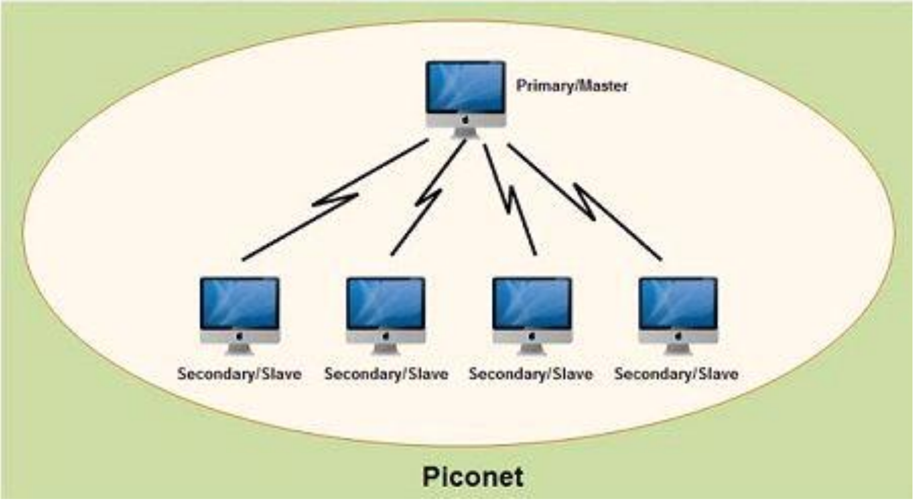
1. Piconet

- Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.

- Thus, piconet can have up to eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.

- There can be only one primary or master station in each piconet.

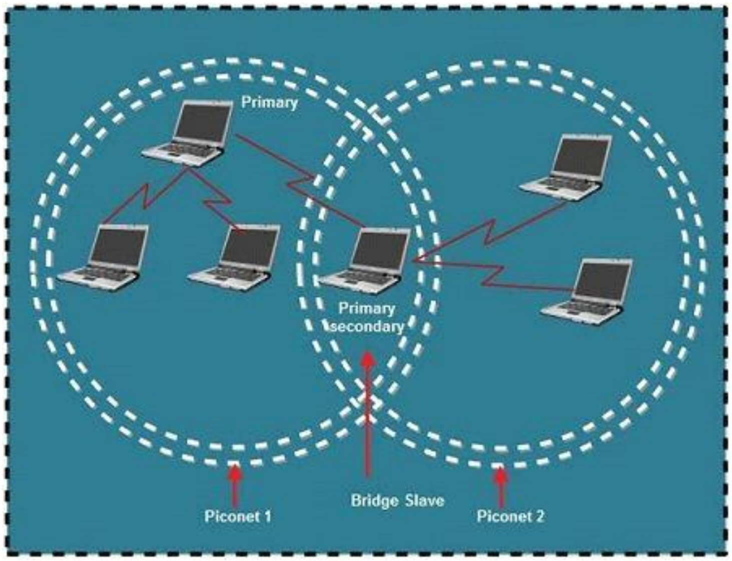
- The communication between the primary and the secondary can be one-to-one or one-to-many.



- All communication is between master and a slave. Salve-slave communication is not possible.
- In addition to seven active slave station, a piconet can have up to 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.

2. Scatternet

- Scattemet is formed by combining various piconets.
- A slave in one piconet can act as a master or primary in other piconet.
- Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave.
- Thus a station can be a member of two piconets.
- A station cannot be a master in two piconets.

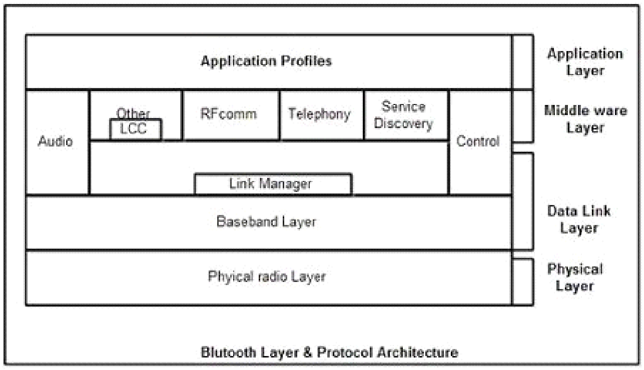


Bluetooth layers and Protocol Stack

• Bluetooth standard has many protocols that are organized into different layers.

• The layer structure of Bluetooth does not follow OS1 model, TCP/IP model or any other known model.

• The different layers Bluetooth protocol architecture



Blutooth Layer & Protocol Architecture

UNIT - IV

Network Layer

Network layer is majorly focused on getting packets from the source to the destination, routing error handling and congestion control.

- **Addressing:**
  Maintains the address at the frame header of both source and destination and performs addressing to detect various devices in network.
- **Packeting:**
  This is performed by Internet Protocol. The network layer converts the packets from its upper layer.

- **Routing:**
  It is the most important functionality. The network layer chooses the most relevant and best path for the data transmission from source to destination.
- **Inter-networking:**
  It works to deliver a logical connection across multiple devices.
-

Network layer design issues:
The network layer comes with some design issues they are described as follows:
1. Store and Forward packet switching:
The host sends the packet to the nearest router. This packet is stored there until it has fully arrived once the link is fully processed by verifying the checksum then it is forwarded to the next router till it reaches the destination. This mechanism is called "Store and Forward packet switching."

2. Services provided to Transport Layer:
Through the network/transport layer interface, the network layer transfers it's services to the transport layer. These services are described below.
But before providing these services to the transfer layer following goals must be kept in mind :-

- Offering services must not depend on router technology.
- The transport layer needs to be protected from the type, number and topology of the available router.
- The network addresses for the transport layer should use uniform numbering pattern also at LAN and WAN connections.

Based on the connections there are 2 types of services provided :

- **Connectionless –** The routing and insertion of packets into subnet is done individually. No added setup is required.
- **Connection-Oriented –** Subnet must offer reliable service and all the packets must be transmitted over a single route.

3. Implementation of Connectionless Service:
Packet are termed as "datagrams" and corresponding subnet as "datagram subnets". When the message size that has to be transmitted is 4 times the size of the packet, then the network layer divides into 4 packets and transmits each packet to router via. a few protocol. Each data packet has destination address and is routed independently irrespective of the packets.
4. Implementation of Connection Oriented service:
To use a connection-oriented service, first we establishes a connection, use it and then release it. In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender.
It can be done in either two ways :

- **Circuit Switched Connection –** A dedicated physical path or a circuit is established between the communicating nodes and then data stream is transferred.
- **Virtual Circuit Switched Connection –** The data stream is transferred over a packet switched network, in such a way that it seems to the user that there is a dedicated path from the sender to the receiver. A virtual path is established here. While, other connections may also be using the same path.

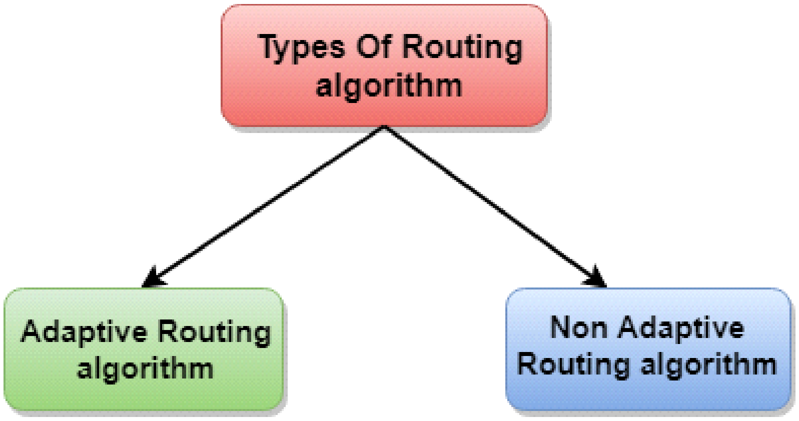
Routing Algorithms

- 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.

Classification of a Routing algorithm

The Routing algorithm is divided into two categories:

- Adaptive Routing algorithm
- Non-adaptive Routing algorithm


Types Of Routing algorithm
Adaptive Routing algorithm
Non Adaptive Routing algorithm

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.

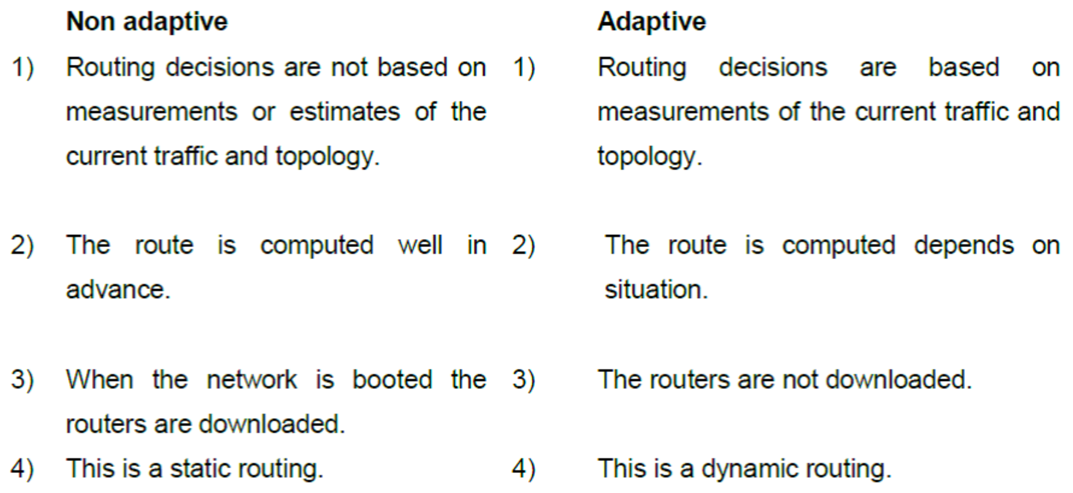
Non-Adaptive Routing algorithm

- 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.

The Non-Adaptive Routing algorithm is of two types:

Flooding: In case of flooding, every incoming packet is sent to all the outgoing links except the one from it has been reached. The disadvantage of flooding is that node may contain several copies of a particular packet.

Random walks: In case of random walks, a packet sent by the node to one of its neighbors randomly. An advantage of using random walks is that it uses the alternative routes very efficiently.



	Non adaptive		Adaptive
1)	Routing decisions are not based on measurements or estimates of the current traffic and topology.	1)	Routing decisions are based on measurements of the current traffic and topology.
2)	The route is computed well in advance.	2)	The route is computed depends on situation.
3)	When the network is booted the routers are downloaded.	3)	The routers are not downloaded.
4)	This is a static routing.	4)	This is a dynamic routing.

Distance Vector Routing: Distance vector algorithms use the Bellman- Ford algorithm. Distance vector algorithms are examples of dynamic routing protocols. Algorithms allow each device in the network to automatically build and maintain a local routing table or matrix.Routing table contains list of destinations, the total cost to each, and the next hop to send data to get there. This approach assigns a number, the cost, to each of the links between each node in the network. Nodes will send information from point A to point B via the path that results in the lowest total cost i.e. the sum of the costs of the links between the nodes used.The algorithm operates in a very simple manner. When a node first starts, it only knows of its immediate neighbours, and the direct cost involved in reaching them. The routing table from the each node, on a regular basis, sends its own information to each neighbouring node with current idea of the total cost to get to all the destinations it knows of.The neighboring node(s) examine this information, and compare it to what they already ‘know’; anything which represents an improvement on what they already have, they insert in their own routing table(s). Over time, all the nodes in the network will discover the best next hop for all destinations, and the best total cost. The main advantage of distance vector algorithms is that they are typically easy to implement and debug. They are very useful in small networks with limited redundancy. When one of the nodes involved goes down, those nodes which used it as their next hop for certain destinations discard those entries, and create new routing-table information.

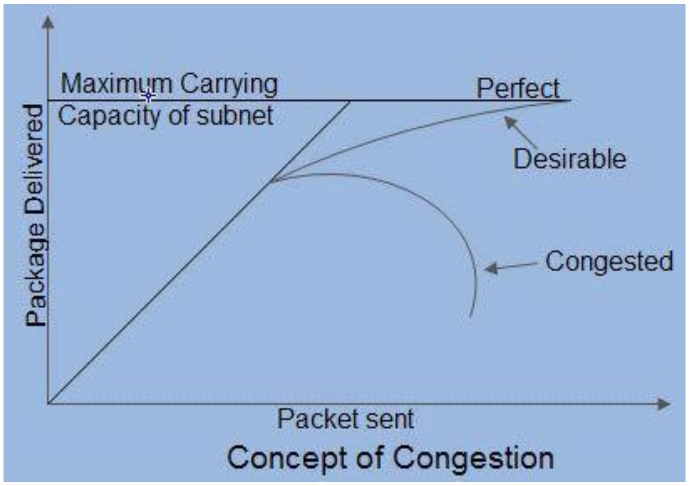
They then pass this information to all adjacent nodes, which then repeat the process. Eventually all the nodes in the network receive the updated information, and will then discover new paths to all the destinations which they can still “reach”.

Link State Routing : A link state is the description of an interface on a router and its relationship to neighboring routers. When applying link-state algorithms, each node uses as its fundamental data a map of the network in the form of a graph.

To produce this, each node floods the entire network with information about what other nodes it can connect to, and each node then independently assembles this information into a map. Using this map, each router then independently determines the least-cost path from itself to every other node using a standard shortest paths algorithm such as Dijkstra’s algorithm.The result is a tree rooted at the current node such that the path through the tree from the root to any other node is the least-cost path to that node. This tree then serves to construct the routing table, which specifies the best next hop to get from the current node to any other node.

Congestion Control Algorithms

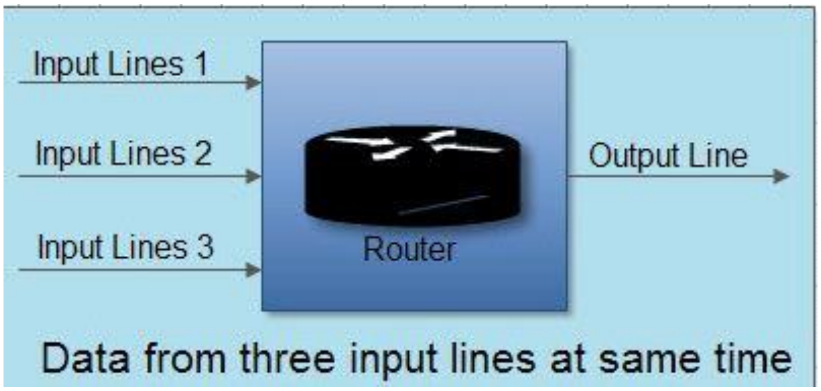
Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades. Congestion in a network may occur when the load on the network *(i.e.* the number of packets sent to the network) is greater than the capacity of the network *(i.e.* the number of packets a network can handle.). Network congestion occurs in case of traffic overloading.In other words when too much traffic is offered, congestion sets in and performance degrades sharply



Causing of Congestion:

The various causes of congestion in a subnet are:

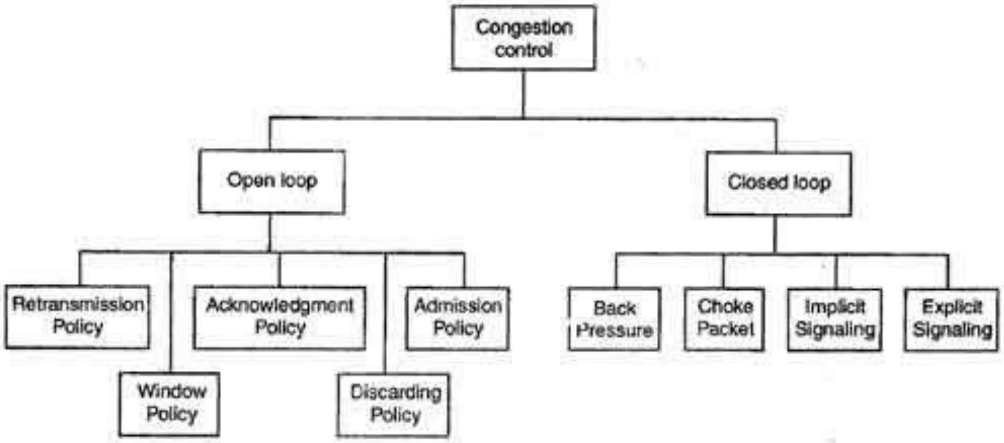
• The input traffic rate exceeds the capacity of the output lines. If suddenly, a stream of packet start arriving on three or four input lines and all need the same output line. In this case, a queue will be built up. If there is insufficient memory to hold all the packets, the packet will be lost. Increasing the memory to unlimited size does not solve the problem. This is because, by the time packets reach front of the queue, they have already timed out (as they waited the queue). When timer goes off source transmits duplicate packet that are also added to the queue. Thus same packets are added again and again, increasing the load all the way to the destination.



- The routers are too slow to perform bookkeeping tasks (queuing buffers, updating tables, etc.).
- The routers' buffer is too limited.
- Congestion in a subnet can occur if the processors are slow. Slow speed CPU at routers will perform the routine tasks such as queuing buffers, updating table etc slowly. As a result of this, queues are built up even though there is excess line capacity.
- Congestion is also caused by slow links. This problem will be solved when high speed links are used. But it is not always the case. Sometimes increase in link bandwidth can further deteriorate the congestion problem as higher speed links may make the network more unbalanced.Congestion can make itself worse. If a route!" does not have free buffers, it start ignoring/discarding the newly arriving packets. When these packets are discarded, the sender may retransmit them after the timer goes off. Such packets are transmitted by the sender again and again until the source gets the acknowledgement of these packets. Therefore multiple transmissions of packets will force the congestion to take place at the sending end.

How to correct the Congestion Problem:

Congestion Control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening and the other category removes congestion after it has taken place.



Types of Congestion Control Methods

These two categories are:

1. Open loop

2. Closed loop

Open Loop Congestion Control

• In this method, policies are used to prevent the congestion before it happens.

• Congestion control is handled either by the source or by the destination.

• The various methods used for open loop congestion control are:

Retransmission Policy

• The sender retransmits a packet, if it feels that the packet it has sent is lost or corrupted.

• However retransmission in general may increase the congestion in the network. But we need to implement good retransmission policy to prevent congestion.

• The retransmission policy and the retransmission timers need to be designed to optimize efficiency and at the same time prevent the congestion.

Window Policy

• To implement window policy, selective reject window method is used for congestion control.

• Selective Reject method is preferred over Go-back-n window as in Go-back-n method, when timer for a packet times out, several packets are resent, although some may have arrived safely at the receiver. Thus, this duplication may make congestion worse.

• Selective reject method sends only the specific lost or damaged packets.

Acknowledgement Policy

• The acknowledgement policy imposed by the receiver may also affect congestion.

• If the receiver does not acknowledge every packet it receives it may slow down the sender and help prevent congestion.

• Acknowledgments also add to the traffic load on the network. Thus, by sending fewer acknowledgements we can reduce load on the network.

• To implement it, several approaches can be used:

1. A receiver may send an acknowledgement only if it has a packet to be sent.

2. A receiver may send an acknowledgement when a timer expires.

3. A receiver may also decide to acknowledge only *N* packets at a time.

Discarding Policy

• A router may discard less sensitive packets when congestion is likely to happen.

• Such a discarding policy may prevent congestion and at the same time may not harm the integrity of the transmission.

Admission Policy

• An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual circuit networks.

• Switches in a flow first check the resource requirement of a flow before admitting it to the network.

• A router can deny establishing a virtual circuit connection if there is congestion in the “network or if there is a possibility of future congestion.

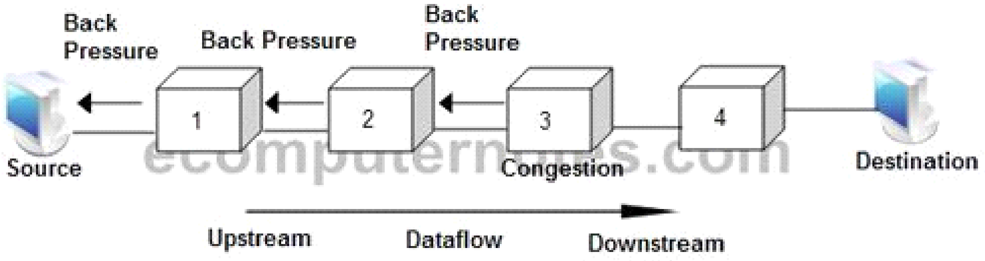
Closed Loop Congestion Control

• Closed loop congestion control mechanisms try to remove the congestion after it happens.

• The various methods used for closed loop congestion control are:

Backpressure

• Back pressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow.



Backpressure Method

• The backpressure technique can be applied only to virtual circuit networks. In such virtual circuit each node knows the upstream node from which a data flow is coming.

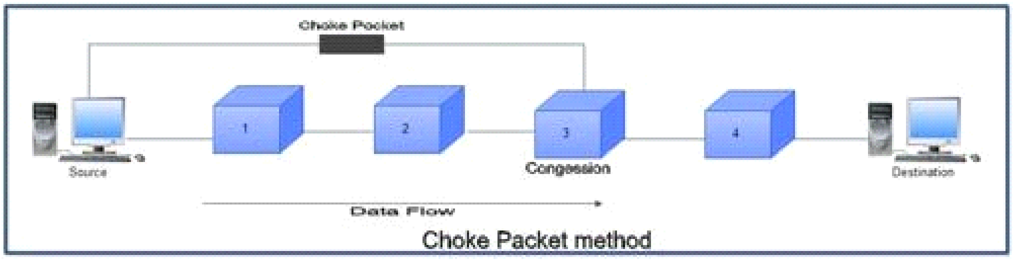
• In this method of congestion control, the congested node stops receiving data from the immediate upstream node or nodes.

• This may cause the upstream node on nodes to become congested, and they, in turn, reject data from their upstream node or nodes.

• As shown in fig node 3 is congested and it stops receiving packets and informs its upstream node 2 to slow down. Node 2 in turns may be congested and informs node 1 to slow down. Now node 1 may create congestion and informs the source node to slow down. In this way the congestion is alleviated. Thus, the pressure on node 3 is moved backward to the source to remove the congestion.

Choke Packet

- In this method of congestion control, congested router or node sends a special type of packet called choke packet to the source to inform it about the congestion.
- Here, congested node does not inform its upstream node about the congestion as in backpressure method.
- In choke packet method, congested node sends a warning directly to the source station *i.e.* the intermediate nodes through which the packet has traveled are not warned.



Implicit Signaling

- In implicit signaling, there is no communication between the congested node or nodes and the source.
- The source guesses that there is congestion somewhere in the network when it does not receive any acknowledgment. Therefore the delay in receiving an acknowledgment is interpreted as congestion in the network.
- On sensing this congestion, the source slows down.
- This type of congestion control policy is used by TCP.

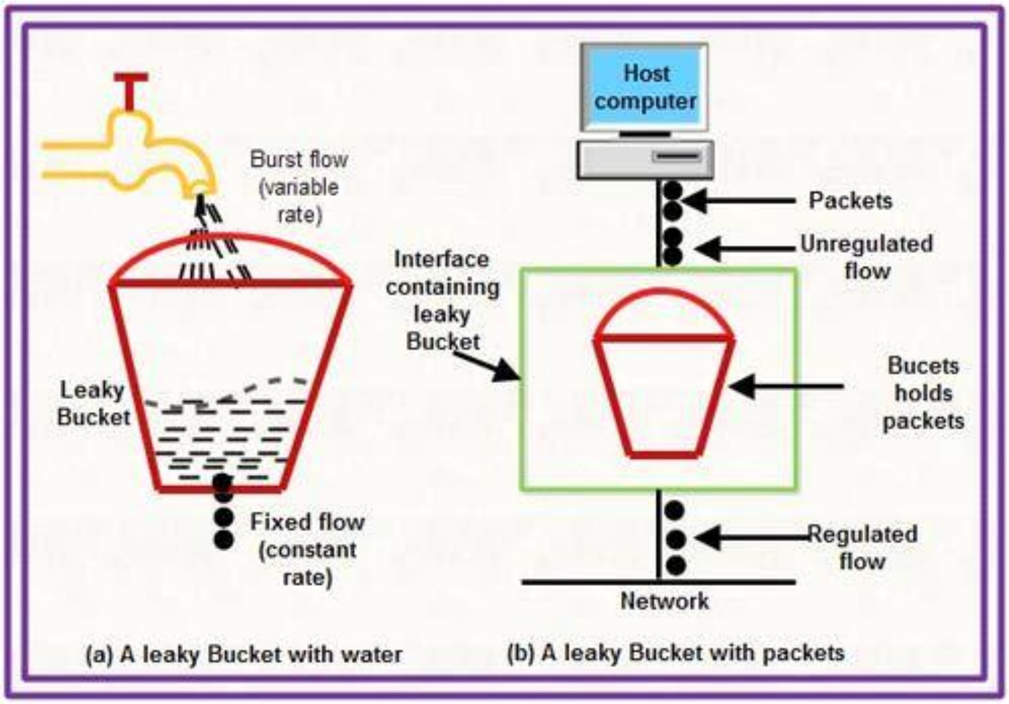
Explicit Signaling

- In this method, the congested nodes explicitly send a signal to the source or destination to inform about the congestion.
- Explicit signaling is different from the choke packet method. In choke packed method, a separate packet is used for this purpose whereas in explicit signaling method, the signal is included in the packets that carry data .
- Explicit signaling can occur in either the forward direction or the backward direction .
- In backward signaling, a bit is set in a packet moving in the direction opposite to the congestion. This bit warns the source about the congestion and informs the source to slow down.
- In forward signaling, a bit is set in a packet moving in the direction of congestion. This bit warns the destination about the congestion. The receiver in this case uses policies such as slowing down the acknowledgements to remove the congestion.

Congestion control algorithms

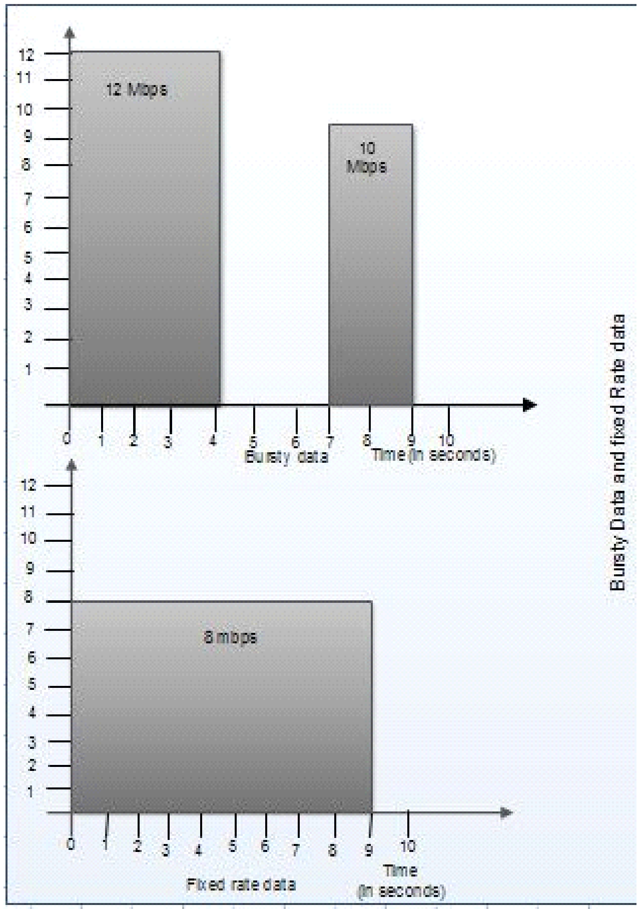
Leaky Bucket Algorithm

- It is a traffic shaping mechanism that controls the amount and the rate of the traffic sent to the network.
- A leaky bucket algorithm shapes bursty traffic into fixed rate traffic by averaging the data rate.
- Imagine a bucket with a small hole at the bottom.
- The rate at which the water is poured into the bucket is not fixed and can vary but it leaks from the bucket at a constant rate. Thus (as long as water is present in bucket), the rate at which the water leaks does not depend on the rate at which the water is input to the bucket.


Burst flow (variable rate)
Leaky Bucket
Fixed flow (constant rate)
(a) A leaky Bucket with water
Host computer
Packets
Unregulated flow
Interface containing leaky Bucket
Bucets holds packets
Regulated flow
Network
(b) A leaky Bucket with packets

- Also, when the bucket is full, any additional water that enters into the bucket spills over the sides and is lost.
- The same concept can be applied to packets in the network. Consider that data is coming from the source at variable speeds. Suppose that a source sends data at 12 Mbps for 4 seconds. Then there is no data for 3 seconds. The source again transmits data at a rate of 10 Mbps for 2 seconds. Thus, in a time span of 9 seconds, 68 Mb data has been transmitted.

If a leaky bucket algorithm is used, the data flow will be 8 Mbps for 9 seconds. Thus constant flow is maintained.



Token bucket Algorithm

• The leaky bucket algorithm allows only an average (constant) rate of data flow. Its major problem is that it cannot deal with bursty data.

• A leaky bucket algorithm does not consider the idle time of the host. For example, if the host was idle for 10 seconds and now it is willing to sent data at a very high speed for another 10 seconds, the total data transmission will be divided into 20 seconds and average data rate will be maintained. The host is having no advantage of sitting idle for 10 seconds.

• To overcome this problem, a token bucket algorithm is used. A token bucket algorithm allows bursty data transfers.

• A token bucket algorithm is a modification of leaky bucket in which leaky bucket contains tokens.

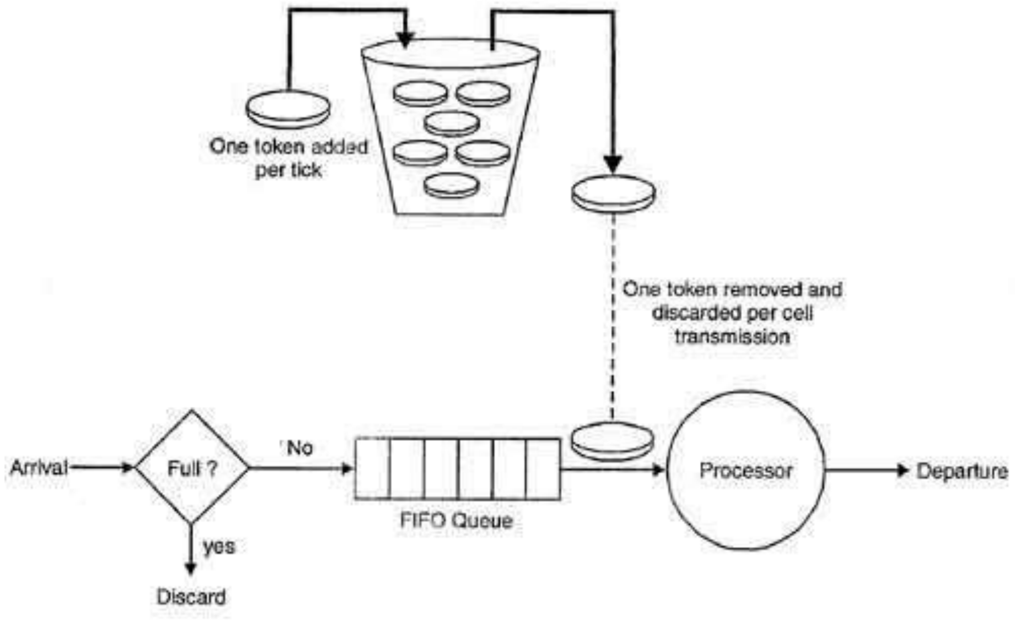
• In this algorithm, a token(s) are generated at every clock tick. For a packet to be transmitted, system must remove token(s) from the bucket.

• Thus, a token bucket algorithm allows idle hosts to accumulate credit for the future in form of tokens.

• For example, if a system generates 100 tokens in one clock tick and the host is idle for 100 ticks. The bucket will contain 10,000 tokens.

Now, if the host wants to send bursty data, it can consume all 10,000 tokens at once for sending 10,000 cells or bytes.

Thus a host can send bursty data as long as bucket is not empty.



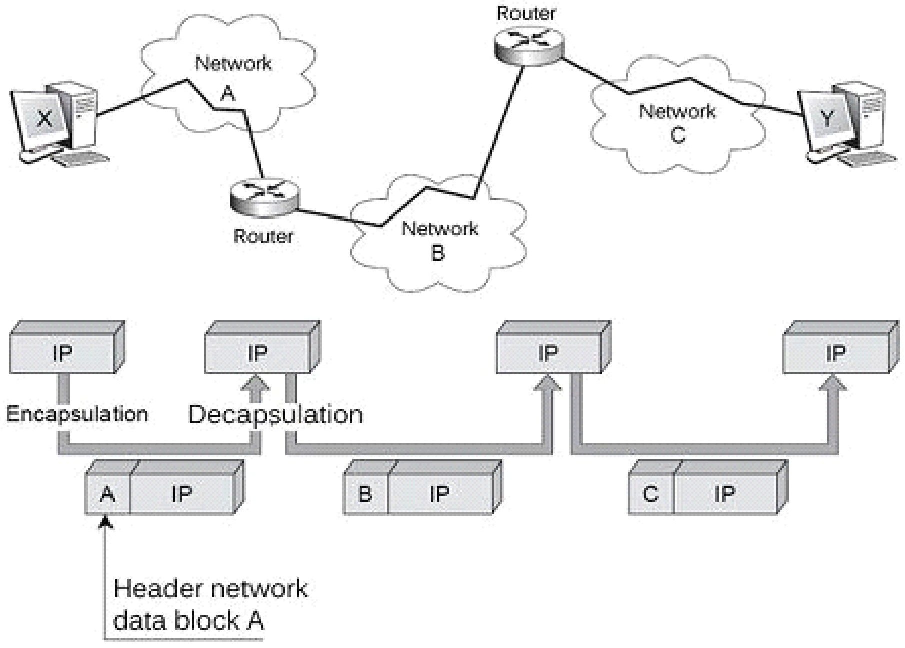
Token bucket algorithm

(IP) Internet Protocol

The Internet’s basic protocol called IP for Internet Protocol. The objective of starting this protocol is assigned to interconnect networks do not have the same frame-level protocols or package level. The internet acronym comes from inter-networking and corresponds to an interconnection fashion: each independent network must transport in the weft or in the data area of the packet an IP packet, as shown in Figure.

There are two generations of IP packets, called IPv4 (IP version 4) and IPv6 (IP version 6). IPv4 has been dominant so far. The transition to IPv6 could accelerate due to its adoption in many Asian countries. The transition is however difficult and will last many years.

• Internet Protocol (IP) of network layer contains addressing information and some control information that enables the packets to be routed.



- IP has two primary responsibilities:

1. Providing connectionless, best effort delivery of datagrams through a internetwork. The term best effort delivery means that IP does not provides any error control or flow control. The term connectionless means that each datagram is handled independently, and each datagram can follow different route to the destination. This implies that datagrams sent by the same source to the same destination could arrive out of order.

2. Providing fragmentation and reassembly of datagrams to support data links with different maximum transmission unit (MTU) sizes.

IP packet format

- Packets in the network layer are called datagrams.

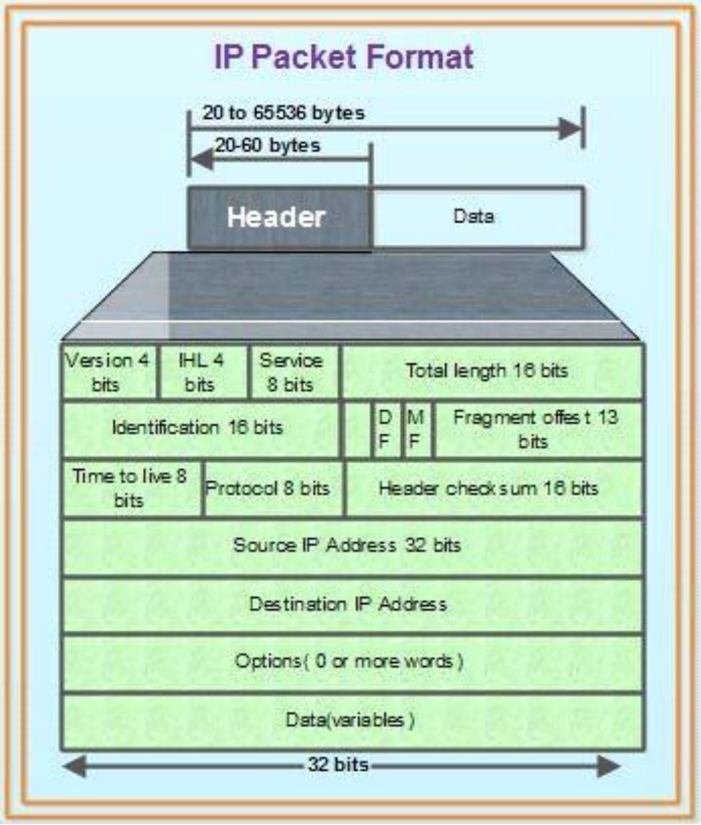
A datagram is a variable length packet consisting of two parts: header and data.

- The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

- The various fields in IP header are:

1. **Version**: It is a 4-bit field that specifies the version of IP currently being used. Two different versions of protocols are IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

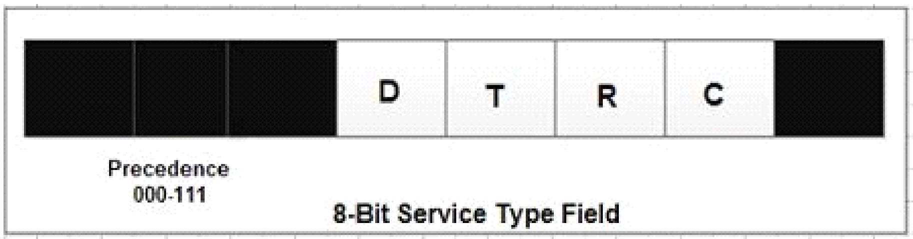
2. **IP Header Length (IHL):** This 4-bit field indicates the datagram header length in 32 bit word. The header length i8 not constant in IP. It may vary from 20 to 60 bytes. When there are no options, the header length is 20 bytes, and the value of this field is 5. When the option field is at its maximum size, the value of this field is 15.



3. **Services**: This 8 hit field was previously called services type but is now called differentiated services.

The various bits in service type are:

• A 3-bit precedence field that defines the priority of datagram in issues such as congestion. This 3-bit subfield ranges from 0 (000 in binary) to 7 (111 in binary).



• After 3-bit precedence there are four flag bits. These bits can be either 0 or 1 and only one of the bits can have value of 1 in each datagram.

The various flag bits are:

D : Minimize delay

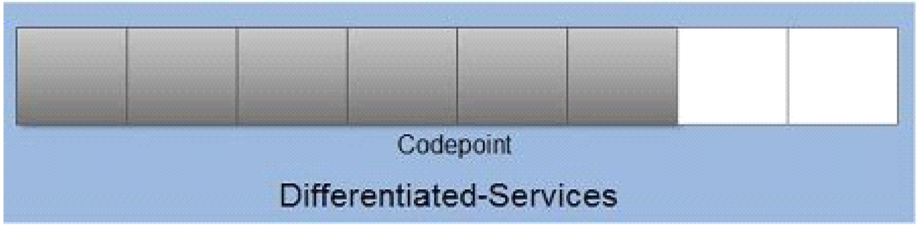
T : Maximize throughout

R : Maximize reliability

C : Minimize Cost

The various bits in differentiated services are:

• The first 6 bits defined a *code-point* and last two bits are not used. If the 3 rightmost bits are 0s, the 3 leftmost bits are interpreted the same as the precedence bits in the service type interpretation



4. **Total length**: This 16 bit field specifies the total length of entire IP datagram including data and header in bytes. As there are 16 bits, the total length of IP datagram is limited to 65,535 (2^{16} – 1) bytes.

5. **Identification**: This 16 bit field is used in fragmentation. A datagram when passing through different networks may be divided into fragments to match the network frame size. Therefore, this field contains an integer that identifies the current datagram. This field is used to help piece together datagram fragments.

6. **Flags**: Consists' of a 3 bit field of which the two low order bit DF, MF control fragmentation. DF stands for Don't Fragment. DF specifies whether the packet can be fragmented MF stands for more fragments. MF specifies whether the packet is the last fragment in a series of fragmented packets. The third or high order but is not used.

7. **Fragment Offset**: This 13 bit field indicates the position of the fragment's data relative to the beginning of the data in the original data-gram, which allows the destination IP process to properly reconstruct the original datagram.

8. **Time to Live**: It is 8 bit field that maintain a counter that gradually decrements down to zero, at which point the datagram is discarded. This keeps the packet from looping endlessly.

9. **Protocol**: This 8 bit field indicates which upper layer protocol receives incoming packets after IP processing is complete.

10. **Header Checksum**: This 16 bit field contains a checksum that covers only the header and not the data.

11. **Source IP address**: These 32-bit field contains the IP address of source machine.

12. **Destination IP address**: This 32-bit field contains the IP address of destination machine.

13. **Options**: This field allows IP to support various options such as security, routing, timing management and alignment.

14. **Data**: It contains upper layer information.

Internet Protocols are a set of rules that governs the communication and exchange of data over the internet. Both the sender and receiver should follow the same protocols in order to communicate the data. Any language has its own set of vocabulary and grammar which we need to know if we want to communicate in that language. Similarly, over the internet whenever we access a website or exchange some data with another device then these processes are governed by a set of rules called the internet protocols.

Types of internet protocol

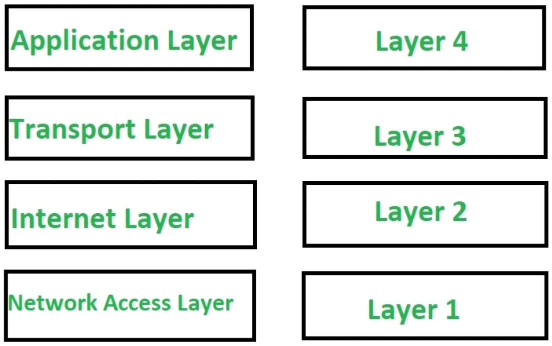
The Internet Protocols are of different types having different uses:-

1. TCP/IP(Transmission Control Protocol/ Internet Protocol): These are a set of standard rules that allows different types of computers to communicate with each other. The IP protocol ensures that each computer that is connected to the Internet is having a specific serial number called the IP address. TCP specifies how data is exchanged over the internet and how it should be broken into IP packets. It also makes sure that the packets have the information about the source of the message data, the destination of the message data, the sequence in which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination.

The functionality of TCP/IP is divided into 4 layers with each one having specific protocols:

- **Application Layer:** The application layer makes sure that the data from the sending end is received in a format that is acceptable and supported at the receiving end.
- **Transport Layer:** The transport layer is responsible for the smooth transmission of data from one end to the other. It is also responsible for reliable connectivity, error recovery, and flow control of the data.
- **Internet Layer:** This Internet Layer moves packets from source to destination by connecting independent networks.
- **Network Access Layer:** The Network Access Layer sees how a computer connects to a network.

4 Layers of TCP/IP Model



Application Layer	Layer 4
Transport Layer	Layer 3
Internet Layer	Layer 2
Network Access Layer	Layer 1

2. SMTP(Simple Mail Transfer Protocol): These protocols are important for sending and distributing outgoing emails. This protocol uses the header of the mail to get the email id of the receiver and enters the mail into the queue of outgoing mails. And as soon as, it delivers the mail to the receiving email id, it removes the email from the outgoing list.

3. PPP(Point to Point Protocol): It is a communication protocol that is used to create a direct connection between two communicating devices. This protocol defines the rules using which two devices will authenticate with each other and exchange information with each other. For example, A user connects his PC to the server of an Internet Service Provider also uses PPP. Similarly, for connecting two routers for direct communication it uses PPP.

4. FTP (File Transfer Protocol): This protocol is used for transferring files from one system to the other. This works on a client-server model. When a machine requests for file transfer from another machine, the FTO sets up a connection between the two and authenticates each other using their ID and Password. And, the desired file transfer takes place between the machines.

5. SFTP(Secure File Transfer Protocol): SFTP which is also known as SSH FTP refers to File Transfer Protocol (FTP) over Secure Shell (SSH) as it encrypts both commands and data while in transmission. SFTP acts as an extension to SSH and encrypts files and data then sends them over a secure shell data stream. This protocol is used to remotely connect to other systems while executing commands from the command line.

6. HTTP(HyperText Transfer Protocol): This protocol is used to transfer hypertexts over the internet and it is defined by the www(world wide web) for information transfer. This protocol defines how the information needs to be formatted and transmitted. And, it also defines the various actions the web browsers should take in response to the calls made to access a particular web page. Whenever a user opens their web browser, the user will indirectly use HTTP as this is the protocol that is being used to share text, images, and other multimedia files on the World Wide Web.

Note: *Hypertext refers to the special format of the text that can contain links to other texts.*

7. HTTPS(HyperText Transfer Protocol Secure): HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network with the SSL/TLS protocol for encryption and authentication. So, generally, a website has an HTTP protocol but if the website is such that it receives some sensitive information such as credit card details, debit card details, OTP, etc then it requires an SSL certificate installed to make the website more secure. So, before entering any sensitive information on a website, we should check if the link is HTTPS or not. If it is not HTTPS then it may not be secure enough to enter sensitive information.

8. TELNET(Terminal Network): TELNET is a standard TCP/IP protocol used for virtual terminal service given by ISO. This enables one local machine to connect with another. The computer which is being connected is called a remote computer and which is connecting is called the local computer. TELNET operation lets us display anything being performed on the remote computer in the local computer. This operates on the client/server principle. The local computer uses the telnet client program whereas the remote computer uses the telnet server program.

9. POP3(Post Office Protocol 3): POP3 stands for Post Office Protocol version 3. It has two Message Access Agents (MAAs) where one is client MAA (Message Access Agent) and another is server MAA(Message Access Agent) for accessing the messages from the mailbox. This protocol helps us to retrieve and manage emails from the mailbox on the receiver mail server to the receiver's computer. This is implied between the receiver and receiver mail server.

IP ADDRESS

An IP address represents an Internet Protocol address. A unique address that identifies the device over the network. It is almost like a set of rules governing the structure of data sent over the Internet or through a local network. An IP address helps the Internet to distinguish between different routers, computers, and websites. It serves as a specific machine identifier in a specific network and helps to improve visual communication between source and destination.

IP address structure:

IP addresses are displayed as a set of four digits- the default address maybe 192.158.1.38. Each number on the set may range from 0 to 255. Therefore, the total IP address range ranges from 0.0.0.0 to 255.255.255.255.

IP address is basically divided into two parts: X1. X2. X3. X4

1. [X1. X2. X3] is the Network ID

2. [X4] is the Host ID

- **NetworkID**– It is the part of the left-hand IP address that identifies the specific network where the device is located. In the normal home network, where the device has an IP address

192.168.1.32, the 192.168.1 part of the address will be the network ID. It is customary to fill in the last part that is not zero, so we can say that the device's network ID is 192.168.1.0.

- **HostingID**– The host ID is part of the IP address that was not taken by the network ID. Identifies a specific device (in the TCP / IP world, we call devices "host") in that network. Continuing with our example of the IP address 192.168.1.32, the host ID will be 32- the unique host ID on the 192.168.1.0 network.

IPAddressTypes:

There are 4 types of IP Addresses- Public, Private, Fixed, and Dynamic. Among them, public and private addresses are derived from their local network location, which should be used within the network while public IP is used offline.

- **PublicIPaddress**–
  A public IP address is an Internet Protocol address, encrypted by various servers/devices. That's when you connect these devices with your internet connection. This is the same IP address we show on our homepage. So why the second page? Well, not all people speak the IP language. We want to make it as easy as possible for everyone to get the information they need. Some even call this their external IP address. A public Internet Protocol address is an Internet Protocol address accessed over the Internet. Like the postal address used to deliver mail to your home, the public Internet Protocol address is a different international Internet Protocol address assigned to a computer device. The web server, email server, and any server device that has direct access to the Internet are those who will enter the public Internet Protocol address. Internet Address Protocol is unique worldwide and is only supplied with a unique device.
- **PrivateIPaddress**–
  Everything that connects to your Internet network has a private IP address. This includes computers, smartphones, and tablets but also any Bluetooth-enabled devices such as speakers, printers, or smart TVs. With the growing internet of things, the number of private IP addresses you have at home is likely to increase. Your router needs a way to identify these things separately, and most things need a way to get to know each other. Therefore, your router generates private IP addresses that are unique identifiers for each device that separates the network.
- **StaticIPAddress**–
  A static IP address is an invalid IP address. Conversely, a dynamic IP address will be provided by the Dynamic Host Configuration Protocol (DHCP) server, which can change. The Static IP address does not change but can be changed as part of normal network management.
  Static IP addresses are incompatible, given once, remain the same over the years. This type of IP also helps you get more information about the device.
- **DynamicIPaddress**–
  It means constant change. A dynamic IP address changes from time to time and is not always the same. If you have a live cable or DSL service, you may have a strong IP address. Internet Service Providers (provide customers with dynamic IP addresses because they are too expensive. Instead of one permanent IP address, your IP address is taken out of the address pool and assigned to you. After a few days, weeks, or sometimes even months, that number is returned to the lake and given a new number. Most ISPs will not provide a static IP address to customers who live there and when they do, they are usually more expensive. Dynamic IP addresses are annoying, but with the right software, you can navigate easily and for free.

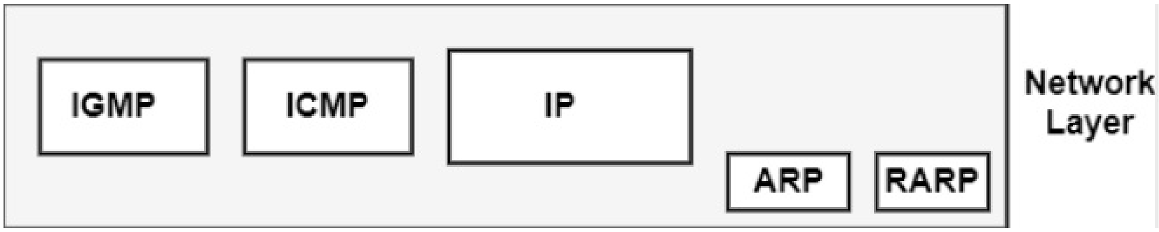
INTERNET CONTROL PROTOCOL

The ICMP represents Internet Control Message Protocol. It is a network layer protocol. It can be used for error handling in the network layer, and it is generally used on network devices, including routers. IP Protocol is a best-effect delivery service that delivers a datagram from its original source to its final destination. It has two deficiencies−

- Lack of Error Control
- Lack of assistance mechanisms

IP protocol also lacks a structure for host and management queries. A host needs to resolve if a router or another host is alive, and sometimes a network manager needs information from another host or router.

ICMP has been created to compensate for these deficiencies. It is a partner to the IP protocol.



ICMP is a network layer protocol. But, its messages are not passed directly to the data link layer. Instead, the messages are first encapsulated inside the IP datagrams before going to the lower layer.

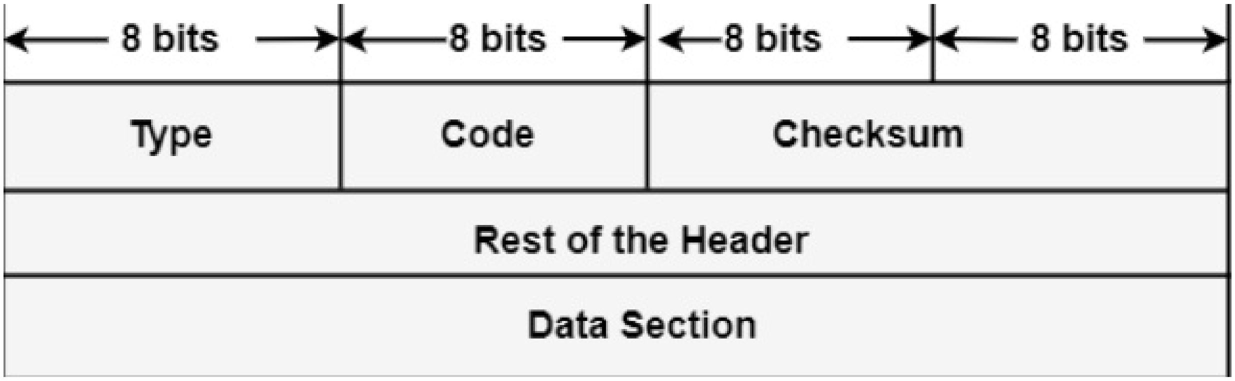
The cost of the protocol field in the IP datagram is I, to indicate that IP data is an ICMP message.

The error reporting messages report issues that a router or a host (destination) may encounter when it phases an IP packet.

The query messages, which appear in pairs, help a host or a network manager to get specific data from a router or another host

ICMP Message Format

AN ICMP message includes an 8-byte header and a variable size data format.



- **Type:** It is an 8-bit field. It represents the ICMP message type. The values area from 0 to 127 are described for ICMPv6, and the values from 128 to 255 are the data messages.
- **Code:** It is an 8-bit field that represents the subtype of the ICMP message.

- **Checksum:** It is a 16-bit field to recognize whether the error exists in the message or not.

UNIT V

TRANSPORT LAYER

TRANSPORT LAYER: The network layer provides end-to-end packet delivery using datagrams or virtual circuits. The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine with a desired level of reliability that is independent of the physical networks currently in use.

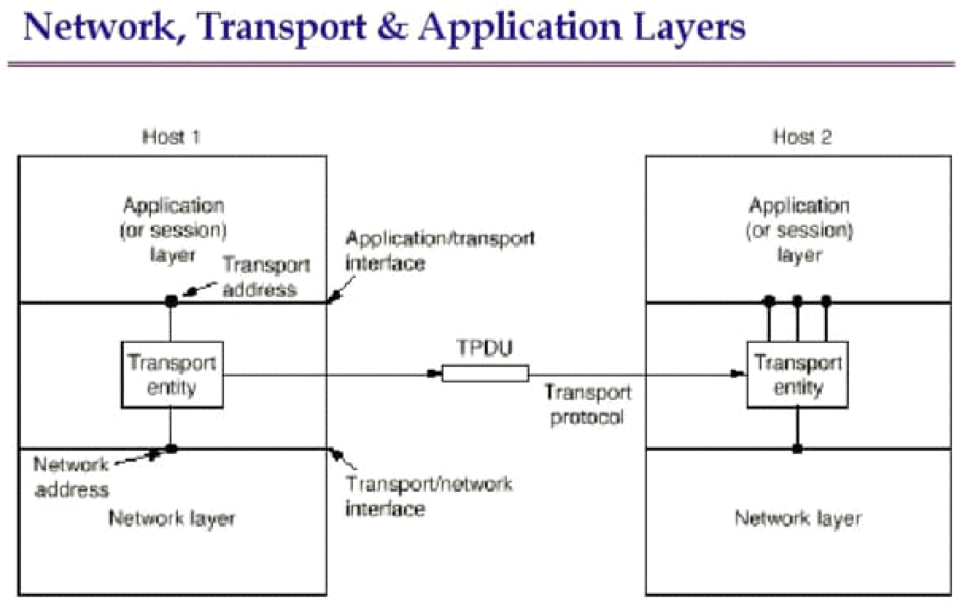
It is the heart of the whole protocol hierarchy. Its task is to provide reliable, cost-effective data transport from the source machine to the destination machine, independently of the physical network or networks currently in use.

TRANSPORT SERVICES

Services Provided to the Upper Layers

The ultimate goal of the transport layer is to provide efficient, reliable, and cost-effective service to its users, normally processes in the application layer. To achieve this goal, the transport layer makes use of the services provided by the network layer. The hardware and/or software within the transport layer that does the work is called the transport entity. The transport entity can be located in the operating system kernel, in a separate user process, in a library package bound into network applications, or conceivably on the network interface card.

The relationship of the network, application and transport layers is shown as


Network, Transport & Application Layers

Just as there are two types of network service, connection-oriented and connectionless, there are also two types of transport service. The connection-oriented transport service is similar to the connection-oriented network service in many ways. In both cases, connections have three phases: establishment, data transfer, and release.

Addressing and flow control are also similar in both layers. Furthermore, the connectionless transport service is also very similar to the connectionless network service.

The bottom four layers can be seen as the transport service provider, whereas the upper layer(s) are the transport service user. This distinction of provider versus user has a considerable impact on the design of the layers and puts the transport layer in a key position, since it forms the major boundary between the provider and user of the reliable data transmission service.

The services provided by the transport layer are explained below −

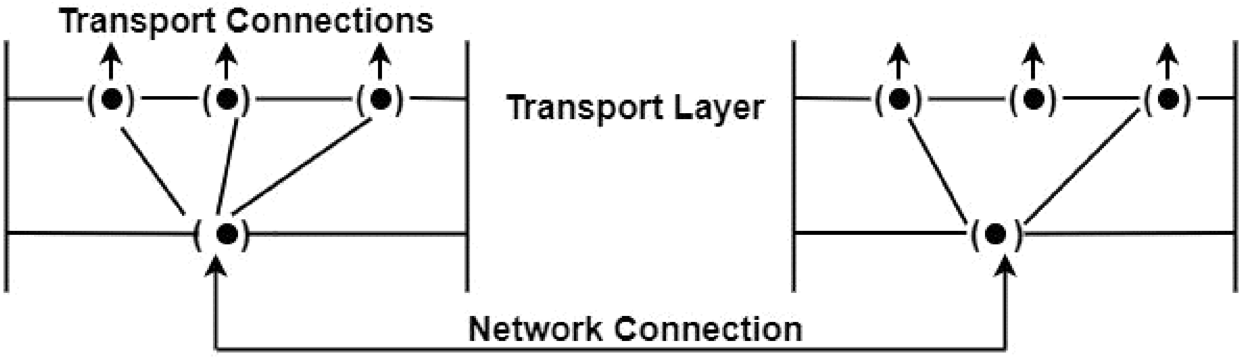
Address Mapping
It means mapping of transport address onto the network address. Whenever a session entity requests to send a transport service data unit (TSDU) to another session entity, it sends its transport service access point address as its identification. The transport entity then determines the network service access point (NSAP) address. This is known as address mapping.

Assignment of Network Connection
The transport entity assigns a network connection for carrying the transport protocol data units (TPDUs). The transport entity establishes this assigned network connection. In some of the transport protocols, recovery from network disconnection is allowed. In such protocols, whenever a disconnection occurs, the transport entity reassigns the transport of TPDUs to a different network connection.

Multiplexing of Transport Connections
For optimum network link uses, the transport entity can create multiple end-to-end transport connections to the network connection, referred to as multiplexing.

There are various TSDUs (multiplexed) identified by the receiving transport entity using the transport connection endpoint identifier (TCEPI), attached to each TSDU by the sending transport entity.

The TCEP identifier is unique for each connection, as shown in the figure below −

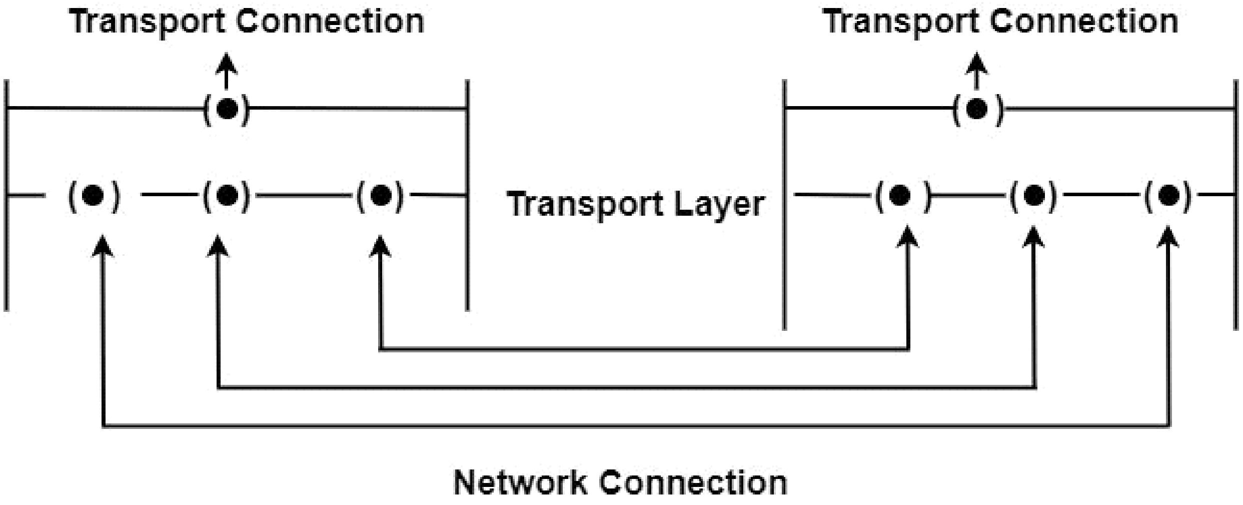


Multiplexing

Splitting of Transport Connection

When the service quality offered by the network service is less than the required quality of service or when greater resilience is required against network connection failures, then splitting is done by the transport entity. Splitting means TPDUs belonging to one transport connection may be sent over different network connections.

Splitting requires the re-sequencing because it results in the reordering of TSDUs, as shown in the figure shown below −



Spliting

Establishment of Transport Connection

The transport layer establishes the transport connection by sending a request. For establishing a link, it uses the T-CONNECT service primitives. The transport entity provides the quality of service, requirement, and collect addresses services.

Data Transfer

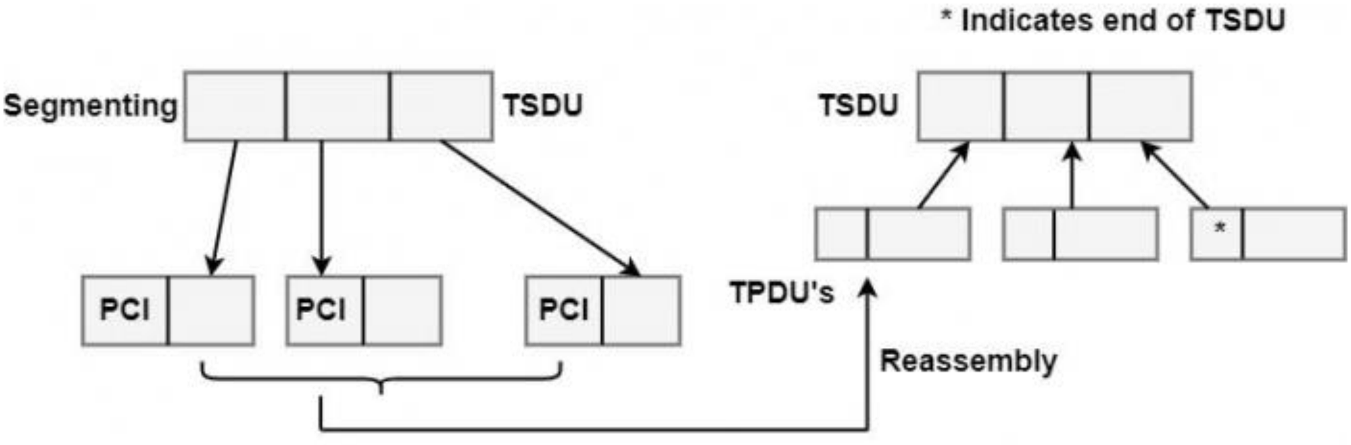
The transport layer provides the data transfer of two types, such as the regular data transfer and expedited data transfer. In normal data transfer, the user can request to transfer user data with any integral number of octets.

This transfer is transparent, i.e., user data boundaries are preserved during the transfer, and there are no constraints on the content and number of octets. The mode of data transfer can be two ways simultaneously. The expedited data transfer has a distinct control flow, and it can pass all the data queue with maximum priority for delivery. It is a user optional or optional provider service. The number of user data octets is restricted to 16.

Segmentation and Concatenation of TPDUs

The transport entity divides the transport service data unit into several transport protocol data units, each with a separate header containing a PCI (Protocol Control Identifier). This function is known as segments.

This segmenting function is used when the network service cannot support the transport protocol data unit's size containing an unsegmented TSDU. A reassembly process is performed at the transmitting end for such TPDUs.

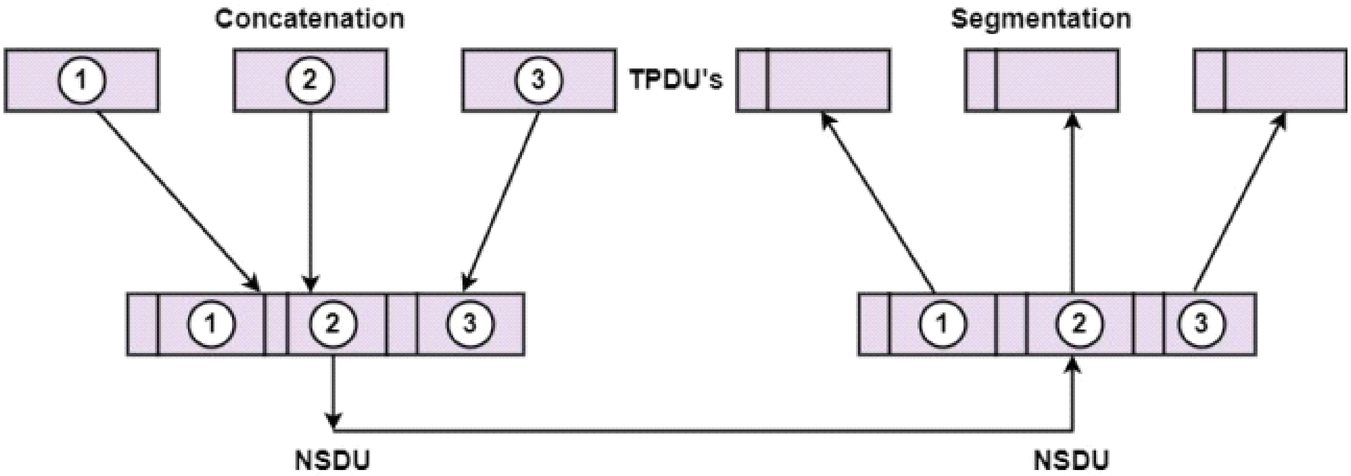


Segmenting and concatenation of TPDUs

The reverse function of segments is known as concatenation. The concatenation enables the mapping of several TPDUs onto a single NSDU (Network Service Data Unit). These TPUs may belong to the same or several transport connections. If they belong to different transport connections, they must be travelling in the exact directions. At the receiving end, a separation function is performed by the transport entity.

The transport entity identifies the boundary of different TPDUs. Concatenation is done for improving the efficiency of utilization of the network service.

On concatenation, there are some restrictions as to which type of TPDUs can be concatenated so that their boundaries should be identified by the transport entity, as shown in the figure below.



Flow Control
The transport entity uses a modified form of sliding window protocol for flow control. This flow control is required because the transport layer may experience back pressure from the network layer.

In the mechanism, the window size is variable and controlled by the receiver. A credit allocated is sent to the receiver's sender, which indicates how many TPDUs can be received by it.

Error Recovery
The errors at this level can be introduced due to TPDU errors, protocol errors or signal failure conditions of network connections, i.e., reset or release of network connections. Such errors occurring at layer 3 are reported to the transport layer. The TPDU errors can be in the form of lost TPDU, duplicated TPDU, re-ordering of sequence, or content errors.

The duplicate TPDUs are discarded, lost are acknowledged to resend. In the recording, they are re-sequenced, and content errors are detected by incorporating error detection bytes in TPDUs by the transport entity.

Such TPDUs with content errors are discarded and treated as lost, and hence they are also acknowledged. In the case of protocol errors, the connection is released, and in the case of signal failure errors, reassignment of network connection and resynchronization is done.

Sequence Numbering
Each TPDU is given a sequence number by a transport entity that is seven bits long in the normal operations mode. This sequence numbering is done to provide flow control and error recovery. In the case of extended mode, the sequence number can be 31 bits long.

TCP is a connection-oriented protocol and every connection-oriented protocol needs to establish a connection in order to reserve resources at both the communicating ends.

TCP Connection Management

Introduction

TCP is a unicast **connection-oriented** protocol. Before either end can send data to the other, a connection must be established between them. TCP detects and repairs essentially all the data transfer problems that may be introduced by packet loss, duplication, or errors at the IP layer (or below).

Because of its management of **connection state** (information about the connection kept by both endpoints), TCP is a considerably more complicated protocol than UDP. UDP is a connectionless protocol that involves no connection establishment or termination. One of the major differences between the two is the amount of detail required to handle the various TCP states properly: when connections are created, terminated normally, and reset without warning. Other chapters discuss what happens once the connection is established and data is transferred.

During connection establishment, several options can be exchanged between the two endpoints regarding the parameters of the connection. Some options are allowed to be sent only when the connection is established, and others can be sent later. The TCP header has a limited space for holding options (40 bytes).

TCP Connection Establishment and Termination

A TCP connection is defined to be a 4-tuple consisting of two IP addresses and two port numbers. It is a pair of **endpoints** or **sockets** where each endpoint is identified by an (IP address, port number) pair.

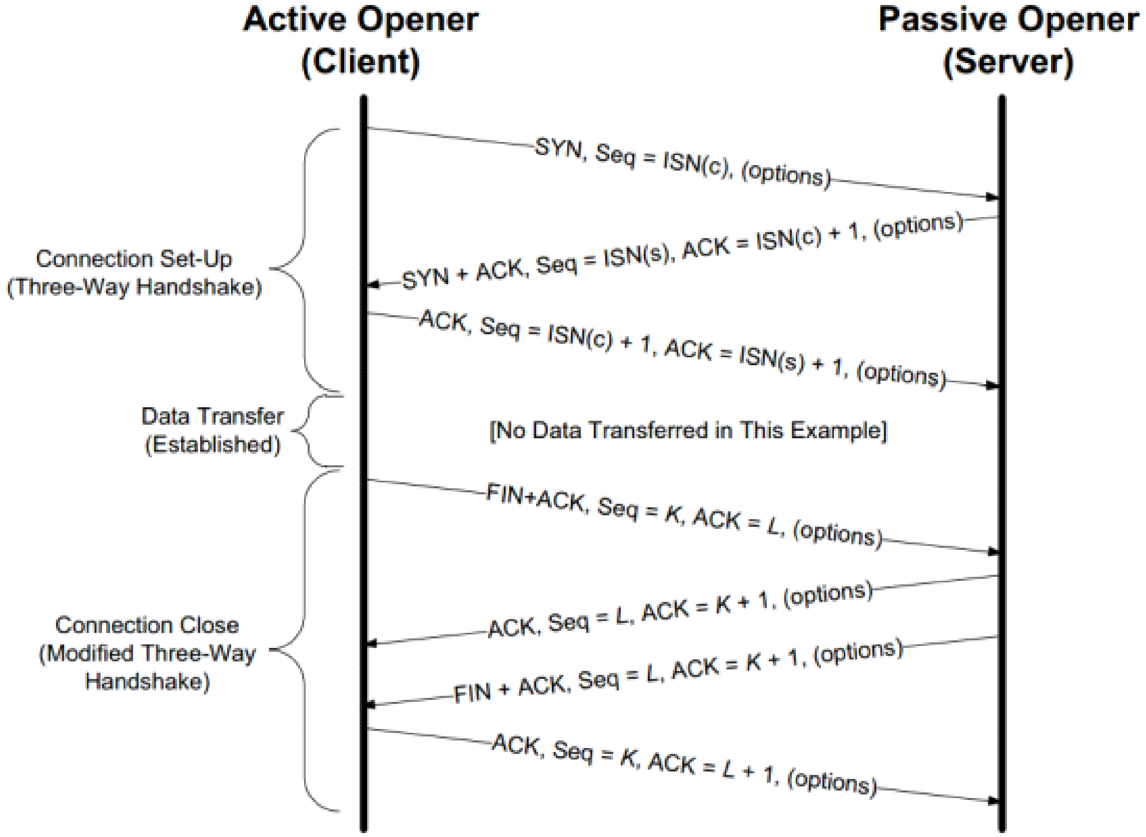
A connection typically goes through three phases:

- Setup

- Data transfer (called *established*)
- Teardown (*closing*).

Some of the difficulty in creating a robust TCP implementation is handling all of the transitions between and among these phases correctly.

A typical TCP connection establishment and close (without any data transfer) is shown below:


Active Opener (Client)
Passive Opener (Server)
SYN, Seq = ISN(c), (options)
SYN + ACK, Seq = ISN(s), ACK = ISN(c) + 1, (options)
ACK, Seq = ISN(c) + 1, ACK = ISN(s) + 1, (options)
Connection Set-Up (Three-Way Handshake)
Data Transfer (Established)
[No Data Transferred in This Example]
FIN+ACK, Seq = K, ACK = L, (options)
ACK, Seq = L, ACK = K + 1, (options)
FIN + ACK, Seq = L, ACK = K + 1, (options)
ACK, Seq = K, ACK = L + 1, (options)
Connection Close (Modified Three-Way Handshake)

Connection Establishment *

To establish a TCP connection, the following events usually take place:

- The **active opener** (normally called the client) sends a SYN segment (a TCP/IP packet with the SYN bit field turned on in the TCP header) specifying the port number of the peer to which it wants to connect and the client's initial sequence number or ISN(c) It typically sends one or more options at this point. This is segment 1.
- The server responds with its own SYN segment containing its initial sequence number (ISN(s)). This is segment 2. The server also acknowledges the client's SYN by ACKing ISN(c) plus 1. A SYN consumes one sequence number and is retransmitted if lost.
- The client must acknowledge this SYN from the server by ACKing ISN(s) plus 1. This is segment 3.

These three segments complete the connection establishment. This is often called the **three-way handshake**. Its main purposes are to let each end of the connection know that a connection is starting and the special details that are carried as options, and to exchange the ISNs.

The side that sends the first SYN is said to perform an **active open**. This is typically a client. The other side, which receives this SYN and sends the next SYN, performs a **passive open**. It is most commonly called the server.A supported but unusual **simultaneous open** when both sides can do an active open at the same time and become both clients and servers.

TCP supports the capability of carrying application data on SYN segments. This is rarely used, however, because the Berkeley sockets API does not support it.

Connection Termination *

Traditionally, it was most common for the client to initiate a close. However, other servers (e.g., Web servers) initiate a close after they have completed a request. Usually a close operation starts with an application indicating its desire to terminate its connection (e.g., using the close() system call). The closing TCP initiates the close operation by sending a FIN segment (a TCP segment with the FIN bit field set). The complete close operation occurs after both sides have completed the close:

- The **active closer** sends a FIN segment specifying the current sequence number the receiver expects to see. The FIN also includes an ACK for the last data sent in the other direction.
- The **passive closer** responds by ACKing value $K + 1$ to indicate its successful receipt of the active closer's FIN. At this point, the application is notified that the other end of its connection has performed a close. Typically this results in the application initiating its own close operation. The passive closer then effectively becomes another active closer and sends its own FIN. The sequence number is equal to L.
- To complete the close, the final segment contains an ACK for the last FIN. Note that if a FIN is lost, it is retransmitted until an ACK for it is received.

While it takes three segments to establish a connection, it takes four to terminate one. It is also possible for the connection to be in a half-open state, although this is not common. This reason is that TCP's data communications model is bidirectional, meaning it is possible to have only one of the two directions operating. The **half-close** operation in TCP closes only a single direction of the data flow. Two half-close operations together close the entire connection. The rule is that either end can send a FIN when it is done sending data. When a TCP receives a FIN, it must notify the application that the other end has terminated that direction of data flow. The sending of a FIN is normally the result of the application issuing a close operation, which typically causes both directions to close.

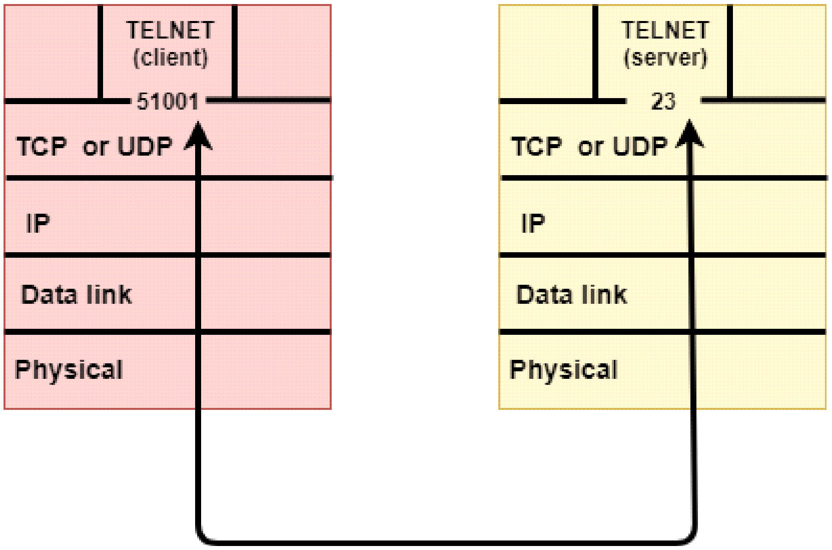
The seven segments discussed are baseline overheads for any TCP connection that is established and cleared "gracefully". (There are more abrupt ways to tear down a TCP connection using special reset segments, which are covered later.) When a small amount of data needs to be exchanged, it is now apparent why some applications prefer to use UDP because of its ability to send and receive data without establishing connections. However, such applications are then faced with handling their own error repair features, congestion management, and flow control.

Transport Layer protocols

- The transport layer is represented by two protocols: TCP and UDP.
- The IP protocol in the network layer delivers a datagram from a source host to the destination host.
- Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process. When a host sends a message to other host means that

source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.

- An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.
- Each port is defined by a positive integer address, and it is of 16 bits.

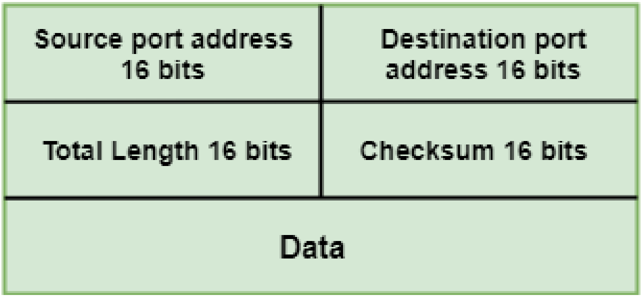


UDP

- UDP stands for **User Datagram Protocol**.
- UDP is a simple protocol and it provides nonsequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.
- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

User Datagram Format

The user datagram has a 16-byte header which is shown below:



Source port address 16 bits	Destination port address 16 bits
Total Length 16 bits	Checksum 16 bits
Data	

Where,

- **Source port address:** It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.
- **Destination port address:** It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
- **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.
- **Checksum:** The checksum is a 16-bit field which is used in error detection.

Disadvantages of UDP protocol

- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

TCP

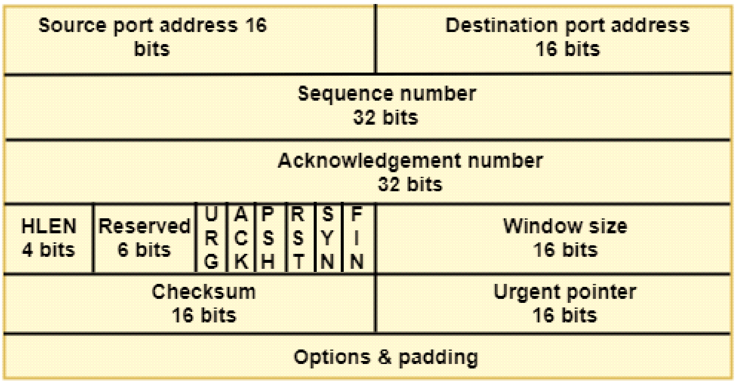
- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

Features Of TCP protocol

- **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
- **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination.
  The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.
- **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
- **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.
- **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.

- **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:
  - Establish a connection between two TCPs.
  - Data is exchanged in both the directions.
  - The Connection is terminated.

TCP Segment Format



<table>
<tr><td colspan="9">Source port address 16 bits</td><td>Destination port address 16 bits</td></tr>
<tr><td colspan="10">Sequence number 32 bits</td></tr>
<tr><td colspan="10">Acknowledgement number 32 bits</td></tr>
<tr><td>HLEN 4 bits</td><td>Reserved 6 bits</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td></td><td>Window size 16 bits</td></tr>
<tr><td colspan="9">Checksum 16 bits</td><td>Urgent pointer 16 bits</td></tr>
<tr><td colspan="10">Options &amp; padding</td></tr>
</table>

Where,

- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
- **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
- **Reserved:** It is a six-bit field which is reserved for future use.
- **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

There are total six types of flags in control field:

- **URG:** The URG field indicates that the data in a segment is urgent.
- **ACK:** When ACK field is set, then it validates the acknowledgement number.

- **PSH:** The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.
- **RST:** The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers.
- **SYN:** The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation (with the ACK bit set), and confirmation acknowledgement.
- **FIN:** The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination confirmation.
  - **Window Size:** The window is a 16-bit field that defines the size of the window.
  - **Checksum:** The checksum is a 16-bit field used in error detection.
  - **Urgent pointer:** If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
  - **Options and padding:** It defines the optional fields that convey the additional information to the receiver.

Network Security

Network security refers to the measures taken by any enterprise or organisation to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organisation that handles large amount of data, has a degree of solutions against many **cyber threats**.

- The most basic example of Network Security is password protection where the user of the network oneself chooses. In the recent times, Network Security has become the central topic of cyber security with many organisations inviting applications of people who have skills in this area. The network security solutions protect various **vulnerabilities of the computer systems** such as:

1. Users
2. Locations
3. Data
4. Devices
5. Applications

Network Security: Working

The basic principle of network security is protecting huge stored data and network in layers that ensures a bedding of rules and regulations that have to be acknowledged before performing any activity on the data.

These levels are:

1. Physical
2. Technical
3. Administrative

These are explained as following below.

- **Physical Network Security:**
  This is the most basic level that includes protecting the data and network though unauthorized personnel from acquiring the control over the confidentiality of the network. These includes

external peripherals and routers might be used for cable connections. The same can be achieved by using devices like bio-metric systems.

- **Technical Network Security:**
  It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One, protection from the unauthorized users and the other being protection from malicious activities.

- **Administrative Network Security:**
  This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done over the infrastructure.

Types of Network Security:

The few types of network securities are discussed as below :

- **Access Control:**
  Not every person should have complete allowance to the accessibility to the network or its data. The one way to examine this is by going through each personnel's details. This is done through Network Access Control which ensures that only a handful of authorized personnel must be able to work with allowed amount of resources.

- **Antivirus and Anti-malware Software:**
  This type of network security ensures that any malicious software does not enter the network and jeopardize the security of the data. The malicious software like Viruses, Trojans, Worms are handled by the same. This ensure that not only the entry of the malware is protected but also that the system is well equipped to fight once it has entered.

- **Cloud Security:**
  Now a day, a lot many organisations are joining hands with the cloud technology where a large amount of important data is stored over the internet. This is very vulnerable to the malpractices that few unauthorized dealers might pertain. This data must be protected an it should be ensured that this protection is not jeopardize over anything. Many businesses embrace SaaS applications for providing some of its employees the allowance of accessing the data stored over the cloud. This type of security ensures in creating gaps in visibility of the data.

Cryptography

Cryptography refers to the science and art of transforming messages to make them secure and immune to attacks. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration but can also be used for user authentication.

Components

There are various components of cryptography which are as follows −

Plaintext and Ciphertext

The original message, before being transformed, is called plaintext. After the message is transformed, it is called ciphertext. An encryption algorithm transforms the plaintext into ciphertext; a decryption algorithm transforms the ciphertext back into plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

Cipher

We refer to encryption and decryption algorithms as ciphers. The term cipher is also used to refer to different categories of algorithms in cryptography. This is not to say that every sender-receiver pair needs their very own unique cipher for secure communication. On the contrary, one cipher can serve millions of communicating pairs.

Key

A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. To encrypt a message, we need an encryption algorithm, an encryption key, and plaintext. These create the ciphertext. To decrypt a message, we need a decryption algorithm, a decryption key, and the ciphertext. These reveal the original plaintext.

Types

There are two types of cryptography which are as follows −

Symmetric Key Cryptography

In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

Asymmetric-Key Cryptography

In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

In public-key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption. The public key is available to the public, and the private key is available only to an individual

*****